SECURUS Technologies™



ITN CFCA #2022000005
OFFENDER COMMUNICATIONS
COLORADO DEPARTMENT OF CORRECTIONS
Attachment 1: Statement of Work



We exist to **SERVE** and **CONNECT** to make our world safe.

An RFP Solution Prepared for:
Colorado Department of Corrections
ITN CFCA #2022000005
Offender Communications
Due: April 7, 2022, 2:00pm MT

Presented to:
Holly Hammel
Associate Director of Procurement
Colorado Department of Corrections
275 W. Hwy 50
Canon City, Colorado 812112
719-429-1724
Holly.hammel@state.co.us

Presented by:
Russell Roberts
Chief Growth Officer
Securus Technologies, LLC
4000 International Parkway
Carrollton, Texas 75007

TABLE OF CONTENTS

COVER LETTER	**2**
EXECUTIVE SUMMARY	**6**
ATTACHMENT 1: STATEMENT OF WORK (SOW)	**11**
CLOSING	**558**
SECURUS ATTACHMENTS	**559**

COVER LETTER

April 7, 2022

State of Colorado
Colorado Department of Corrections
Division of Canteen Services
Attn: Holly Hammel, Associate Director of Procurement
275 W. Hwy 50
Canon City, CO 81212

Re: ITN CFCA #2022000005 – Offender Communications

Dear Ms. Hammel,

Securus Technologies, LLC (Securus) appreciates the opportunity to submit our proposed solution for Offender Communications to the Division of Canteen Services. In addition to our telephone services, our solution includes implementing tablet services and focusing on offender educational opportunities. We thoroughly reviewed your Invitation to Negotiate (ITN) and are confident that our proposed solution will exceed your specifications.

As a leader in prison communications, we are excited about the opportunity to provide your offenders with industry-leading tablets, telephone services, video visitation, educational capabilities, music, games, and much more. Our proposal also includes a wide variety of GED-prep, K-12, post-secondary, and life skills content that will positively affect the lives of your residents.

To execute our vision for Colorado, Securus will install and maintain a fiber optic IT network that will enable offenders to make monitored and recorded telephone calls, both via physical phones and their tablets, to approved family members and friends. This network will also support our correctional grade tablets, which provide additional services, including but not limited to scheduling, commissary ordering, secured messaging, phone calling, educational programming, training, music, e-books, and more.

Securus will furnish all labor, materials, equipment, and services necessary for the installation, maintenance, repair, and replacement of our offender telephone, tablet, and kiosk solutions. We will also implement and support all services' ongoing operation and maintenance. Our entire solution, including full training and documentation, will be

provided at **no cost** to the Division of Canteen Services or any other State of Colorado entity.

Additionally, we will provide the following services to The Division of Canteen Services and the DOC:

Proficient Industry Experience – We have over 30 years of experience providing offenders communications solutions to prisons. Over 2,600 prisons and jails have our Secure Call Platform (SCP) installed, making it the industry's **most deployed offender telephone system.** More than 450,000 offenders currently use Securus tablets.

Managed Product Portfolio – Our employees work, service, and enhance our technologies and services. We believe it is essential to own and maintain our platforms and services to quickly respond to partner requests without depending on a third party.

Increased Staff Efficiency through Technology and Automation – We will continue to deliver web and tablet-based applications to enhance and improve staff and facility efficiencies. We will provide ongoing training at **no cost** to ensure that the Division of Canteen Services, DOC personnel, and residents benefit from all of Securus' industry-leading technologies and products.

Patented Technology – We are a leading technology innovator in the offender communications. We have developed and currently own over 285 patents focused on bettering the lives of offenders and staff.

Unmatched Service and Support – We understand that service is one of the most critical differentiators in the offender communications industry. We have more full-time field service technicians than any other offender technology provider, and our commitment to customer service is genuine. We focus on what we do, enabling the DOC to focus on what you do – protect and serve your community.

Over the past 30 years, we have fine-tuned our equipment, technology, support, and service for prisons and law enforcement agencies of all sizes. Our partners' needs have always guided our direction, leading us to provide impactful technology.

As Chief Growth Officer of Securus Technologies, I am authorized to contractually commit Securus to the terms of this proposal and any resulting contract. Please do not hesitate to contact me with any additional questions, or to request supporting information. You may contact me by telephone at (972) 277-0300, or by email at rroberts@securustechnologies.com.

Thank you again for the opportunity to provide this proposal. We look forward to working with the Division of Canteen Services to build a mutually beneficial partnership.

Sincerely,



Russell Roberts
Chief Growth Officer
Securus Technologies, LLC
4000 International Parkway

Carrollton, Texas 75007

rroberts@securustechnologies.com

EXECUTIVE SUMMARY



Executive Summary

Thank you for the opportunity to respond to the Colorado DOC ITN for Offender Communications.

We are proud to present our response to your ITN – a response that we hope you find meets and exceeds the needs of the Division of Canteen Services and DOC. Your ITN presents us with the opportunity to introduce new technologies and value-added services such as our new unified tablet program, voice biometrics and new investigative support services to assist your intelligence gathering. It also provides us with the opportunity to prove to you that Securus is a competent partner. Our proposal includes capabilities that will provide the Division of Canteen Services and DOC with requested capabilities such as offender tablets, secure e-messaging for offenders and new kiosks that are multi-functional and able to facilitate expanded offender self-help capabilities.

Proposal Strategy

Our strategy in providing this proposal has been to provide the latest in offender technology and investigative services, while also offering the CDOC with lowered calling rates. Services included in this ITN include:

- Offender Telephone System

- Video Connect Service
- Wireless Tablets
- Kiosks
- Investigative Tools
- Post-Incarceration Services
- Installation, Maintenance, Technical Support, and customer services

We have an experienced team of design and installation professionals who are dedicated to making the transition to Securus seamless.

Why Choose Securus?

We hope the ITN process will exemplify why the Division of Canteen Services and Colorado Department of Corrections should select Securus. We believe that a Division of Canteen Services and CDOC/Securus partnership makes sense for the following two reasons:

1. Securus presented a proposal that exceeds the requirement of the current ITN.
2. Securus presented a proposal that we feel will exceeds the offerings of all other vendors' proposals in the critical areas that are of the most importance to DOC.

Proposing Solutions That Exceed the ITN Requirements

The Securus proposal has carefully considered the specific requirements of the ITN and we have proposed technologies that meet and exceed the requirements. Not only have we included the technologies that meet your requirements; we have bundled in additional capabilities such as the ability to identify called party voices on recordings. In this way, we believe our proposal meets every requirement in the ITN and includes enhancements to CDOC investigative capabilities, which should exceed your expectations in every way.

We are constantly improving our service. We have experienced service technicians who are highly trained, certified in all aspects of our business, and are qualified to perform service on the technologies included in our proposal.

Consistent Account Management

We realize it is imperative that that we meet with you frequently and you can contact us anytime to discuss issues, concerns, or ideas. We understand your requirement for proactive, creative discussions with key departmental contacts so we can best design

and develop the technologies that you most need to run your facility efficiently and safely. Senior Account Executive, Daniel Furrer, will lead the team and will draw from his years of experience working with Departments of Corrections across the country.

Family Members and Friends Focus

Securus continues to focus on providing the industry's best service for the family members and friends of offenders. We continue to increase the number of associates serving offenders' loved ones from our state-of-the-art customer care center based in Dallas, Texas. In-house Securus associates are available to assist family members and friends of offenders 24 hours a day, 7 days a week, 365 day a year.

Televerde

Since October 2020, Securus Technologies has partnered with Televerde to provide incarcerated women opportunities in the customer service industry. Televerde has been working with state level correctional industry agencies since 1994 and has current operations at agency facilities in Arizona, Indiana and Florida where incarcerated women provide service support from contact centers. As part of the partnership between Securus and Televerde, Securus would work with Televerde and the state of Colorado to review a potential expansion project to establish a contact center model at a female Colorado DOC agency facility similar to the Arizona, Indiana, and Florida models aforementioned. All of these programs are independently managed by each state correctional industries agency. Specific to the Indiana Correctional Industries, Televerde participates in an additional program with the Department of Labor apprenticeship program to build workforce development programs with private sector industries. In addition to working with correctional industries with incarcerated women, Televerde also currently employs over 120 ex-offenders within their organization; and provides job training, transitional assistance and job placement through the Televerde Foundation (a non-profit founded by Televerde) opportunities for both pre and post release individuals associated with the Televerde programs and has proven, validated results of reducing recidivism rates for the population participating in their programs.

Securus appreciates the opportunity to earn your business. As you review our proposal and evaluate the information we have provided, remember these commitments we make to the State of Colorado:

- Educational Opportunities
  - Securus will provide the Division of Canteen Services and CDOC with the most-widely-used offender education platform (Learning Management System) today

    - Securus will provide the Division of Canteen Services and CDOC with continuing, innovative education advancement such as new courses and course sharing
- Delivery of Services
    - Securus will provide the Division of Canteen Services and CDOC with a proven, seamless transition process
    - Securus will provide the Division of Canteen Services and CDOC with frequent training opportunities
- Telecommunications Capabilities
    - Securus will provide the Division of Canteen Services and CDOC with the industry's best technology
    - Securus will provide the Division of Canteen Services and CDOC with innovation through continued investment
- Business Operations Capabilities
    - Securus will provide the Division of Canteen Services and CDOC with unsurpassed service and support
    - Securus will provide the Division of Canteen Services and CDOC with outstanding Family and Friends product and support

It is our goal to earn the business of the Division of Canteen Services and CDOC, your residents and their friends and family. Through good or bad times, we will always be there. You have been working with our subsidiary JPay for several years and the same reliable service and support you receive from them you can expect to receive for all of the additional products and services discussed in this submission. We want to be more than a vendor; we aim to be your trusted partner.

ATTACHMENT 1: STATEMENT OF WORK (SOW)

1. BACKGROUND

Within the Colorado Department of Corrections, there are currently 20 state and two (2) privately- owned facilities with a total capacity of 16,339 Offender. The Department currently provides offender communications through the use of telephones, tablets, video visitation kiosks and TTY. With regard to the tablets, currently the tablets not only provide a communication medium but also provide entertainment options such as music, games and movies. The funds that are used for these services come from Offender's personal trust fund accounts and/or offender families/friends and are not funded in part or in whole by the State. The current service provider supplies all hardware, infrastructure, software, technical support and maintenance for the system. The Department is looking for a more comprehensive approach to offender communication with exceptional customer service and reduced offender recidivism in mind.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

2. ACRONYMS AND DEFINITIONS

A. Acronyms

The list below provides acronyms and definitions critical to understanding this SOW. This list is not intended to be an all- inclusive list of acronyms or definitions for terms used throughout the SOW.

- **AC – Alternating Current**
- **ACM – Asbestos-containing material**
- **ADA – American with Disabilities Act**
- **AP – Access point**
- **API – Application Programming Interface**
- **AR – Administrative Regulation**
- **BIOS – Basic input/output system**
- **CD – Compact Disc**
- **CDOC – Colorado Department of Corrections**
- **CFR – Code of Federal Regulations**
- **CLEC – Competitive Local Exchange Carrier**
- **COB – Close of business**
- **CSV – Comma Separated Variable**
- **EOMIS – Electronic Offender Management Information System**
- **EPEAT – Electronic Product Environmental Assessment Tool**
- **FCC – Federal Communications Commission**
- **FM – Frequency modulation**
- **ID - Identification**
- **ITN – Invitation to Negotiate**
- **ITS – Inmate Telephone System**
- **KVM – Keyboard Video Mouse**
- **LAN – Local Area Network**
- **LEC – Local exchange carriers**
- **NEMA – National Electrical Manufacturers Association**
- **OCS – Offender Communication System**

- **OIT – Office of Information Technology**
- **OS – Operating System**
- **PC - Personal Computer**
- **PIN – Personal Identification Number**
- **PREA – Prison Rape Elimination Act**
- **QCP – Quality Control Plan**
- **STG – Security Threat Group**
- **TDD – Telephone Devices for the Deaf**
- **TTY – Teletype**
- **UCC – Uniform Commercial Code**
- **UL – Underwriters Laboratory**
- **UPS- Uninterruptible Power Supply**
- **VRS – Video Relay Service**
- **WPA-PSK – Wi-Fi Protected Access – Pre-Shared Key**
- **XML – Extensible Markup Language**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. Additional Definitions

i. AR – CDOC Administrative Regulation

ii. Data Sharing Agreements – a formal Contract that details what data is being Shared and appropriate use for the data.

iii. Deliverable – a unit or increment of work required to be completed and delivered under the Contract terms, including such items as goods, services, reports or documents.

iv. Offender– a member of the CDOC inmate population (including YOS).

v. Transition – the expectations that encompass all the task the incoming Offeror is expected to perform to assume all aspects of the requirement from the predecessor.

vi. Offeror – the entity selected to provide services as the Contractor.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

CDOC FACILITY DEMOGRAPHICS

A. List of Facilities:

The Colorado State facilities to be served as follows:

FACILITIES	LOCATION
PUBLIC FACILITIES	
Arkansas Valley Correctional Facility	Crowley, CO
Arrowhead Correctional Facility	Canon City, CO
Buena Vista Correctional Facility	Buena Vista, CO
Centennial Correctional Facility	Canon City, CO
Colorado Correctional Center	Golden, CO

Colorado State Penitentiary	Canon City, CO
Colorado Territorial Correctional Facility	Canon City, CO
Delta Correctional Center	Delta, CO
Denver Reception and Diagnostic Center	Denver, CO
Denver Women's Correctional Facility	Denver, CO
Four Mile Correctional Center	Canon City, CO
Fremont Correctional Facility	Canon City, CO
La Vista Correctional Facility (women's facility)	Pueblo, CO
Limon Correctional Facility	Limon, CO
Rifle Correctional Center	Rifle, CO
San Carlos Correctional Facility	Pueblo, CO
Skyline Correctional Center	Canon City, CO
Sterling Correctional Facility	Sterling, CO
Trinidad Correctional Facility	Trinidad, CO
Youthful Offender System	Pueblo, CO
CONTRACT FACILITIES	
Bent County Correctional Facility	Las Animas, CO
Crowley County Correctional Facility	Olney Springs, CO

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. Additions or Subtractions:

Additional contract facilities housing CDOC offenders maybe added or subtracted and would then require services during the time of the Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

3. GENERAL EXPECTATIONS

A. Background, Consent to Search:

The Offeror and any employee(s) of the Offeror who will be providing services on CDOC property may be required to undergo a CDOC criminal background check, and may be required to sign a "Consent to Search Authorization" form. Admittance of any persons to CDOC facilities or properties will be at the sole discretion of the CDOC.

i. Background check approvals for site visits are required. For security reasons, each form must be signed and returned for each vendor's employee who will be attending the site visit and performing any Contract at both CDOC and privately- owned facilities. The Offeror is expected to complete the following documents:

a. Consent to Search Authorization and Registration,

b. Certification of COVID-19 Vaccination, and return the completed forms to the requesting CDOC personnel. Because of space considerations, each site visit will be limited to two people per vendor.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will submit all required documents as instructed.

ii. Upon Contract award, and at least seven (7) days prior to beginning work, the awarded Offeror will submit the following completed documents:

a. CDOC Consent to Search,

b. Certification of COVID-19 Vaccination and Registration for each vendor employee who will be working on this project (unless previously cleared for the Site Visit).

- **Completed forms must be sent to the designated project manager designated by the CDOC.**
- **Forms are provided as attachments to the ITN, Attachment 9 and Attachment 10.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Forms will be completed and submitted to the CDOC as required.

B. Security

i. All Offeror employees entering prison grounds will adhere to the Department Security Regulations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All Securus personnel reporting to the CDOC facilities will adhere to the Department's security regulations.

ii. Any potential Offerors who are in non-compliance with the expectations of the Security Regulations will not be allowed access to the facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands that personnel will be required to comply with all security regulations, or they will not be allowed access to the facility.

iii. The Offeror is expected to ensure that, while at the facility, offenders do not have access to telecommunication devices in accordance with State Statutes, Rules and Regulations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will follow all DCOC regulations and state statutes in regard to telecommunications devices.

iv. Approved Offeror and Offeror staff shall be subject to search of person or vehicle at any time while on any CDOC facility, and grounds. Any search conducted shall be at the discretion of CDOC security personnel, and does not require probable cause.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands that on-site personnel will be subject to searches by authorized CDOC security personnel.

v. In the event of a facility disturbance or event, CDOC may temporarily detain the entry, and exit of all traffic from the facility. All reasonable efforts shall be made to release the Offeror or Offeror staff as quickly as possible while maintaining the security of the CDOC facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands that in the event of a facility disturbance or event, CDOC may temporarily detain the entry and exit of all traffic from the facility. Securus understands that all reasonable efforts shall be made to release the Offeror or Offeror staff as quickly as possible while maintaining the security of the CDOC facility.

vi. Offeror and Offeror employees are prohibited from using, possessing, or introducing tobacco, tobacco related products, tobacco substitutes, vaping products or e-cigarettes within CDOC facilities in accordance with C.R.S. 18-8- 204.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will abstain from the introduction or use of tobacco, tobacco related products, tobacco substitutes, vaping products, or e-cigarettes within CDOC facilities in accordance with C.R.S. 18-8- 204.

vii. In the event of a hostage situation, CDOC will not negotiate with an offender or any other person to secure the release of any individual, including the Offeror or Offerors

staff. The Offeror will notify all of its employees of this policy prior to entering any CDOC Facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understand this policy and will communicate it to all our employees of this policy prior to them entering any CDOC facility.

viii. Offeror(s) recognize and shall advice their staff that correctional facilities present an inherently dangerous environment, in part due to the presence of offenders, many of whom have been convicted of having performed violent crimes.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. Training for Offeror and Offeror staff

i. Offeror and Offeror staff will complete CDOC's on-line training program required for all contract workers.

ii. Prior to start date Offeror and Offeror staff will have completed all training required.

iii. Annual refresher training is required every twelve (12) months.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will complete required CDOC training as required in fulfillment of the contract resulting from this ITN.

4. WORK AREA PREPARATION

A. Prior to commencement of work, the awarded Offeror will ensure that:

i. Arrangements have been made for any disposal of waste materials per Scope of Work;

ii. All tools, equipment and materials are on hand; and

iii. Any applicable worker training has been completed and documentation is required on site.

iv. Jobsites is expected to be cleaned every day.

v. The Offeror will ensure that any and all equipment that is taken out of service is removed and disposed of at the Offerors expense.

vi. Once the awarded Offeror(s) has possession of the equipment to be installed, the responsibility for all equipment, including storage during installation work, will be at the awarded Offerors expense when storage space is unavailable at the jobsite.

vii. Work will be performed in accordance with manufactures' recommendations and with all current local codes, regulations, and installation guidelines.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will ensure that all items detailed above are professionally completed and that all site-related issues defined here are completed to the complete satisfaction of CDOC personnel.

B. Asbestos

i. Asbestos may be present within State-owned facilities, and may be encountered in previously inspected buildings.

ii. Any discovery of asbestos must be reported to the CDOC facility.

iii. All remediation work must be performed by a Offeror specifically licensed and/or certified to perform asbestos remediation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands the need to watch for asbestos and that, if any is located, remediation work must be done be someone licensed and/or certified to do asbestos remediation.

C. Securing of tools

i. Offeror to adhere to all CDOC policies and procedures regarding tools control. 0300_09_04152021.pdf

a. Offerors responsibility to ensure incarcerated individuals do not have access to any tools or equipment brought in by Offeror and subcontractor(s) if applicable.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will adhere to all CDOC policies and procedures regarding tools control and accept responsibility to ensure incarcerated individuals do not have access to any tools or equipment brought in by Offeror and subcontractor(s) if applicable.

D. Health and Safety Standards

i. The awarded Offeror(s) will comply with all applicable federal, state and local expectations for protecting the safety of the Offerors employees, building occupants, and the environment.

ii. The awarded Offeror(s) will be expected to comply with all Federal, State and Local rules and regulations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

If awarded the contract, Securus will comply with all federal, state, and local expectations for protecting the safety of Offenders, employees, building occupants, and the environment. Securus will comply with all Federal, State and Local rules and regulations.

5. OFFEROR EXPECTATIONS

A. Offeror Expectations

i. The Offeror will have direct oversight, be responsible for and monitor the performance of all Offerors staff performing services under the Contract. The authorized

CDOC staff will provide security for the Offerors employees and agents consistent with the security provided at all CDOC facilities.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will have direct oversight, be responsible for and monitor the performance of all Offerors staff performing services under the Contract. The authorized CDOC staff will provide security for the Offerors employees and agents consistent with the security provided at all CDOC facilities.

ii. The Offeror will designate a single point of contact to be the liaison for state information technology staff to handle day-to-day operations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The single point of contact is:

Daniel Furrer, Senior Account Executive
Daniel.Furrer@securustechnologies.com
786-246-7761

iii. The Offeror will identify and define their key full-time positions supporting the CDOC inmate Telephone Systems (ITS).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Proposed Project Team	
Name	**Qualifications/Responsibility**
Daniel Furrer, **Senior Account Executive**	Daniel has 6 years of communications experience with JPay and Securus. He will work alongside Michele Paige and the rest of the CDOC Project Team to ensure a hundred percent customer satisfaction during the installation and throughout the duration of the contract. Daniel works with 13 DOCs around the country and brings substantial background into theCDOCenvironment.
Steve Viefhaus, **Vice President, Sales**	Steve has more than 39 years of communications experience with Securus, MCI and Verizon. He will work with the CDOC project team to ensure the project is implemented on time and answer any questions the State may have.
Josh Conklin, **Sales Vice President**	Joshua (Josh) Conklin is Vice President of Sales at Securus Technologies, LLC with more than 13 years of communications experience. Josh will work with Steven and CDOC to ensure that the project is completed on time and

	above expectations, answering any key questions that may come up during installation. Before joining Securus, Mr. Conklin served as Senior Vice President and General Manager of California and Nevada for Integra Telecom, a privately owned, facilities-based, integrated communications carrier and equipment provider headquartered in Portland, Oregon.
Michele Paige, **Senior Account Manager**	Michele is a results-oriented manager with over 25 of experience working in the public and private sectors. Extensive experience in customer service, account management, sales, event planning, team building and public relations. Expert manager of people and resources, easily develop rapport with people of diverse backgrounds and experiences. She has served as account executive for the largest correctional facility accounts with more than 200,000 customers. Michele has effectively developed and implemented innovative tracking and customer satisfaction programs to meet customer's needs.
David Bensmihen, **Sales Engineer**	David has supported offender systems and correctional facility accounts for more than 10+ years. He will provide assistance throughout the installation.
Nestor Nunez, **Sr. Manager, Implementation Project Manager**	Nestor has experience managing multiple projects and delivering results on time and within budget. He will oversee the CDOC installation from initiation to completion and will be the first-line escalation during implementation.
Johnny Hagins, **Director, Operations**	Johnny has more than 23 years of experience in the telecommunications industry. His current management responsibilities include overseeing all managers, field technicians and field site administrators who service and maintain state DOCs, county jails, and other private prisons and jails in the Eastern Region of the United States.
Jonathan Jones **Regional Manager, Field Services**	Jonathan brings more than 20 years of progressive experience and accomplishments in technical and service delivery environments requiring strong leadership, IT/telecommunications, communication, and customer support skills. He is a strategic and proactive leader with a proven track record of managing people, resources, processes, and technologies to meet business objectives, customer goals, and revenue and profit goals

Jerimy Thompson Regional Manager, Field Services	Jerimy has direct Supervision of Installs encompassing 17 States to includeCDOCFacilities and County Jails. He managers Day to Day functions and scheduling of all major installs in the Western Region. Jerimy works hand and hand with facilities to meet timeframes and schedules that fully benefit the customer.
David Brannan, Manager, Field Services	David has 16 years of experience in the Telecom Industry, including 10 years of this experience as a Field Operations Senior Manager. He is experienced in managing time-critical projects, delivery of our services across cross functional teams, and experience in managing high profile and large-scale deployments across the continental United States, Canada, Mexico and the U.S. Virgin Islands. David is proficient in Microsoft Word, Excel, Visio, and Wrike. I am also skilled in Project Management, RF Network Design, Structured Cabling design, Planning and deployment, as well as RF Network Deployment and Testing.
Tony Westbrook, Field Service Technician	Tony will serve as the lead technician for the planned installation at CDOC.
Chris Pair, Field Service Technician	Chris will serve as back up to the assigned onsite technician and provide additional support during implementation as needed.
Trevor Lipscomb, Field Service Technician	Trevor will serve as back up to the assigned onsite technician and provide additional support during implementation as needed
David McTee, Instructor, Customer Training & Product Adoption	David brings more than 35 years of professional training experience. He will provide CDOC staff with the knowledge and skills needed to efficiently administer the system.

iv. The Offeror will be responsible for all expenses incurred for travel, including transportation, and meals incurred on behalf of Offerors staff positions.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will be responsible for all expenses of staff provided in fulfillment of the resulting contract—including expenses tied to transportation, means, and lodging.

v. Additionally, the Offerors staff will liaise with and maintain a good working relationship with CDOC staff and other providers working with the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has extensive experience installing and maintaining offender telecommunications systems and has developed installation and cut-over procedures that minimize disruptions and errors and maximize customer satisfaction. Securus has developed a preliminary implementation plan that includes all of the required components.

Implementation Plan

Securus has a proven track record of providing successful turnkey installations for mega-county, county, and city agencies, as well as large state department of corrections agencies. Over the last several years, our team has completed more than 2,800 quality installations of our calling service and has averaged a 4.6 (out of 5) customer satisfaction rating every year.

Recent customer testimonials include:

"I could not be more pleased with the quality and professionalism of the SECURUS personnel associated with the installation of our inmate telephone system."

- Captain John Donegan – Suffolk County Jail, Riverhead, NY

"The Securus installation team is the most professional group of people that I have ever had the pleasure of working with on this type of project. Their attention to detail and dedication to customer satisfaction allowed them to complete a statewide, multi-location installation well under the projected completion date with virtually no unforeseen problems. I would love to work with them on another project."

-- Karl Prince, IT Manager, Louisiana DOC

The Securus Project Team consistently demonstrates project management expertise that simply cannot be matched by any other service provider. We look forward to the opportunity to provide the CDOC with industry-leading project support and services.

Project Description

The CDOC implementation project includes a complete, turnkey installation of all equipment, facilities, and connectivity for offender telecommunications services.

Project Plan Overview

The project plan identifies the deployment of specific technologies under a phased-in schedule that delivers efficiencies where the CDOC needs efficiencies first. Securus proposes a preliminary implementation plan that transitions all offender telecommunications services to conform to contractually agreed deadlines. This includes complete, turn-key installation of all hardware, software, and configurations for the offender telecommunications system.

The project begins with Securus representatives on-site at a designated CDOC location to kick-off our implementation plan within days of contract execution.

Degree of Involvement from CDOC

Securus makes every effort to limit the administrative burden that can occur during a transition of service providers. We have experience installing our system at more than 2,800 customer locations. This level of experience ensures that we do not waste any of your time.

At the beginning of the project, the Securus Project Team will meet with the CDOC team on site at a CDOC location. These well-organized meetings introduce project team members and review the project plan and timetables with the CDOC team in person to ensure a successful project kick-off.

Our project managers work with the CDOC team to coordinate equipment deliveries and facility access. When Securus technicians arrive on site, they may require escorts to the phone/terminal and equipment locations. Most of the project activity will occur during normal business hours. However, Securus can accommodate late-night/overnight cut-over activities. Some customers choose this method to eliminate service interruptions.

After each facility transitions to our NextGen Secure Communications Platform™ (NextGen SCP™), our project manager and field service technician review our quality checklists with the CDOC team.

The Securus project team hosts weekly stakeholder meetings with participation from the CDOC team.

At the beginning of the implementation project, the Securus project management team will work with the CDOC team to identify key stakeholders and primary points of contact. The team defines roles and responsibilities for the duration of the project.

The Securus project management team will establish regular meeting forums and communication protocols that accommodate the requirements of the CDOC team.

Throughout the project, our project management team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

In addition to the personal communication from our project managers, Securus can set-up automated email notifications for the CDOC team. The automated email notifications the communication of updates and status changes for major milestones and other tasks.

vi. The Offeror is expected to guarantee all equipment is compatible to the best industrial standards and functions as designed after installation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All Securus equipment used will be compatible to the best industrial standards and functions as designed after installation

vii. The Offeror is expected to guarantee workmanship at Offerors expense for a period of twelve (12) months from the date of installation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide maintenance, repairs, service, and replacement throughout the life of the contract.

viii. The awarded Offeror(s) may be required to do some work after normal business hours (8am-5pm, unless otherwise specified by CDOC); however, it is anticipated that most work will be completed during normal business hours.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands some work could be required after normal business hours, but the expectation is that most work will be completed during normal business hours.

B. Escalation Procedures During Repair Service

i. The Offeror will provide escalation procedures to address inadequate response to service calls, frequent repetition of the same service problem, inadequate repairs to ITS, etc. These described procedures will include the name and title of service and

management personnel as well as criteria for service escalation to a certain "level" within the Offerors organization.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus' Technical Support Center (TSC) serves as a single point of contact for facility staff to request service or make inquiries for all Securus products **24 hours a day, 7 days a week, 365 days per year** and has three convenient methods of contact:

- Telephone: 866-558-2323
- Email: technicalsupport@securustech.net
- Fax: 800-368-3168

The TSC uses a call distribution system to automatically manage the flow of inbound customer calls, routing calls directly to our support technicians in a skills based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request.

Upon contact from a facility, each service request is assigned one of three initial priority levels, each with its own resolution and escalation timelines. Every effort is made to resolve the problem remotely within the designated timeframes and many service requests can be resolved during the initial request. If the service request cannot be resolved remotely, a field service technician is dispatched to the facility to expedite resolution.

The TSC uses an event tracking system that logs, tracks, manages, and assures appropriate response to all service requests. The service request generates a trouble ticket with priority level assignment which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem and either resolves the problem or engages the appropriate party for problem resolution. The TSC retains ownership of all service requests and is responsible for the escalation and update functions.

Securus has had more than 230 patents issued and another 100 pending patent applications, all of which are supported by our TSC. No competitor can match Securus' TSC experience in working with corrections officials to quickly resolve and manage calling programs. Securus' experience and technology allows us to create and manage calling programs for corrections facilities that put top priority on providing safety and security to the public.

Service Levels

When a facility calls Securus, an event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific

system events and has a prescribed resolution timeline and escalation procedure. In all cases, Technical Support will respond to the customer within the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects 30 percent or more of system functionality. Examples of P1 service assignments include:

- Voice prompts not operating
- Features are not operating appropriately
- CD-burning abilities disabled
- Live call monitoring is not operating appropriately
- NextGen SCP access denied
- All phones out-of-service

The response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

A P1 events escalate to:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If the problem resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment—our mid-level priority assignment—occurs when a system event adversely affects 5 to 29 percent of system functionality. Examples of a P2 service assignment include problems or errors with related to:

- Workstation
- Specific system ports
- Local Exchange Carrier (LEC) circuits
- Unblocks

- Blocked numbers
- Missing call detail records (CDRs)
- Call searching

The response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival. P2 events escalate to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment—our lowest priority assignment—occurs when a system event adversely affects 5 percent or less of system functionality. System events adversely affecting some of available facility phones. Examples of P3 service assignments include:

- Static on the phone
- A party's inability to hear
- An offender's inability to dial
- A broken phone
- Non-functioning dial pad
- Non-functioning cutoff switches
- An inability to generate reports

The response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival. P3 events escalate to the Technical Support Department.

Escalations

If response is delayed, escalation procedures within Securus' Management Team are activated to resolve the service request.

Below are the names of people responsible for escalated issues.

Name	Position/Authority	Contact Information
Bobby Folsom	Technical Support Manager, 1st Line of Escalation	214-775-4936 bfolsom@securustechnologies.com

Dan McNally	Field Services Manager, 1st Line of Escalation	469-235-9884 dmcnally@securustechnologies.com
Ian Jones	Sr. Director, Operations (Tech Support), 2nd Line of Escalation	972-277- 0456 ijones@securustechnologies.com
Pat Robertson	Director, Operations (field), 2nd Line of Escalation	502-432-5924 probertson@securustechnologies.com
Aaron Bacher	Sr. Director, Operations (field), 2nd Line of Escalation	716-307-1300 abacher@securustechnologies.com
Matt Pareti	Chief Operating Officer – Final Line of Escalation	972-277-0300 mpareti@securustechnologies.com

ii. Updated contact names and telephone numbers of the service and management positions listed/described in the escalation procedures will be made available to the authorized CDOC staff immediately upon request.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Throughout the life of the contract, Securus will ensure that contact names and numbers will be kept current as required.

iii. Provide for an external audit of services on an annual basis by an independent auditing firm verifying the Offerors timing and billing systems are accurate and capture all calls. Selection of the independent auditing firm will be subject to CDOC approval. The staff that performs the audit will be subject to background checks in advance of entering CDOC facilities.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide for an external audit of services on an annual basis by an independent auditing firm—subject to CDOC approval—verifying Securus' timing and billing systems are accurate, and that they capture all calls.

Sarbanes-Oxley Compliance

Securus access controls for all systems are internally audited for compliance with The Sarbanes–Oxley Act of 2002 (SOX), which set new or enhanced standards for all U.S. public company boards, management, and public accounting firms. These widely recognized distinctions confirm that the company has effective controls and safeguards in place to manage its financial matters. This internal audit ensures the CDOC will get accurate and timely reporting of all financial transactions.

iv. Offeror is expected to include proposed escalation procedures with their proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Please see item B.i., immediately above.

6. WARRANTY INFORMATION

A. Offeror to provide all warranty information to CDOC for all goods and services.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus assumes all responsibility for repair and replacement of all equipment for the life of the contract, with the exception of tablets, which come with a one-year warranty against physical defects. This however, does not cover intentional damage, and Securus will work with the State on a policy to replace intentionally damaged equipment at the expense of the individual who damaged said equipment.

B. CDOC prefers equipment to have a minimum one (1) year warranty that it is free from defects in material and workmanship. If defects are identified, the successful Offeror agrees to repair or replace defective parts promptly on a like-for-like basis without additional cost to the CDOC. Any and all items failing during the warranty period will be replaced promptly free of charge. Significant failure will be determined by the Contract Monitor. The Offeror will be responsible for all equipment throughout the duration of the contract regardless of manufacturer's warranty.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All the equipment that Securus is proposing is corrections-grade hardware and backed by standard manufacturers' warranties. Securus will coordinate and facilitate all warranty claims and services. Notwithstanding these warranties, Securus will repair, replace, and update all equipment and software during the contract to maintain efficient operation of all systems at no cost to the CDOC.

7. DOCUMENTATION

The awarded Offeror will provide to the CDOC detailed technical system documentation, detailed system design specifications, descriptions of all proposed kiosk/tablet hardware and software, operating instructions, footprints, power and environmental requirement, model numbers, makes, serial numbers, electrical and grounding expectations, temperature and humidity ranges, software components and features, etc.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All stipulated documentation will be provided to the CDOC upon execution of the contract.

8. INTERFACE, TECHNICAL, SECURITY FOR ALL DATA

The following information along with additional information needs to be included in a data sharing agreement to be completed after award of contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Attachment No. 7, Data Sharing Agreement Template, will be completed after award of contract.

9. QUALITY ASSURANCE PROGRAM

The Offeror is responsible for developing and monitoring quality metrics and implementing corrective action plans for any variance. CDOC anticipates the metrics will be included in the Offerors Quality Control Plan. This required and non-negotiable.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

A. Quality Control Plan

Offeror must draft a Quality Control Plan for the contract to address the following seven key items below which are negotiable:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus continually enhances quality to maximize customer satisfaction. We do this through a comprehensive approach that includes our culture, our employee selection process, measurements and feedback, system and process design, and internal controls.

Our Culture

At Securus, we believe a commitment to quality starts with culture. Securus has developed a culture of measurement and continuous improvement. Each Securus department measures and reports customer satisfaction and performance toward quality objectives. Internal teams review and analyze the results, and action items and initiatives are created to improve on results. Each quarter the company recognizes employees and work teams that have achieved outstanding results in the areas of teamwork, quality, innovation, and customer satisfaction.

Employee Selection

Having a quality-oriented culture is vital, but employees committed to our values and performing at the highest level is what sets us apart. Securus uses a formal process for employee selection that involves multiple departments and management levels. An in-house recruiter seeks out top candidates for open positions. Screenings ensure candidates match the requirements for positions and background checks ensure we only hire candidates with the highest integrity standards. Our formal processes ensure only the top candidates are selected.

Measurement and Feedback Systems

An important foundation of our quality focus is our measurement system. Securus uses a variety of quantitative and qualitative information gathering tools to solicit feedback from customers in our quality improvement process. These tools include:

- **Transactional Surveys** – We survey customers after key events (e.g. installations, adds, moves, changes, repairs) to gather information on performance. Respondents rate their experience through 21 questions. A low rating (a 1 or 2 on a 5 point scale) on any single question requires a management review, immediate contact with the customer, and an action plan for improvement.
- **Relationship Survey** – We survey our customers periodically to understand if we are meeting their expectations. This survey specifically evaluates the performance of our customer operations and account management teams. Again, we ask 21 questions, and a low rating requires a management review, immediate contact with the customer, and an action plan for improvement.
- **User Groups** – Securus periodically sponsors user groups inviting customers to discuss their ideas and future development of our products and platforms. Operational and security challenges customers brought to Securus are at the heart of many of our patented innovations.

These feedback mechanisms provide invaluable information and help Securus meet our customers' expectations.

System and Platform Design

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Software Development

The Securus use of information technology (IT) best practices, industry standard quality measurement tools, and strict environmental controls, ensure the highest system functionality and availability. The Securus development team uses the Waterfall Software Development Lifecycle (SDLC) to ensure high-quality deliverables. The feature/functionality enhancements process stages are:

- Analysis
- Design
- Development
- Quality Assurance
- Implementation
- Post Implementation Support

Each phase has specific deliverables and gates (controls) to ensure high quality and to minimize rework. Securus uses the following distinct system environments in conjunction with our SDLC:

- Development – Used by IT Development to create and unit test new enhancements
- Quality Assurance – Used by Quality Assurance Analysts to test and certify new enhancements and bug fixes
- Pre-Production – Used by Production Support to validate hot fixes for production, and for final validation and mock deployment of major functionality releases
- Production – Used by all Securus customers and accessible by only Securus Production Support and Tech Support

Each environment has access controls, and we use source code control systems to ensure the proper promotion of code and as a document repository.

Securus uses industry-standard HP Quality Center for defect tracking and follows a rigorous test cycle including:

- Verification of New Functionality – Ensures a feature is working as designed
- Load Testing – Determines the upper threshold or breaking point of the component or feature
- Performance Testing – Determines the expected user experience
- Regression Testing – Ensure all existing functionality still works as designed
- Exception Testing – Tests boundary conditions and unexpected usage scenarios

New releases typically create new functionality. Upon completion of the Quality Assurance stage, the code changes are packaged and deployed into our pre-production environment for the final end-to-end quality check, and to optimize the implementation. This effort enables Securus to minimize the maintenance window related to system changes.

Both IT and business stakeholders review and must approve all scheduled changes to production in two change control meetings to safeguard the stability of the production environment.

Upon implementation of new code into production, Securus Production Support, and IT Development monitor changes closely to minimize the impact of any adverse or unexpected system behavior.

This attention to detail allows Securus to build feature functionality that leads the industry in quality and performance. For example, the Securus three-way call detection feature has been proven to be more accurate than the same feature offered by competitors. Independent testing by an outside research and testing company proves it. Similarly, our voice biometric feature leads the industry in accuracy.

The voice quality available on our call platform provides near perfect fidelity. Customers have used information heard through background conversations to prevent and solve crimes.

Our quality control does not end with our system design but continues all the way through site installation. Securus and each customer develop a defined quality checklist to install the system in a manner that meets their unique operating requirements. As described and included with our installation plan, Securus uses quality control checkpoints for each phase of an installation:

- Quality Control Checkpoint 1 – Provisioning: After customer provisioning is complete, Securus technicians submit a quality control review to the Engineer, Project Manager, and Account Manager for the project.
- Quality Control Checkpoint 2 – Pre-Installation: While on-site, Securus Field Service Technicians complete a checklist to ensure that the physical installation characteristics meet or exceed Securus standards.
- Quality Control Checkpoint 3 – Equipment Testing/Functional Validation: Technicians complete test call scenarios and phone labels, call durations, on/off times, administrative terminals, and verify other customer configurations.
- Quality Control Checkpoint 4 – Acceptance: The Securus Project Team provides copies of all quality control documents, equipment inventory records, and network diagrams. The Securus Project Team will host a review of these documents with CDOC.

These tools are used to verify that work is completed properly before moving to the next step in a process. Customers must indicate their satisfaction with a sign off moving to the next step in a process.

Internal Controls

Finally, Securus has developed the best internal controls in the industry to make sure we follow our processes and that our information is accurate and ensure its security. Securus access controls for all systems are internally audited for compliance with the Sarbanes–Oxley Act of 2002 (SOX), which set new or enhanced standards for all U.S. public company boards, management, and public accounting firms. This internal audit ensures CDOC will get accurate and timely reporting from Securus.

Securus also employs an internal audit team that constantly reviews and audits our systems and security procedures and verifies our performance compared to our standards.

i. Documented standard operating processes and procedures for services provided to meet contract performance desirable.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

a. Describe the Offerors standard operating procedures and processes for performing SOW essential contract desirables for itself, as well as for subcontractor(s).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Based on years of experience and ongoing updates and revisions as needed, Securus has a comprehensive set of Standard Operating Procedures used to ensure compliance to requirements, consistency in processes, cost containment, and accountability.

In the contract process, Securus will work with authorized CDOC personnel to ensure all items required are defined in the contract and that deliverables and quality and performance metrics are built into our processes.

Our Standard Operating Procedures include, but are not limited to:

- Definitions of processes, services, and products
- Prerequisites in software, hardware, and capacity
- Project summaries to ensure uniform understanding
- Identification of departments and roles who will be critical to meeting the requirements
- Step by step descriptions of processes and materials
- Review and status checkpoints
- Checklists to verify full completion and compliance.

b. Describe the Offerors standard operating procedures and processes for ensuring that data reported are:

- **Confidential: All findings will be treated as confidential,**
- **Accurate: The data is correct,**
- **Reliable: The methods by which data is collected and analyzed remain stable over time.**
- **Complete: The data does not have missing values or missing data records,**
- **Timely: The data is up to date,**
- **Consistent: The data has the expected format and can be cross referenced with the same results.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As described above, Securus Standard Operating Procedures (SOP) are used to ensure we meet all schedule and contractual requirements. Where required, Securus SOPs will be adapted to ensure all contractual obligations area met.

These SOPs will ensure that data reported are defined and measurable to meet CDOC requirements as stipulated in this requirement:

- **Confidential**: All findings will be treated as confidential,
- **Accurate**: The data is correct,
- **Reliable**: The methods by which data is collected and analyzed remain stable over time.
- **Complete**: The data does not have missing values or missing data records,
- **Timely**: The data is up to date,
- **Consistent**: The data has the expected format and can be cross referenced with the same results .

Our SOPs ensure consistency, measurability, and accountability throughout the process with specific groups assigned to each activity throughout the duration of the contract.

Project Initiation Phase

Immediately after award, the Securus Project Management Team will host a meeting with the CDOC Team to review project scope, critical success factors, and the implementation timeline. During this face, SOPs will be amended to accommodate CDOC requirements to ensure all elements of the contract are defined and agreed to.

Project Execution Phase

During the Project Execution Phase, Securus Technicians will travel to each location and complete pre-installation activities in preparation for the product launch. The pre-installation activities include pre-wiring, hardware staging, and telecom test & turn-up activities as needed that can be done in advance to reduce the amount of time and complexity of the actual go live.

The Securus Team will perform a thorough inspection of the installation and will resolve any potential issues prior to finalizing the implementation. The technicians completing the installation activity will perform a walk-through with the CDOC Team to review all installation documentation and checklists. At this time, SOPs can be reviewed with the CDOC team to ensure all processes are in place to completely satisfy the contract requirements. The Securus Project Management Office will host a Customer Acceptance Review Meeting with the CDOC Team prior to finalizing the cut-over at each location.

Onsite training seminars as well as web-based training activities (if applicable) will occur during this phase of the project.

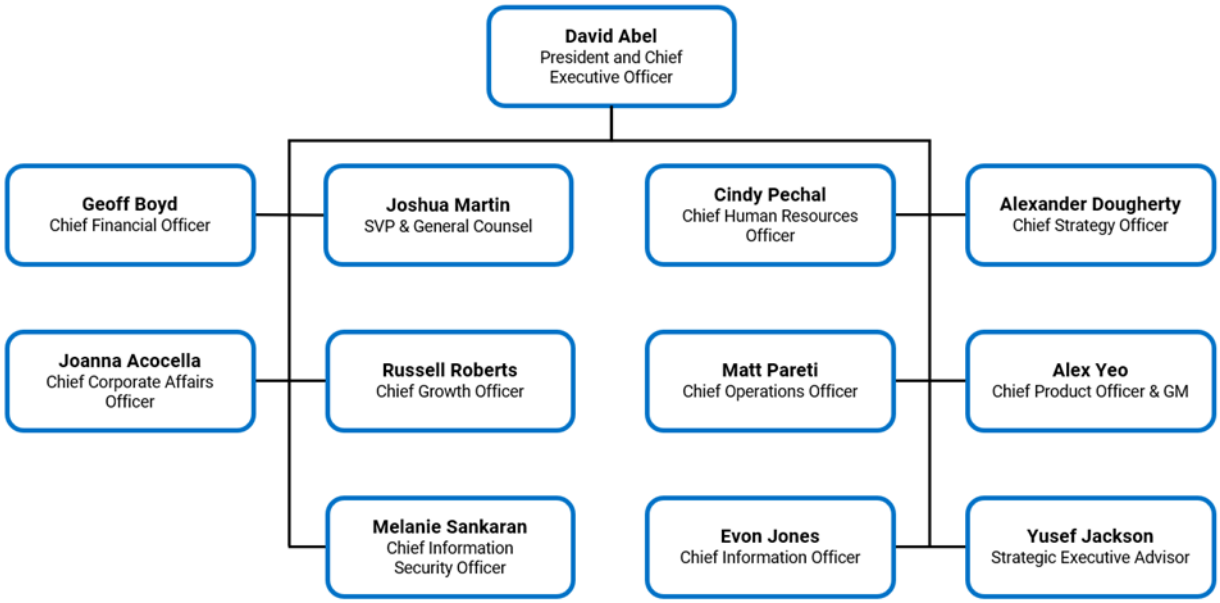
Project Monitoring/Controlling Phase

During the Project Monitoring/Controlling Phase, the Securus Project Management Office will focus on satisfying any outstanding action items. Additionally, the Securus Installation and Site Engineering Team will exercise daily diagnostic checks and monitoring protocols to ensure the recently installed equipment is working well and meeting the requirements of the CDOC.

The Securus Project Management Office will maintain frequent communication with the CDOC Team throughout the project implementation phases as identified within the SOPs and PMI best practices and methodologies.

c. Include a current corporate organization chart listing staff and operational business functions.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.



d. Documented change management program to ensure that correct processes and procedures are followed. Describe the Offerors change management program, processes, and procedures, and how its level of effort is determined for implementing Change Requests.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The version number is a unique identifier that always aligns with the software release build for a given deployment. A description of the change will vary based on the business requirements provided by the team requesting the change. For change initiations, back- end changes are primarily requested and initiated by our Account Management and Product teams but can also originate from within our IT Department, depending on the solution being implemented. This same process applies for the person requesting the change. Creation of the change is driven by our IT Department; the tactical deployment of the change, as well as the date and time of the change, is managed through our Network Operations Center (NOC).

e. Provide and maintain Offeror inspection and audit systems for services provided to meet contract performance desirables

- **Identify which area(s) on the Offeror's organization chart are responsible for inspecting products/services and which area(s) perform audit functions**
- **Describe what systems are used and how are they maintained**
- **Include a current risk assessment**
- **Describe the Offeror's internal audit, as well as external audit processes and procedures**
- **Describe the Contractor's procedures for auditing**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with authorized CDOC personnel to put in place inspection and audit systems for services provided to meet performance deliverables.

Audit & Activity Tracking Procedures

Log CDOC user activities for investigative purposes: The NextGen SCP™ audit and tracking feature can be accessed by specified site administrators only or by site personnel with authorized security credentials. NextGen SCP gives you 24x7x365 access to all systems including reporting functions, recordings, live call/video session monitoring, and all configuration settings.

Securus NextGen SCP Audit and Tracking Feature Logs Activity

- System access, such as user log in time and user activity duration
- Recording access, such as recording playback and associated user
- Communication activity
- Searches
- Webpage visits

- Data change, such as changes to personal allowed number (PAN) lists, custody accounts, global list entries, and security permissions

Securus uses Oracle for its database file structure. Oracle Database delivers economies of scale on easily managed grids, making it easier to:

- Reduce downtime with maximum availability
- Partition and compress data to run queries faster
- Securely protect and audit data, and enable total recall of data
- Make productive use of standby resources

Oracle simplifies the process of linking data in multiple tables. This is a key feature of a relational database management system or RDBMS. Storing data in multiple tables enables Securus to define relationships between the tables, as well as the applications that feed information to those tables.

Oracle allows NextGen SCP to link the call data to multiple tables and also maintains consistency between them, ensuring that the data among related tables is correctly matched to maintain referential integrity. Oracle supports all standard relational data types, as well as native storage of XML, Text, Documents, Images, Audio, Video and Location data. Access to data is via standard interfaces such as SQL, JDBC, SQLJ, ODBC, .NET, OLE, .NET, and ODP .NET, SQL/XML and Xquery and WebDAV.

Securus can use the Oracle database to respond faster to changing business conditions, providing clients a system that is more responsive to their evolving needs.

Data Reports

Authorized CDOCstaff can generate reports to spot trends through the NextGen SCP user interface. NextGen SCP™ retains communication detail records on all communication attempts and events. Authorized users can quickly run reports to spot calling trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

CDOC users can customize reports by changing search criteria such as date, time, offender identifier, dialed number (calls), visitor contact number (video visitation), destination, termination reason, and much more.

The following steps show the ease of producing valuable, customized reports:

1. Verify that the correct “Facility” and “Site” levels are selected or make changes as necessary. (This setting allows you to select the facilities, sites, phone groups, or phones you want to search.)

2. Click the **Explore** menu.
3. Select **Communication Records**. Also, CDOC users can select **Offender Activity**, **Covert Alerts**, **System Logs**, or **PAN Frequency** to generate reports within these categories.
4. Select the search criteria for a simple (dynamic) search or click the **Advanced Search** link to perform a more detailed search based on additional criteria.
6. Enter your search criteria in the appropriate fields and click **Search**.

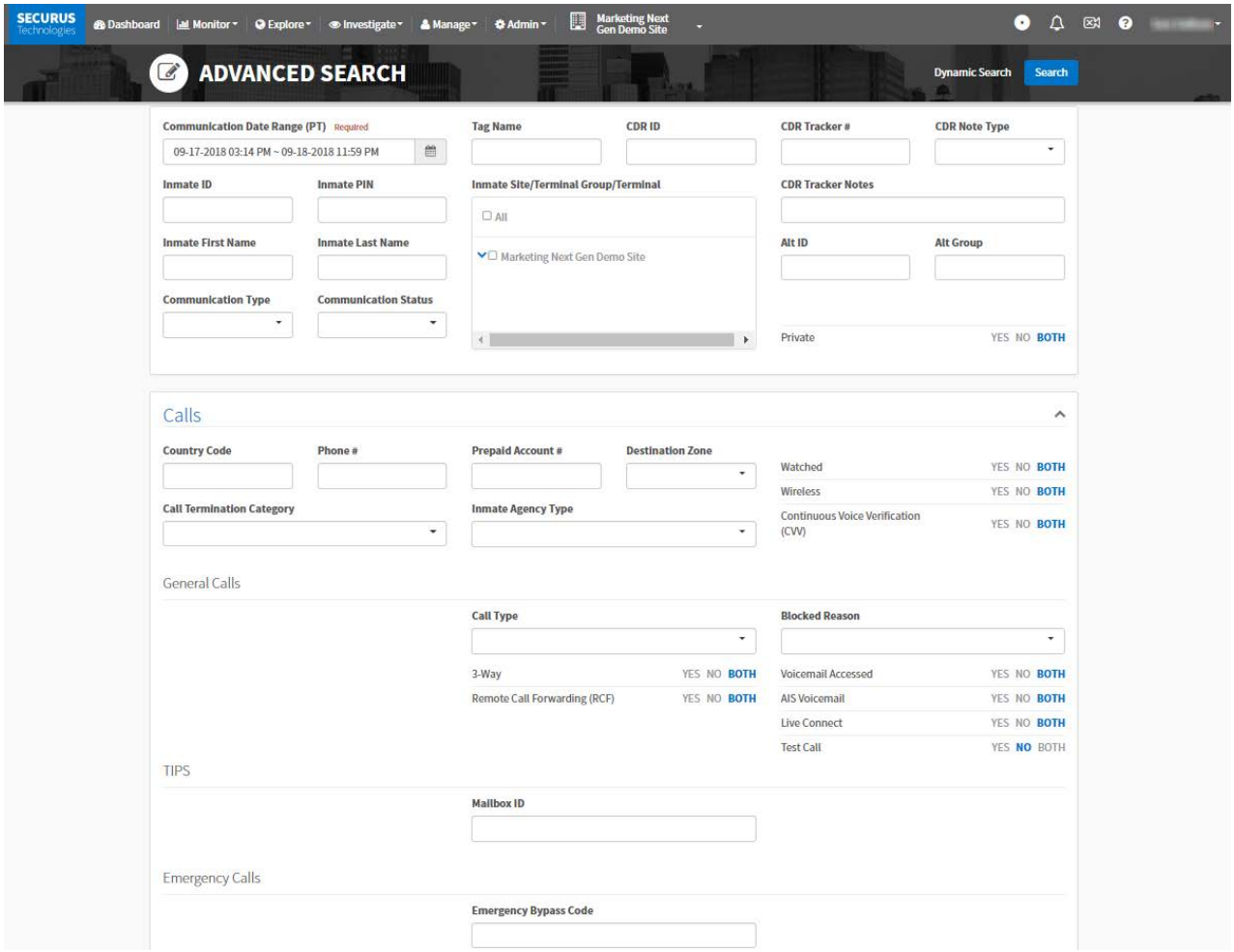
The records matching the search criteria appear. With a single click, the data can be exported to Excel, CSV (Comma Separated Values), or Adobe PDF format.

Authorized CDOC users can sort the results within the NextGen SCP user interface on the following criteria, while exporting a result to Excel allows the user to sort the results based on any of the communication event details.

- Offender Name (IS)
- Other Party
- Start Date/Time
- Duration

The resulting report can easily be saved, printed out, or emailed to others.

Advanced Search, Calls Section



Spotting Trends

Securus' THREADS platform can help CDOC staff identify trends that could pose a security threat to other offenders, staff, and facilities. Through Securus' data analytics platform— THREADS™—facility data is automatically ingested the moment THREADS is enabled.

Additional external data sources can be imported and analyzed to build an investigation. All of this takes place without purchasing any additional equipment, and it can be managed remotely at any time through an assigned Web-based facility portal. This means that the CDOC can access data remotely from any location that provides Internet access.

THREADS is the most widely used investigative telecommunications platform in the industry today, with more than 1.5 million offenders served, petabytes of aggregated

intelligence data, and more than 2 million phone calls processed per day. THREADS' powerful data analytics engine analyzes multiple types of facility data, such as offender communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate focused leads for investigators. THREADS is extremely robust and accurate, but is extremely intuitive, and easy to use —making it a perfect tool for busy investigative officers operating within a correctional institution.

Unlike our competitors' software, which requires users to manually upload facility data, THREADS was developed directly within the corrections market; it automatically uploads facility data and does not require any equipment to reside on-site. The unique algorithms within THREADS were designed by high-profile investigators with more than 50 years of combined experience in communications data and training of other investigative units on how to analyze that data. What used to take an entire day of multiple officers working eight-hour shifts now takes just moments.

THREADS Reports

THREADS provides the following types of reports:

- Statistical
- Linkage
- Working Group
- Correlation
- Time-Based
- Financial

Statistical Reports

Statistical analysis includes basic reports to start your investigation. This includes all occurrences of a phone number or a bounce list of numbers in the database and the most frequently called numbers by an offender or person.

- Identify everywhere a phone number occurs in the database, such as calls, SMS, phonebook, and BNA. This analysis can be run with a bounce list.
- Identify an offender as a potential owner of a device.
- Identify the phone numbers that an offender or person calls with the highest frequency.
- Identify all phone numbers associated with an offender or person including all calls, SMS, emails, and phonebook contacts. A bounce list can be generated from this report.

- Identify all communication details (calls, SMS and emails) between 2 or more targets or groups of targets. This report produces a CSV file for download.

Communication Activity Summary



Linkage Reports

Linkage analysis shows how offenders and people are related. All the reports in this section generate graphical results that let you explore the relationships between your targets.

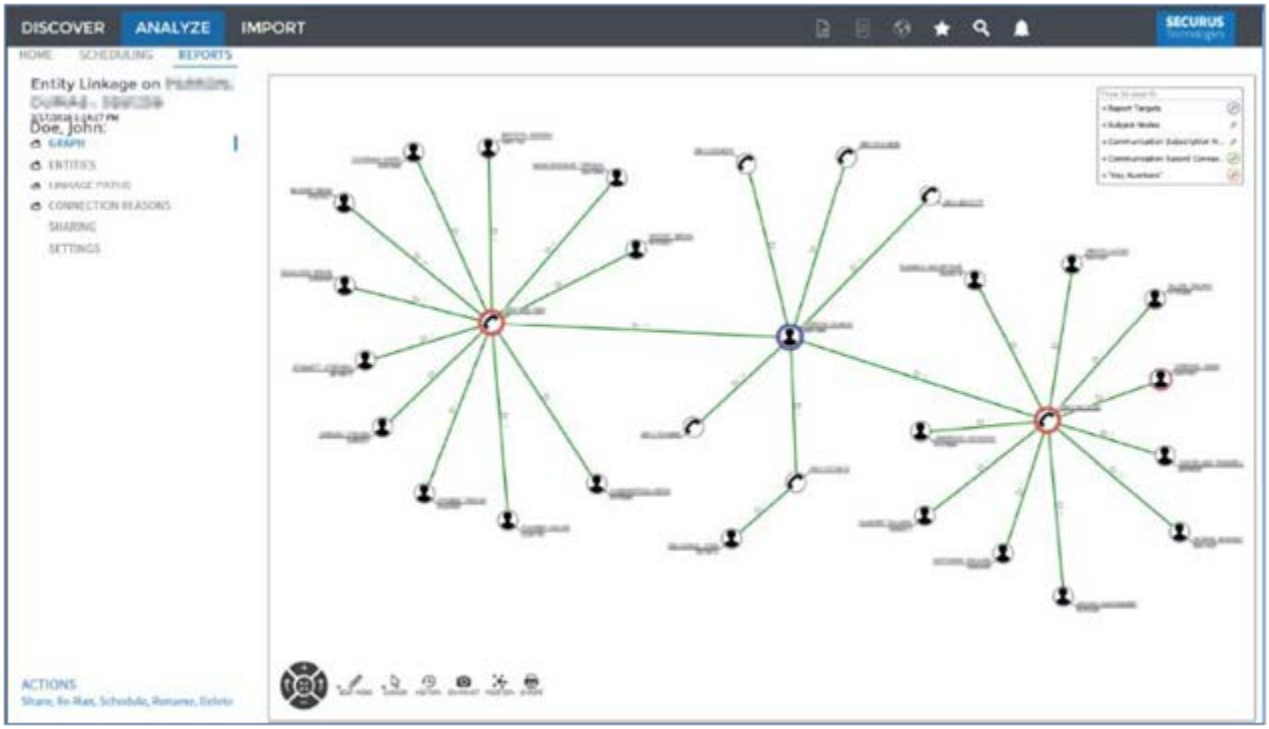
This visual reporting tool is a quick way to understand who offenders are talking to and how the calls are related to other known numbers or offenders.

Users can generate a linkage chart that identifies:

- A target(s) relationships based on user-selected connection types, such as calls, financials, visitation, etc.
- Connections between two selected targets or two sets of targets based on user-selected connection types, such as calls, financials, visitation, etc.
- Connections between two or more targets based on user-selected connection types, such as calls, financials, visitation, etc.

- Direct relationships between selected targets based solely on phone calls

Linkage Analysis



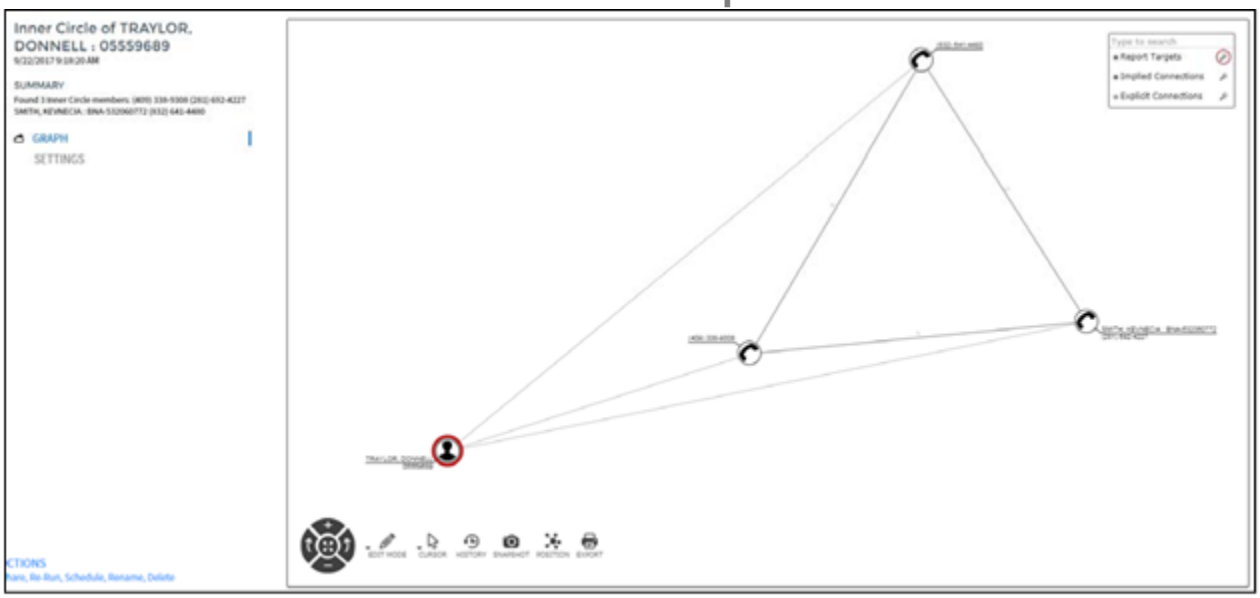
Working Group Reports

Working Group analysis uses a person's communication behavior and calling patterns to identify phone numbers and people of interest. One of the key techniques used is temporal analysis, which associates people based on time between calls. The closer the time between calls, the more likely those calls are related. By leveraging working group reports, facilities can identify gang and other organized activity. Knowing organized groups and gangs can aid staff in monitoring member activity or even taking preventive measures against illicit activities.

- Identify a target's "working group" or inner-circle based on their communication patterns. This report is a graphical linkage chart.
- Display a target's inner circle changes over a predetermined time
- Show communication sequences where a target calls two or more numbers in a pattern
- Identify communication patterns—such as two or more of the same sequence—and when they occurred

- Find a target's chain of calls. A chain is a series of calls triggered by the previous call in the chain. This report requires imported phone calls from outside the facility.
- Identify the most-likely boss in an organization based on chain analysis. This report requires imported phone calls from outside of the facility.

Inner Circle Report



Correlation Reports

Correlation analysis identifies common contacts and phone numbers between offenders, persons, and workspaces. Through correlation reporting, investigators can identify common contacts between offenders as well as fraternization between offenders and facility staff.

- Find any common communications between offenders, persons, or groups of targets
- Identify potential three-way calls between offenders
- Discover common phone numbers between two workspaces

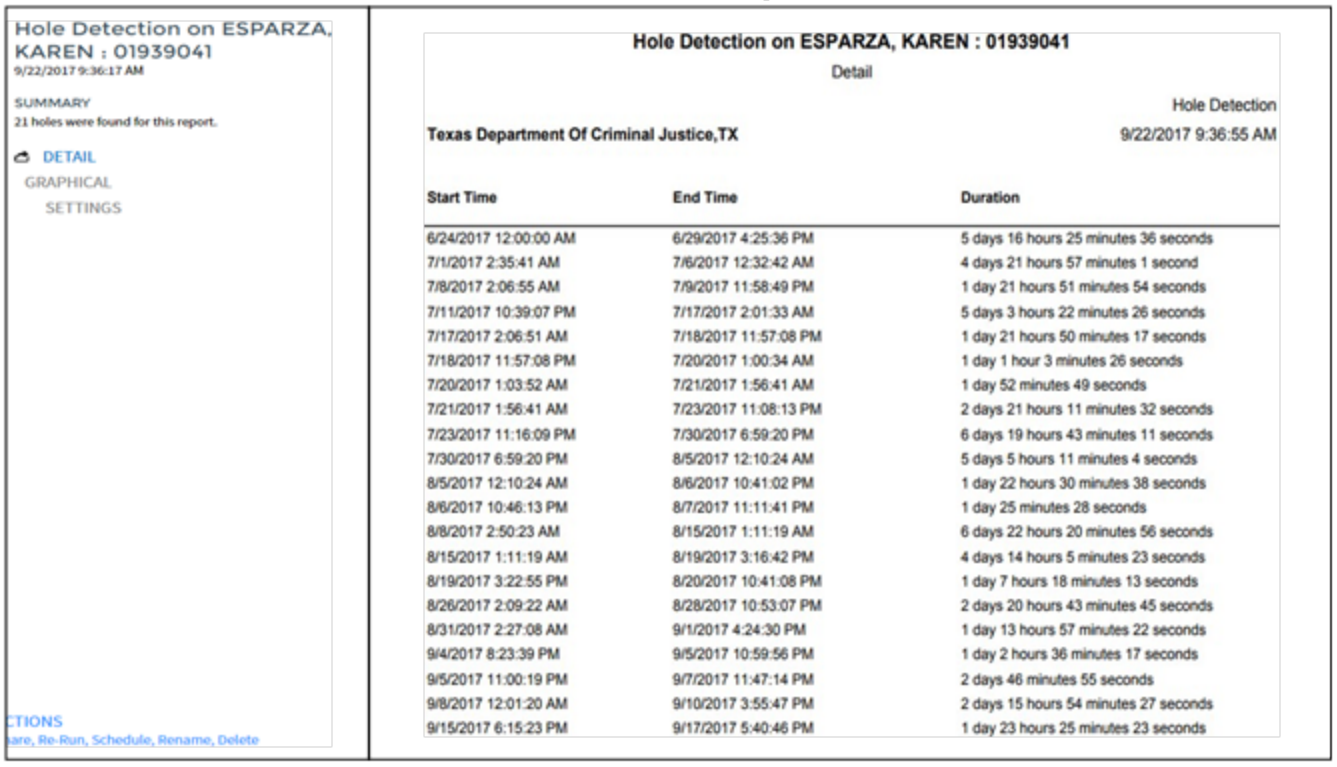
Time-Based Reports

Time-based analysis provides reports based on the timing and frequency of an offender's or other person's communications. Find out when communication is frequently taking place, then identify periods of time where communication is not

taking place. These gaps in communication can indicate behavioral changes as well as cell phone usage.

- Identify holes or gaps in an offender's or person's communication activity
- Display a set of phone numbers that a person called where communications stop with one phone number and starts communication with a different phone number within a close proximity of time. This might indicate a change of phone number or an organizational shift.
- Identify if two or more phones are being used at overlapping times. If there is a significant time overlap, it could indicate that the phones are being used by different people.
- Generate a graphical timeline of any activity—such as communication, association, financial transactions, etc.—that includes a date and time.

Hole Detection Report



Hole Detection on ESPARZA, KAREN : 01939041
9/22/2017 9:36:17 AM

SUMMARY
21 holes were found for this report.

DETAIL
GRAPHICAL
SETTINGS

CTIONS
are, Re-Run, Schedule, Rename, Delete

Hole Detection on ESPARZA, KAREN : 01939041
Detail

Hole Detection
Texas Department Of Criminal Justice,TX 9/22/2017 9:36:55 AM

Start Time	End Time	Duration
6/24/2017 12:00:00 AM	6/29/2017 4:25:36 PM	5 days 16 hours 25 minutes 36 seconds
7/1/2017 2:35:41 AM	7/6/2017 12:32:42 AM	4 days 21 hours 57 minutes 1 second
7/8/2017 2:06:55 AM	7/9/2017 11:58:49 PM	1 day 21 hours 51 minutes 54 seconds
7/11/2017 10:39:07 PM	7/17/2017 2:01:33 AM	5 days 3 hours 22 minutes 26 seconds
7/17/2017 2:06:51 AM	7/18/2017 11:57:08 PM	1 day 21 hours 50 minutes 17 seconds
7/18/2017 11:57:08 PM	7/20/2017 1:00:34 AM	1 day 1 hour 3 minutes 26 seconds
7/20/2017 1:03:52 AM	7/21/2017 1:56:41 AM	1 day 52 minutes 49 seconds
7/21/2017 1:56:41 AM	7/23/2017 11:08:13 PM	2 days 21 hours 11 minutes 32 seconds
7/23/2017 11:16:09 PM	7/30/2017 6:59:20 PM	6 days 19 hours 43 minutes 11 seconds
7/30/2017 6:59:20 PM	8/5/2017 12:10:24 AM	5 days 5 hours 11 minutes 4 seconds
8/5/2017 12:10:24 AM	8/6/2017 10:41:02 PM	1 day 22 hours 30 minutes 38 seconds
8/6/2017 10:46:13 PM	8/7/2017 11:11:41 PM	1 day 25 minutes 28 seconds
8/8/2017 2:50:23 AM	8/15/2017 1:11:19 AM	6 days 22 hours 20 minutes 56 seconds
8/15/2017 1:11:19 AM	8/19/2017 3:16:42 PM	4 days 14 hours 5 minutes 23 seconds
8/19/2017 3:22:55 PM	8/20/2017 10:41:08 PM	1 day 7 hours 18 minutes 13 seconds
8/26/2017 2:09:22 AM	8/28/2017 10:53:07 PM	2 days 20 hours 43 minutes 45 seconds
8/31/2017 2:27:08 AM	9/1/2017 4:24:30 PM	1 day 13 hours 57 minutes 22 seconds
9/4/2017 8:23:39 PM	9/5/2017 10:59:56 PM	1 day 2 hours 36 minutes 17 seconds
9/5/2017 11:00:19 PM	9/7/2017 11:47:14 PM	2 days 46 minutes 55 seconds
9/8/2017 12:01:20 AM	9/10/2017 3:55:47 PM	2 days 15 hours 54 minutes 27 seconds
9/15/2017 6:15:23 PM	9/17/2017 5:40:46 PM	1 day 23 hours 25 minutes 23 seconds

Financial Reports

Financial analysis identifies correlations between offenders and people based on the funding of an offender's accounts.

- Identify offender financial accounts with multiple funding sources
- Identify and list financial transactions of interest for a set of targets

Efficient Automated Reports

When key information is gathered, investigators must determine where all of that data will go and then take part in the time-consuming method of analysis. However, THREADS takes it one step further by allowing facilities to set up automated reports. Reports can be scheduled to take place daily, weekly, or monthly. Through this automated reporting process, users receive notifications regarding the data they use at the timeframes they select.

Managed Data Analytics

For facilities interested in using THREADS but requiring additional investigative resources, Securus offers Guarded Exchange to provide this service. Guarded Exchange is a Securus company run by current and former law enforcement and corrections personnel. With more than 20 years of experience, Guarded Exchange has the resources to run THREADS reporting and analytics, and provide actionable intelligence to the CDOC facility members. Guarded Exchange is here to serve the CDOC, import and filter data, and provide the investigative leads that the State is looking for.

Risk Mitigation and Proactive Monitoring/Auditing

The Securus Network Operations Center (NOC) continuously monitors all data centers, infrastructure components, platform systems, and network/communication systems using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus NOC also monitors real-time video surveillance and environmental alerts for the Securus data centers. In the event there is an issue at the Securus Network Operations Center, **Securus maintains a fully redundant backup Network Operations Center at a separate physical location.**

The Securus Technical Support Team monitors all facility-based equipment and connectivity 24x7x365 including firewalls, integrated access devices (IADs), visitation phone monitoring (VPM) units, routers, switches, on-site systems, wireless access points, user interfacing kiosks and terminals, and uninterrupted power supply (UPS) systems.

The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. In addition to real-time monitoring and alerting, Securus Technical Support also leverages our network performance monitoring system to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. This ongoing, proactive, in-depth analysis of your systems' performance enables our Technical Support Team to prevent and mitigate facility issues.

Data storage redundancy is a key component of Securus' Risk Mitigation and Disaster Recovery Plan. Securus maintains two data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.995% availability.



Securus' data centers meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier III, with some Tier IV (highest level) attributes, for data centers including:

- ability to withstand a 96-hour power event
- multi-layer physical security
- multiple power delivery paths

Each data center has redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity.

Securus' data centers are staffed 24x7x365 for immediate physical assistance inside the data center.

Data is no longer susceptible to loss due to an individual drive failure or issues at your location: The Securus communication platform uses technology that is much more advanced than traditional local onsite storage. Securus uses a mix of Storage Area Network (SAN)—a high-speed sub-network of shared storage devices—and Network-Attached Storage (NAS). This architecture avails all storage devices to all servers on Local Area Networks (LANs) or Wide Area Networks (WANs). Data is stored in Redundant Arrays of Independent Disk (RAID) formats, spreading the data across multiple drives, which provides additional protection. Accordingly, this architecture provide facilities with the ultimate protection against single drive or server failures, as well as increased security. **Securus maintains hardware replacement inventory on**

your site, in our Field Service Team vehicles, and at centralized locations. In addition, we have distribution agreements with our vendors so that in the event of disaster recovery efforts, we can get replacement equipment to your facilities quickly.

Localized Event Affecting Only Securus Facilities

In the event of a disaster impacting Securus, the local Securus Network and systems, or NextGen SCP, Securus immediately assembles a team of engineers to investigate and restore services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and a list of third-party vendors to engage if needed. Our priority is fast resolution and minimal downtime. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Upon confirmation of a service-impacting event, the Network Operations Center will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

The Securus Executive Team and the Securus Account Management Team receive SIRs and communicate with you directly. In addition, the Securus Technical Support Team may communicate a service-impacting event via a splash screen on the NextGen SCP user interface introductory page. Securus updates you regularly throughout resolution. Securus investigates every service-impacting event, completes a root-cause analysis, and provides the analysis to you upon request.

Risk Assessment Plan

Securus has included below a list of Assumptions and a Risk Assessment Plan Sample to concisely demonstrate how Securus plans and handles unexpected or unknown issues or situations that may take place as part of the project implementation process.

Resource Assumptions

- The project will have Securus executive management attention and periodic review.
- Project staff resources including multiple technicians will be available when and as they are needed.
- Required hardware resources will be available when and as they are needed.
- A minimum number of Facility Escorts will be available during normal business hours at multiple locations at the same time.
- A significant percentage of the project staff will be experienced with the technical environment.

- A significant percentage of the project staff will be experienced with the operating environment.
- Access to industry experts and specialized skills will occur as needed.

Delivery Assumptions

- Deliverables will be subject to no more than a specific number of review cycles.
- Schedule is based on circuits being installed and delivered before project start date. Circuit order takes 30 to 45 days.
- Equipment order lead times are known and can be expected to be met.

Environmental Assumptions

- No industrial action will be taken that will affect the project.
- Issues will be resolved in a timely manner.
- The project organization described in the project plan will be put in place.
- Systems components will be capable of being integrated with minimum rework.

Functionality Assumptions

- The scope of the project is limited to that described in the project as engineered.
- Schedule changes may occur after on-site surveys.
- Site Addresses information and contact information that are provided are correct for the purpose of shipping equipment and/or ordering lines/circuits.
- Features are generally available at time of install
- One of the teams Securus will assign is a specialized integration that has significant experience and expertise is this field. JMS integration will have a very high priority with the assignment of the most senior Securus integration resources for this project.
- Formal charter and scope change procedures will be followed during the lifecycle of the installation schedule.

Risk Assessment Plan

Risk Assessment Plan

Risk Description #1:	Telecom Deliver – Requirements for installation

Risk Impact / Why is this a Risk?	Installation of a new telecom circuit could require extended delivery time frames based on accessibility and construction of new lines to the facility
Solution:	Escalations and additional funds will be allocated for expedited requests to the LEC chosen but this will not guarantee a reduction in delivery of the transport to the facility
Documented Performance:	Securus Telecom provisioning will document dates of request to LEC, response from LEC, timeframe of installation projected from the LEC, and actual performance of delivery. All documentation will be provided to the Agency as work is performed and included in project risk log.

Risk Description #2:	**Custom Hardware delivery**
Risk Impact / Why is this a Risk?	Hardware which may be required outside of the standard offering from Securus will require manufacturing time outside of committed installation project plan
Solution:	Identify requirements prior to project initiation and request for manufacture prioritization during order processing
Documented Performance:	Bill of Material provided to Agency and vendor of special hardware requests, tracking details of build performance, and tracking of delivery of hardware post manufacturing

Risk Description #3:	**Integration with JMS and Commissary**

Risk Impact / Why is this a Risk?	Custom requirements beyond both parties which are outside of the standard custom configurations of the software
Solution:	Discuss the requirements for integration, agree to a Level of Effort (LOE), and agree to Securus and Agency software access for timeline to meet the project installation timeframe. Any outstanding items will be move to post cutover statement of work development
Documented Performance:	Each integration item will be identified in a project contractual log to build the design of the integration and follow through of the project checklist for testing and QA of integration between agency and vendor.

Risk Description #4:	**Natural Weather Events (weather and/or physical damage to corporate offices)**
Risk Impact / Why is this a Risk?	Removes the ability for Technical Support Associates to perform task at home office in a comfortable stable environment.
Solution:	We have established a disaster recovery program that affords Associates the ability to work at an alternate location and/or remote. All staff have been allocated laptop units with remote VPN access to allow normal daily function to be performed remotely.
Documented Performance:	Reporting Operational Analysis manages and maintains reporting on executed practice runs for these events with documented performance over the past several years.

Risk Description #5:	**Telecom carrier outages**
Risk Impact / Why is this a Risk?	Full outages of telecom / transport services

Solution:	Dedicated staff that works with the telco providers to push for resolution on any/all outages. Additionally they work to transition to new service type and/or provider if deemed necessary.
Documented Performance:	We measure the team on responsiveness to all priority levels (P1 – P3) with all P1 "all phones down" type issues must be responded to w/in 20 mins. 2017 YTD the team achieved this 96% of the time as documented in our Monthly Operations Review performance deck.

Risk Description #6:	**Customer Driven Delays – Agency facility Access, facility power, Escorts, Keys, facility operations Telecom Deliver – Requirements for installation**

Internal and External Audit Management

Internal auditing and product inspection is performed within the Operations organization, with the Network Operations Center (NOC), and Technical Support Services (TSC) monitoring and responding to system notifications, flags, or ticketing. These report into Matt Pareti, Chief Operations Officer; and Alex Yao, Chief Product Officer and General Manager.

Internal and external financial audits are performed under the direction of the Legal department, assisted by the financial department. These report into Christine Lally, Director of Internal Audits; and Josh Martin, SVP and General Counsel.

Audit

Securus takes the security and access to our software/application very seriously and hence have implemented one of the strongest controls in the industry. Securus access controls for all systems are audited for compliancy with the following accreditations/certification:

- SSAE16; (SOC1, SAS70): Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization

- SOX: The Sarbanes–Oxley Act of 2002, is a United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms.

Securus will provide for an external audit of services on an annual basis by an independent auditing firm—subject to DOC approval—verifying Securus' timing and billing systems are accurate, and that they capture all calls.

Sarbanes-Oxley Compliance

Securus access controls for all systems are internally audited for compliance with The Sarbanes–Oxley Act of 2002 (SOX), which set new or enhanced standards for all U.S. public company boards, management, and public accounting firms. These widely recognized distinctions confirm that the company has effective controls and safeguards in place to manage its financial matters. This internal audit ensures the CDOC will get accurate and timely reporting of all financial transactions.

f. Provide methods of identifying non-conformance in services provided that affect contract performance

- **Describe the process for how and when the Offeror documents nonconformance in services provided**
- **Identify who is involved in the process**
- **Address how instances of nonconformance are communicated throughout the entire organization, and to CDOC as applicable**
- **Identify the systems (i.e., electronic or manual) used to identify nonconformance, and how the systems interface with personnel**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Non-conformance is identified through the Network Operations Center and through tickets opened by authorized personnel identifying con-conformances that need to be addressed. These processes are described below.

The NOC and TSC are under the Operations Organization.

Network Operations Center (NOC)

Our Network Operations Center (NOC) technicians continuously monitor and control all hardware, software, and system performance, including the ability to reboot kiosks remotely. This allows our dedicated personnel to diagnose and resolve issues, often before the CDOC notices a problem. If the NOC is unable to remotely resolve a software issue, technicians may be dispatched to conduct onsite repairs. If the team detects that a larger fix is required, Securus collaborates with the account manager and field technicians to resolve the issue. All application and software updates are loaded onto field equipment remotely. These upgrades are vetted by a Change Control Committee,

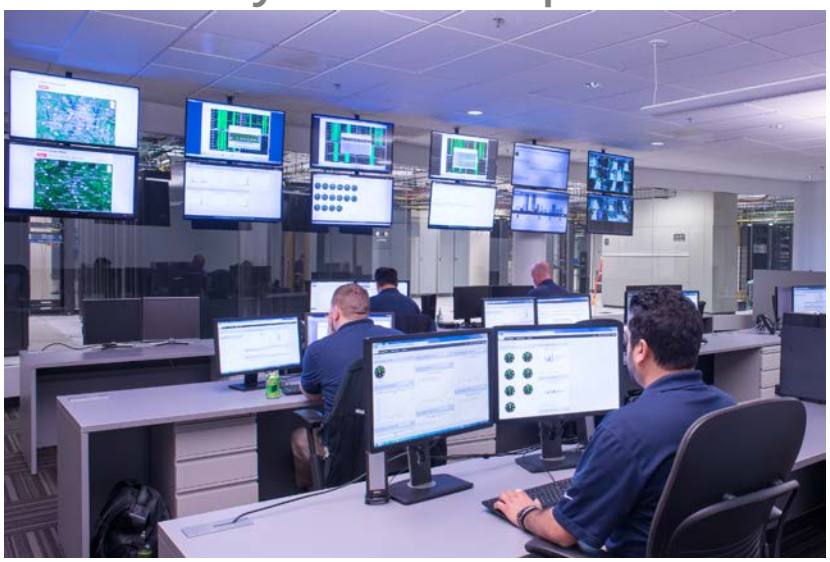
then subject to a rigorous testing phase before being released into the field. JPay monitors and manages the entire process remotely, allowing for zero impact on resources.

Continuous Monitoring

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring and proactively monitors our systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

Securus Primary Network Operations Center



Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment. The systems are polled every two minutes to ensure proper operation, and their vital

operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. I

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Ticketing process for service and Non-Conformance

In 2009, Securus made a strategic decision to centralize management of all technical support. Today, Securus provides superior customer service capabilities from a state-of-the-art technical support center located in the Dallas, Texas, metro area.

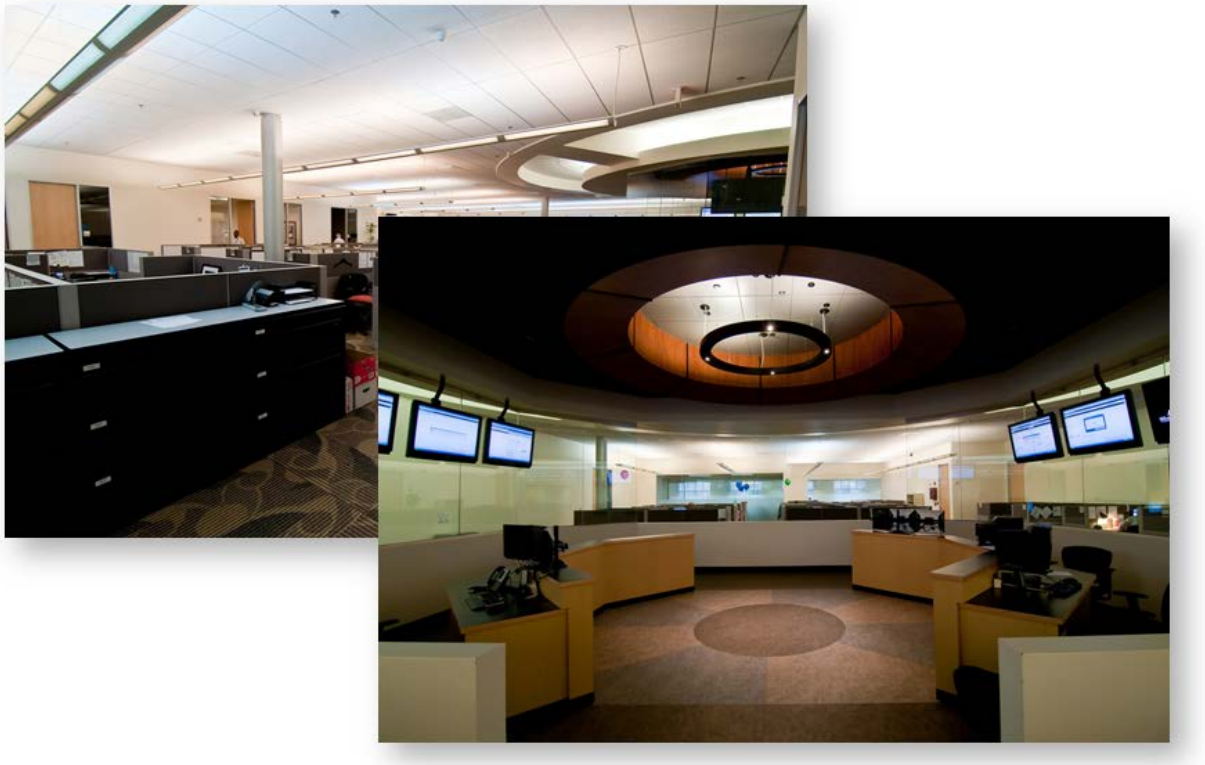
Approximately 50 technical professionals staff the Securus Technical Support Center (TSC) which handles approximately 8,000 inbound queries per month. The TSC provides a single-point-of-contact for Securus customers for issues ranging from minor maintenance issues to service outages. Clients can contact the TSC 24x7x365 by any of the following convenient methods:

- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - http://www.securustech.net/facility/Default.asp

The technical service center offers our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure achievement of Service Level Agreements
- Certified technicians to provide quick problem resolution
- System and individual site connectivity monitored 24x7x365

24x7x365 Securus Technical Support Center



Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

Service Levels

When a facility calls Securus, an event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a prescribed resolution timeline and escalation procedure. In all cases, Technical Support will respond to the customer within the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects 30 percent or more of system functionality. Examples of P1 service assignments include:

- Voice prompts not operating
- Features are not operating appropriately
- CD-burning abilities disabled

- Live call monitoring is not operating appropriately
- NextGen SCP access denied
- All phones out-of-service

The response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

A P1 events escalate to:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If the problem resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment—our mid-level priority assignment—occurs when a system event adversely affects 5 to 29 percent of system functionality. Examples of a P2 service assignment include problems or errors with related to:

- Workstation
- Specific system ports
- Local Exchange Carrier (LEC) circuits
- Unblocks
- Blocked numbers
- Missing call detail records (CDRs)
- Call searching

The response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P2 events escalate to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment—our lowest priority assignment—occurs when a system event adversely affects 5 percent or less of system functionality. System events adversely affecting some of available facility phones. Examples of P3 service assignments include:

- Static on the phone
- A party's inability to hear
- An offender's inability to dial
- A broken phone
- Non-functioning dial pad
- Non-functioning cutoff switches
- An inability to generate reports

The response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P3 events escalate to the Technical Support Department.

Escalations

If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

The supervisory escalation chain is:

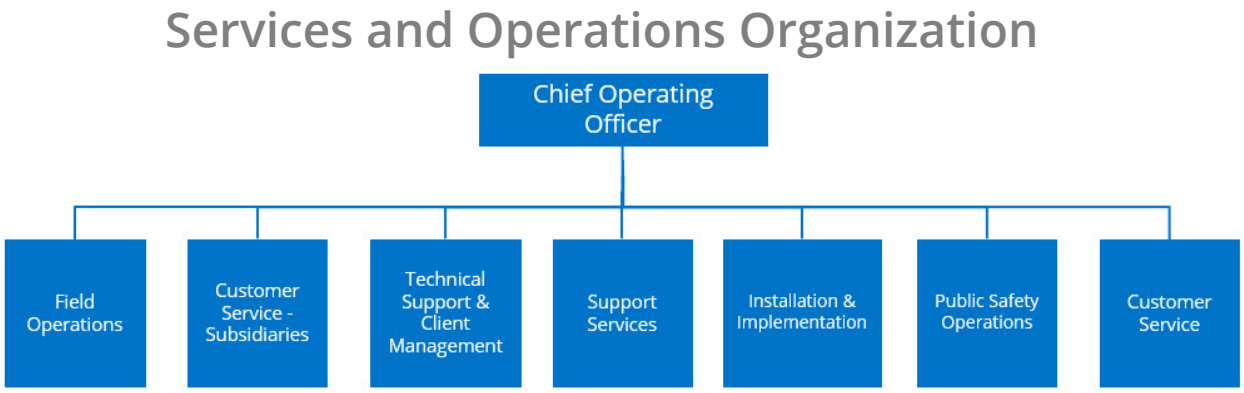
- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Chief Operating Officer

Centralized Services Operations Model

All Securus services and operations are managed centrally, from our Service and Operations organization in Dallas, Texas. The Operations team's responsibility is supporting external customers, including Customer Service, Field Services, Installation and Engineering, and Technical Support. The Support Services team provides internal

support services including Quality, Training and Customer Satisfaction, and Reporting and Analysis.

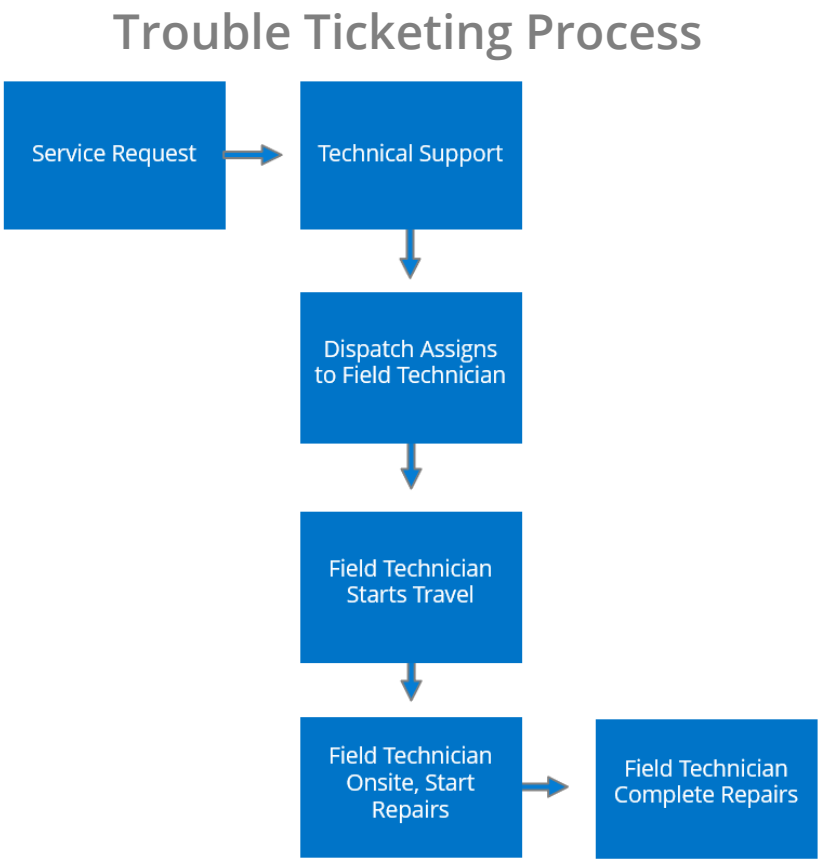
The following figure illustrates the Securus Service and Operations organization, which is staffed by full-time Securus employees.



Securus adopted this operational model because of the natural interaction between functional groups. Having our support services integrated and centrally managed enables cross-functional group interaction, improving the response time, and efficiencies of our services.

Call Routing

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.



In all instances, service will be requested through the TSC and field service personnel will be dispatched through trouble ticketing system to ensure documentation and timely resolution of all service tickets.

Event Tracking System

The Securus event tracking system logs, tracks, manages, and assures an appropriate response to all service requests. The service request generates a unique trouble ticket number linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.

The TSC maintains ownership of all service requests and responsibility for the escalation and update functions. Every effort is made to resolve problems remotely and within the framework of resolution timeframes. However, if the problem requires on-

site service, a technician is dispatched. Securus will contact the facility to arrange for the on-site service at the convenience of the facility.

Facilities can also use Securus' request portal to create self-help tickets and monitor and track ticket status.

Facility Service Request Portal

CDOC can access Securus' service request portal as an alternative to calling Securus Technical Support to create new service requests or to track the status of existing service requests.



Securus' service request portal is an automated ticketing system that logs, tracks, manages, and assures appropriate responses to all service requests for a correctional facility, regardless of whether the request was initiated from a call to Securus Technical Support or entered directly into the service request portal.

The service request portal is one of the major tools in our arsenal to meet service level agreements with confidence, increase overall operational effectiveness, solve problems, streamline repetitive tasks, and improve customer satisfaction.

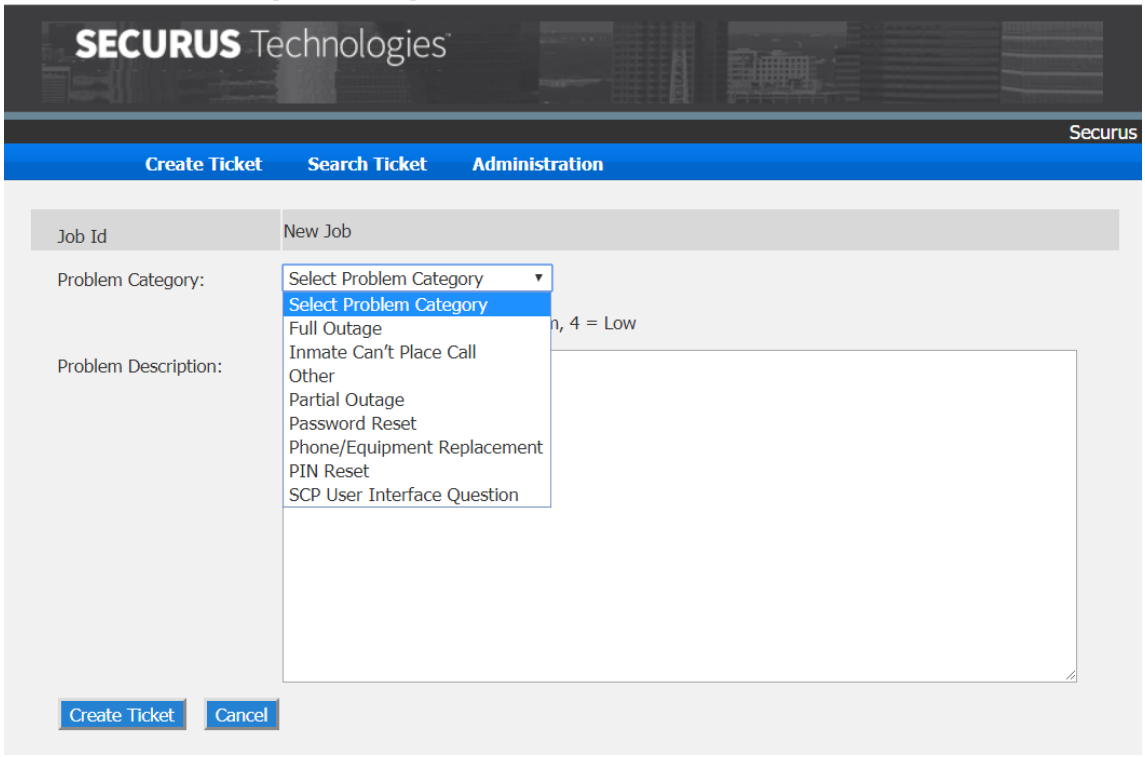
When a facility requires a service visit for any reason, including routine maintenance, a service ticket is opened and visible within the service request portal to track the event and allow for further analysis of any system issues and/or performance.

As with all service requests, those entered directly into the service request portal include information collected on the issue as gathered by the certified technician(s) to ensure our response is appropriate for the service event. Diagnosis of the event will determine whether the request or repair can be performed remotely or if onsite trouble-shooting assistance with our local field technician, working in conjunction with our Network Operations Center (NOC), is necessary. All service events, whether resolved remotely or via an onsite visit, are tracked and our customers can provide feedback on how we have performed and if we met their expectations. Further, the service event will be assessed to avoid repetitive service issues, which may indicate a system deficiency issue or fraudulent activity.

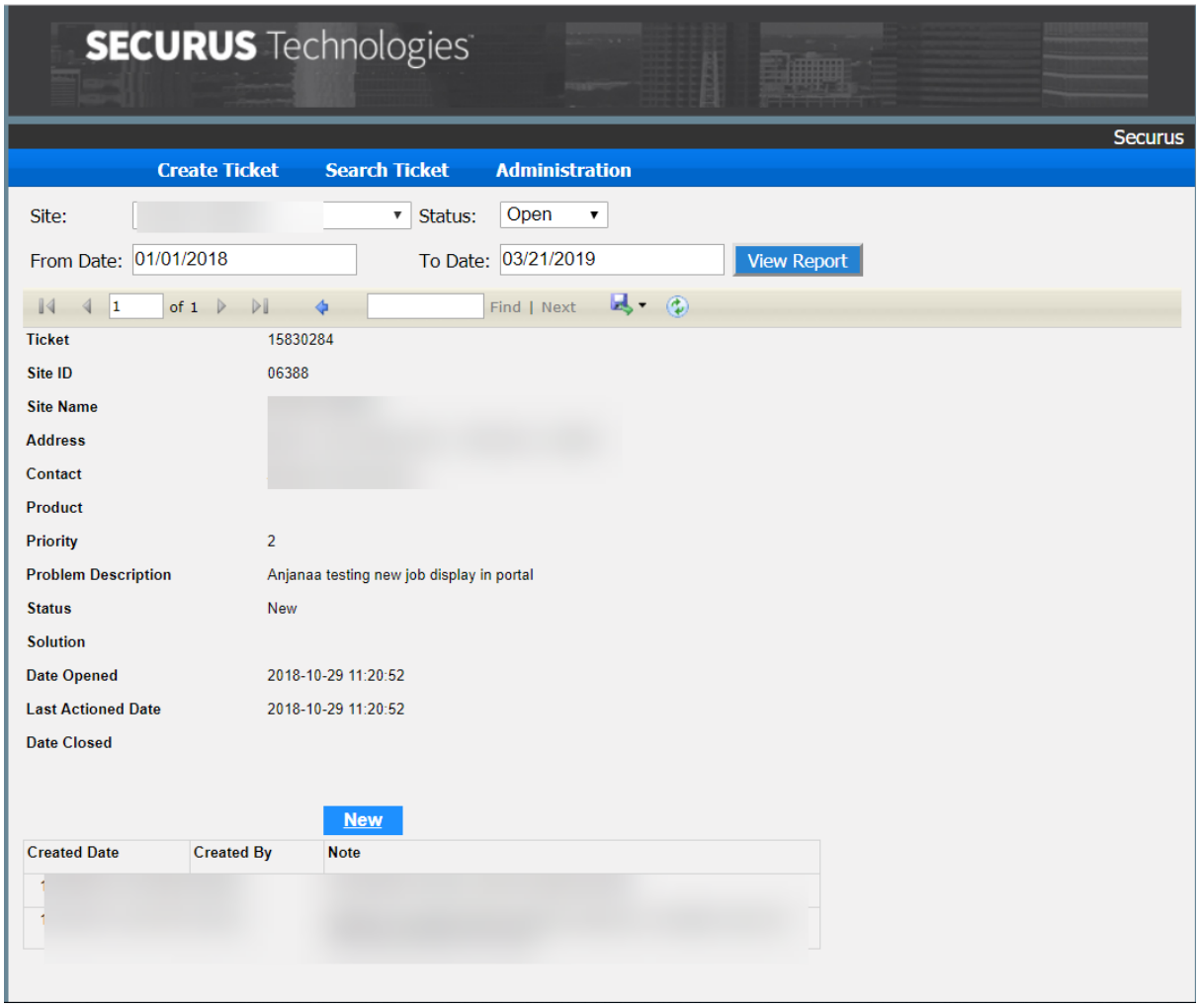
The service request ticketing system is used in various departments throughout Securus to provide a current view of any open items. The system automatically generates reports internally that are sent to management for service level reviews and customer status.

Through the Securus service request portal, CDOC staff can view, track, and open service tickets; the portal also offers CDOC the advantage of knowing the status of a resolution or viewing comments on any service request, which results in efficient and effective communication through this direct line of communication without needing to place a call.

Opening a New Service Ticket



Ticket Number with Detail



g. Provide formal systems to implement corrective actions when there are non-conformances in services provided that affect contract performance

- **Describe any electronic system used to implement corrective actions**
- **Describe how long it takes to document nonconformance**
- **Explain whether the same corrective action processes and procedures are implemented for subcontractors**
- **Explain how the Offeror determines the effectiveness and timeliness of implemented corrective actions**
- **Describe the means used to ensure that appropriate corrective actions are taken, and that the Offeror's senior management and executive leadership are involved as needed**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As discussed above, Non-conformance is identified through the Network Operations Center and through tickets opened by authorized personnel identifying con-conformances that need to be addressed. Very often, the NOC identifies issues before they are “symptomatic” to the customer and issues are often resolved in advance of a manifestation of the need for corrective action. Because support is 24/7/365, how long it takes to identify a non-conformance will vary, dependent on the specific circumstances. The ticketing process is described below.

It is not expected that any subcontractors will be involved in this contract in addressing the identification or resolution of non-conformances. Securus is proud of its domestic services team.

Securus uses proprietary systems developed with the Corrections industry in mind.

Patents, showing Securus leadership in the Corrections Industry

Every company has a source of significant pride. For Securus, our pride comes from our growing patent portfolio because it is a tangible representation of our leadership in

Emerging technologies are those technical innovations that represent progressive development. Securus has a long history of providing progressive solutions to its customers, as evidenced by its impressive intellectual property portfolio. Securus has had more than 230 patents issued and 100 pending patents.

Securus serves all customers from a single, Securus-owned technology platform built from the ground up. The requests from correctional and law enforcement professionals guided the development of the platform’s features and functionality. We heard our customers, and we created a user experience based on their feedback. We manage, service, and enhance our platform using only Securus associates. Most other providers do not own and service their entire platform. Dilution of accountability and service is inevitable when a company outsources their technology. We believe it is important to own and maintain our communications platform so that we can quickly respond to customer requests without depending on a third party. We lead the industry in available features today, and we are continuously developing more.

Ticketing process for Service and Non-Conformance

In 2009, Securus made a strategic decision to centralize management of all technical support. Today, Securus provides superior customer service capabilities from a state-of-the-art technical support center located in the Dallas, Texas, metro area.

Approximately 50 technical professionals staff the Securus Technical Support Center (TSC) which handles approximately 8,000 inbound queries per month. The TSC provides a single-point-of-contact for Securus customers for issues ranging from minor

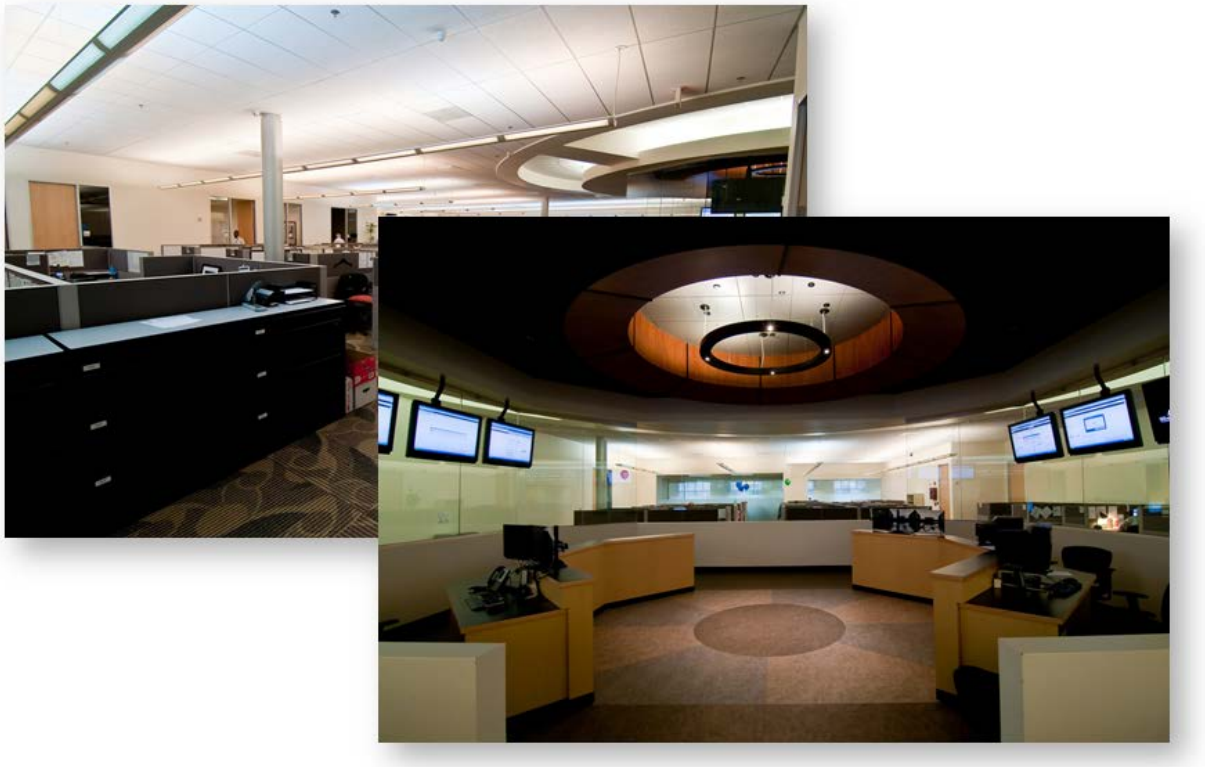
maintenance issues to service outages. Clients can contact the TSC 24x7x365 by any of the following convenient methods:

- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - http://www.securustech.net/facility/Default.asp

The technical service center offers our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure achievement of Service Level Agreements
- Certified technicians to provide quick problem resolution
- System and individual site connectivity monitored 24x7x365

24x7x365 Securus Technical Support Center



Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

Securus Maintenance and Technical Support Services

Securus provides superior customer service from a state-of-the-art operations center located in Carrollton, Texas. More than 50 technicians staff the Securus Technical SupportCenter (TSC) to ensure prompt resolution. The average tenure of our technicians is 8 years and the average tenure for our technical support management is 10 years.

The Securus TSC serves as a single point of contact for facility staff for all Participating States to request service **24 hours a day, seven days a week, 365 days per year** via toll-free number or email. Calls are automatically routed directly to our support technicians in a skills-based, platform-specific manner.

Technicians assign each service request one of three initial priority levels, each with resolution and escalation timelines. Every effort is made to resolve the problem remotely within the designated timeframes, and Securus resolves most service requests during the initial request. If necessary, a field service technician is dispatched to the facility to expedite resolution.

The TSC logs, tracks, manages, and assures appropriate response to all service requests. The service request generates a trouble ticket with priority level assignment that drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages an appropriate party for resolution. The TSC retains ownership of all service requests and is responsible for the escalation and customer status update functions. The following service response times are guidelines; we will always work to resolve all issues as quickly as possible.

Service Levels

When a facility calls Securus, an event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a prescribed resolution timeline and escalation procedure. In all cases, Technical Support will respond to the customer within the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects 30 percent or more of system functionality. Examples of P1 service assignments include:

- Voice prompts not operating
- Features are not operating appropriately
- CD-burning abilities disabled
- Live call monitoring is not operating appropriately
- NextGen SCP access denied
- All phones out-of-service

The response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

A P1 events escalate to:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If the problem resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment—our mid-level priority assignment—occurs when a system event adversely affects 5 to 29 percent of system functionality. Examples of a P2 service assignment include problems or errors with related to:

- Workstation
- Specific system ports
- Local Exchange Carrier (LEC) circuits
- Unblocks
- Blocked numbers
- Missing call detail records (CDRs)
- Call searching

The response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P2 events escalate to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment—our lowest priority assignment—occurs when a system event adversely affects 5 percent or less of system functionality. System events adversely affecting some of available facility phones. Examples of P3 service assignments include:

- Static on the phone
- A party's inability to hear
- An offender's inability to dial
- A broken phone
- Non-functioning dial pad
- Non-functioning cutoff switches
- An inability to generate reports

The response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P3 events escalate to the Technical Support Department.

Escalations to ensure corrective actions are taken

If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

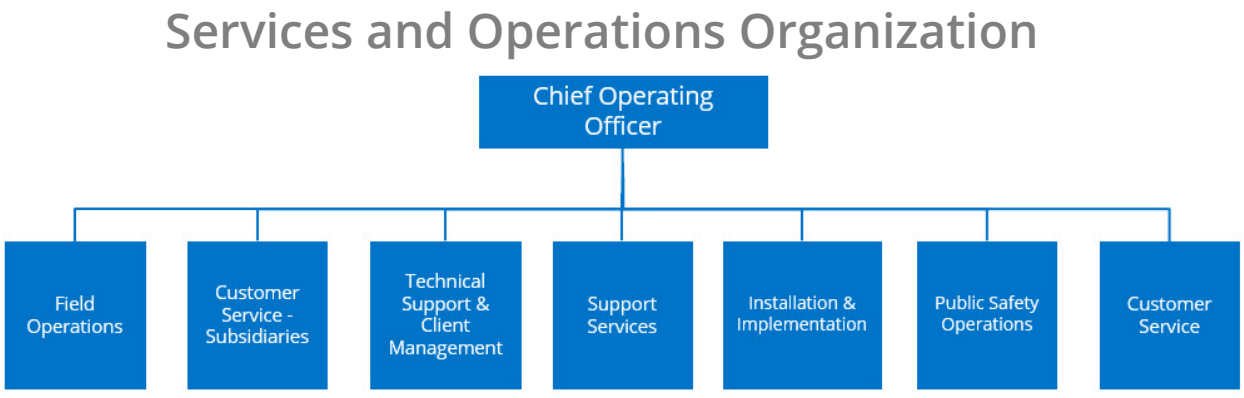
The supervisory escalation chain is:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Chief Operating Officer

Centralized Services Operations Model

All Securus services and operations are managed centrally, from our Service and Operations organization in Dallas, Texas. The Operations team's responsibility is supporting external customers, including Customer Service, Field Services, Installation and Engineering, and Technical Support. The Support Services team provides internal support services including Quality, Training and Customer Satisfaction, and Reporting and Analysis.

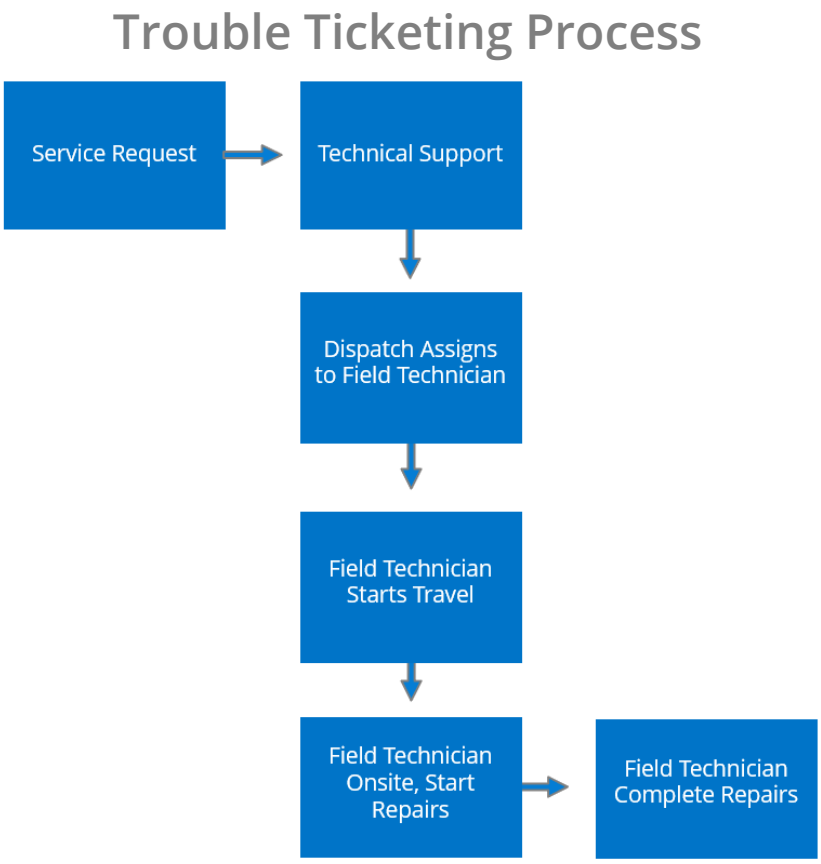
The following figure illustrates the Securus Service and Operations organization, which is staffed by full-time Securus employees.



Securus adopted this operational model because of the natural interaction between functional groups. Having our support services integrated and centrally managed enables cross-functional group interaction, improving the response time, and efficiencies of our services.

Call Routing

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.



In all instances, service will be requested through the TSC and field service personnel will be dispatched through trouble ticketing system to ensure documentation and timely resolution of all service tickets.

Event Tracking System

The Securus event tracking system logs, tracks, manages, and assures an appropriate response to all service requests. The service request generates a unique trouble ticket number linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.

The TSC maintains ownership of all service requests and responsibility for the escalation and update functions. Every effort is made to resolve problems remotely and within the framework of resolution timeframes. However, if the problem requires on-site service, a technician is dispatched. Securus will contact the facility to arrange for the on-site service at the convenience of the facility.

Facilities can also use Securus' request portal to create self-help tickets and monitor and track ticket status.

Facility Service Request Portal

CDOC can access Securus' service request portal as an alternative to calling Securus Technical Support to create new service requests or to track the status of existing service requests.



Securus' service request portal is an automated ticketing system that logs, tracks, manages, and assures appropriate responses to all service requests for a correctional facility, regardless of whether the request was initiated from a call to Securus Technical Support or entered directly into the service request portal.

The service request portal is one of the major tools in our arsenal to meet service level agreements with confidence, increase overall operational effectiveness, solve problems, streamline repetitive tasks, and improve customer satisfaction.

When a facility requires a service visit for any reason, including routine maintenance, a service ticket is opened and visible within the service request portal to track the event and allow for further analysis of any system issues and/or performance.

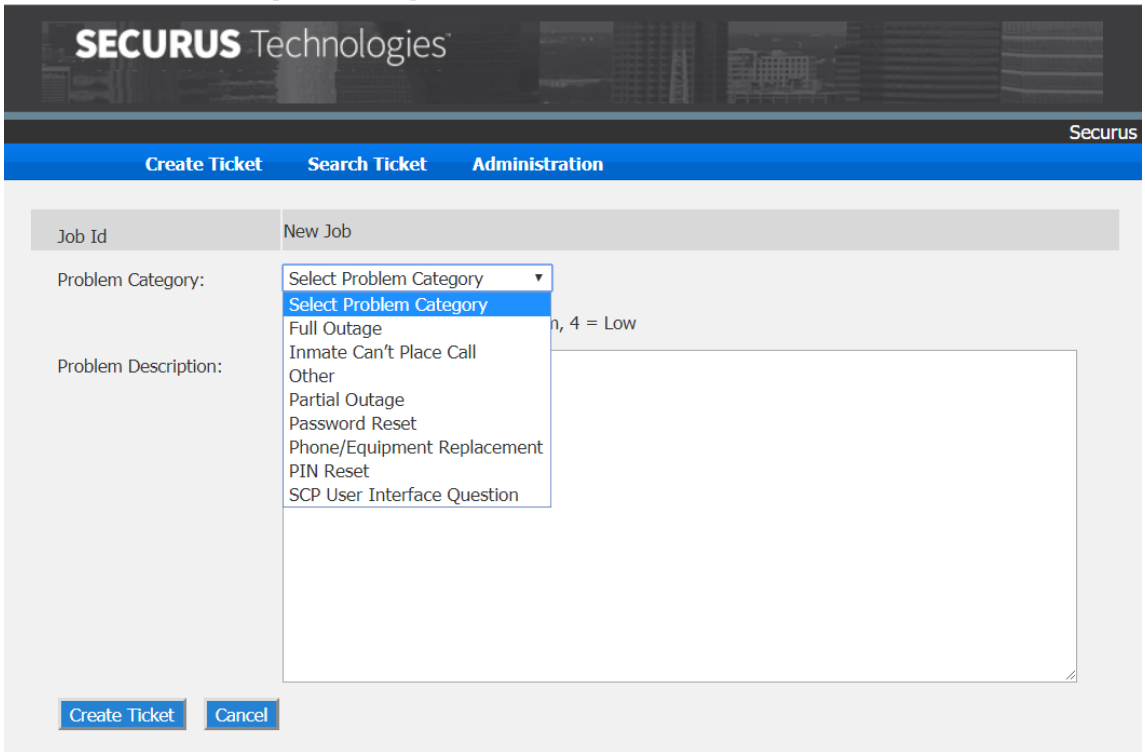
As with all service requests, those entered directly into the service request portal include information collected on the issue as gathered by the certified technician(s) to ensure our response is appropriate for the service event. Diagnosis of the event will determine whether the request or repair can be performed remotely or if onsite

trouble-shooting assistance with our local field technician, working in conjunction with our Network Operations Center (NOC), is necessary. **All service events, whether resolved remotely or via an onsite visit, are tracked and our customers can provide feedback on how we have performed and if we met their expectations.** Further, the service event will be assessed to avoid repetitive service issues, which may indicate a system deficiency issue or fraudulent activity.

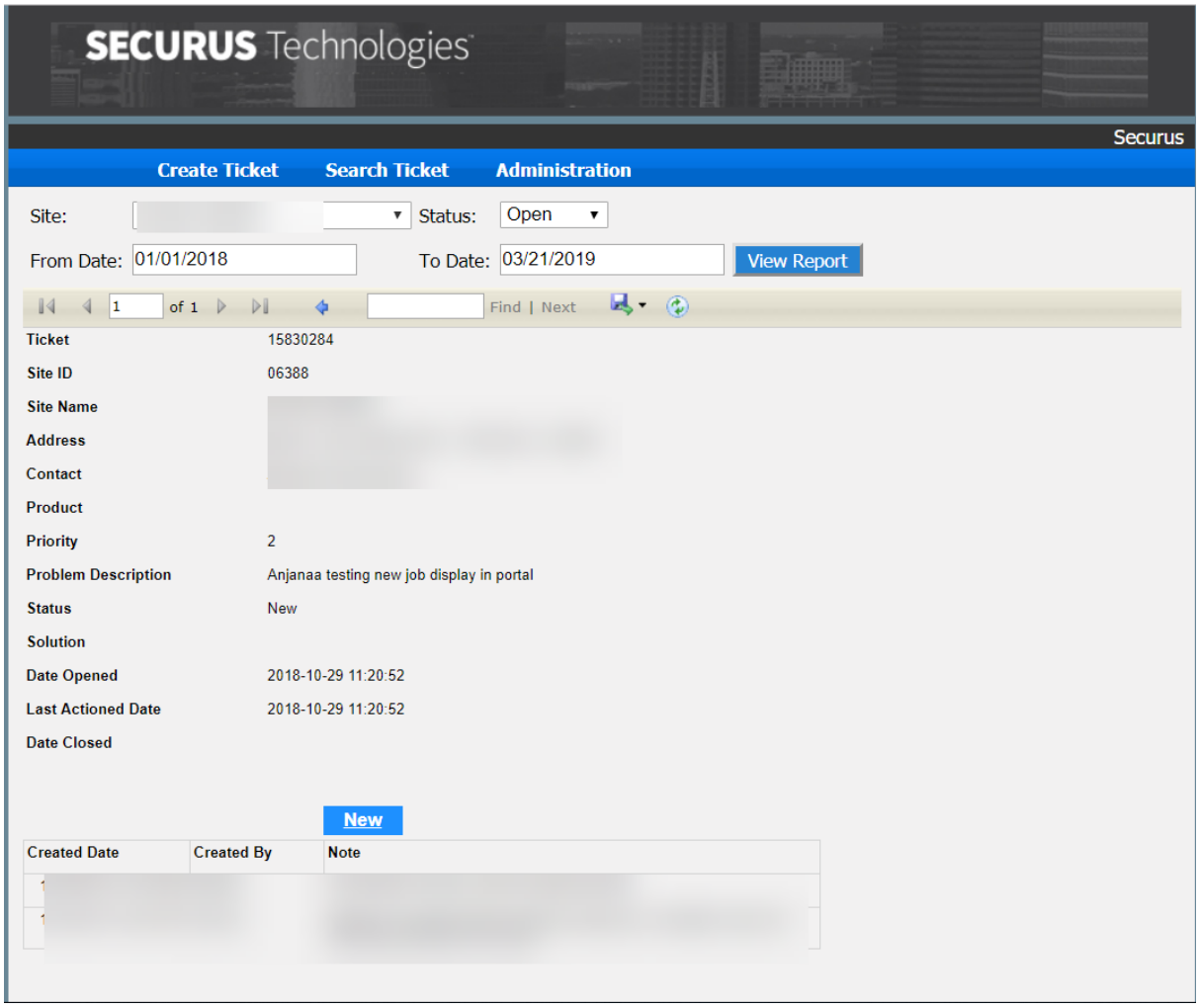
The service request ticketing system is used in various departments throughout Securus to provide a current view of any open items. The system automatically generates reports internally that are sent to management for service level reviews and customer status.

Through the Securus service request portal, CDOC staff can view, track, and open service tickets; the portal also offers CDOC the advantage of knowing the status of a resolution or viewing comments on any service request, which results in efficient and effective communication through this direct line of communication without needing to place a call.

Opening a New Service Ticket



Ticket Number with Detail



h. Provide all files to CDOC relating to inspections and audits conducted and corrective actions implemented for the duration of its contract

- **Describe the Offeror's records retention process**
- **Describe how the Offeror maintains its inspections and audits records**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus maintains books, records, and documents in accordance with generally accepted accounting practices that sufficiently and properly reflect all gross revenues generated.

Annual audits are conducted by a big-four independent accounting and auditing firm, which is regulated by the Security and Exchange Commission and ensures CDOC will get accurate and timely reporting and payments from Securus. External financial audits are conducted by Price Waterhouse Coopers (PWC).

These audits indicate a comprehensive and in-depth evaluation and testing of our internal controls over financial reporting and confirm that Securus has effective controls and safeguards to manage financial information and data. A PCI assessment is performed annually by an independent qualified audit firm and confirms that Securus has effective controls and safeguards over our customers' and clients' financial data.

Offender telecommunications providers like Securus need to install and operate highly sophisticated call management platforms and related services to meet the security and public safety needs of correctional facilities; therefore, we need to accurately process, manage, and control millions of call records and call recordings for security and investigative purposes.

Records Retention Policy

"Aventiv Technologies Records Retention and Disposal Policy".

Effective from June 11, 2020.

Policy applies to Aventiv Technologies and subsidiaries, including Securus Technologies, LLC.

Policy statement sets frameworks and criteria for retention and disposal of all records covered under the policy. This is intended to ensure that Aventiv and subsidiaries:

- Meet legal standards
- Properly manager use of electronic and physical storage space, and
- Properly dispose of outdated records

The following terms are specifically defined to ensure consistent and legal treatment of all records and documents: Record, Active Record, Electronic Record, Inactive Record, and Personal Information.

All records are to be maintained for specific periods of time, taking into account legal and/or other organizational requirements.

To ensure full compliance, each department is trained and responsible for managing records in accordance with policies.

The following areas are executed by assigned departments:

- Implementing Records, Management Practices consistent with corporate policies.
- Educating staff in records management policy.
- Preserving records consistent with corporate policy

- Properly disposing of inactive records at the end of applicable retention periods.
- Protecting records against misuse, misplacement, damage, destruction, or theft.
- Monitoring compliance with this policy.

The policy document includes an appendix assigning retention periods appropriate to the type of document.

All records pertaining to pending or ongoing subpoenas, known government investigations, lawsuits, etc., are protected from disposal, destruction, or removal in compliance with law and good faith best practices.

Disposal processes of the various types of documents are defined.

i. Provide assistance to Review Teams during CDOC's inspections and audits while work is in process or complete. Describe how the Offeror will assist CDOC reviewers during their inspections and audits.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work closely with CDOC personnel in pulling a variety of reports, and in helping customize reports, to assist in documenting data required by the CDOC.

j. Offeror is expected to include proposed Quality Control/Corrective Action Plan with their proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus continually enhances quality to maximize customer satisfaction. We do this through a comprehensive approach that includes our culture, our employee selection process, measurements and feedback, system and process design, and internal controls.

Our Culture

At Securus, we believe a commitment to quality starts with culture. Securus has developed a culture of measurement and continuous improvement. Each Securus department measures and reports customer satisfaction and performance toward quality objectives. Internal teams review and analyze the results, and action items and initiatives are created to improve on results. Each quarter the company recognizes employees and work teams that have achieved outstanding results in the areas of teamwork, quality, innovation, and customer satisfaction.

Employee Selection

Having a quality-oriented culture is vital, but employees committed to our values and performing at the highest level is what sets us apart. Securus uses a formal process for employee selection that involves multiple departments and management levels. An in-house recruiter seeks out top candidates for open positions. Screenings ensure candidates match the requirements for positions and background checks ensure we only hire candidates with the highest integrity standards. Our formal processes ensure only the top candidates are selected.

Measurement and Feedback Systems

An important foundation of our quality focus is our measurement system. Securus uses a variety of quantitative and qualitative information gathering tools to solicit feedback from customers in our quality improvement process. These tools include:

- **Transactional Surveys** – We survey customers after key events (e.g. installations, adds, moves, changes, repairs) to gather information on performance. Respondents rate their experience through 21 questions. A low rating (a 1 or 2 on a 5 point scale) on any single question requires a management review, immediate contact with the customer, and an action plan for improvement.
- **Relationship Survey** – We survey our customers periodically to understand if we are meeting their expectations. This survey specifically evaluates the performance of our customer operations and account management teams. Again, we ask 21 questions, and a low rating requires a management review, immediate contact with the customer, and an action plan for improvement.
- **User Groups** – Securus periodically sponsors user groups inviting customers to discuss their ideas and future development of our products and platforms. Operational and security challenges customers brought to Securus are at the heart of many of our patented innovations.

These feedback mechanisms provide invaluable information and help Securus meet our customers' expectations.

System and Platform Design

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Software Development

The Securus use of information technology (IT) best practices, industry standard quality measurement tools, and strict environmental controls, ensure the highest system functionality and availability. The Securus development team uses the Waterfall Software Development Lifecycle (SDLC) to ensure high-quality deliverables. The feature/functionality enhancements process stages are:

- Analysis
- Design
- Development
- Quality Assurance
- Implementation
- Post Implementation Support

Each phase has specific deliverables and gates (controls) to ensure high quality and to minimize rework. Securus uses the following distinct system environments in conjunction with our SDLC:

- Development – Used by IT Development to create and unit test new enhancements
- Quality Assurance – Used by Quality Assurance Analysts to test and certify new enhancements and bug fixes
- Pre-Production – Used by Production Support to validate hot fixes for production, and for final validation and mock deployment of major functionality releases
- Production – Used by all Securus customers and accessible by only Securus Production Support and Tech Support

Each environment has access controls, and we use source code control systems to ensure the proper promotion of code and as a document repository.

Securus uses industry-standard HP Quality Center for defect tracking and follows a rigorous test cycle including:

- Verification of New Functionality – Ensures a feature is working as designed
- Load Testing – Determines the upper threshold or breaking point of the component or feature
- Performance Testing – Determines the expected user experience
- Regression Testing – Ensure all existing functionality still works as designed

- Exception Testing – Tests boundary conditions and unexpected usage scenarios

New releases typically create new functionality. Upon completion of the Quality Assurance stage, the code changes are packaged and deployed into our pre-production environment for the final end-to-end quality check, and to optimize the implementation. This effort enables Securus to minimize the maintenance window related to system changes.

Both IT and business stakeholders review and must approve all scheduled changes to production in two change control meetings to safeguard the stability of the production environment.

Upon implementation of new code into production, Securus Production Support, and IT Development monitor changes closely to minimize the impact of any adverse or unexpected system behavior.

This attention to detail allows Securus to build feature functionality that leads the industry in quality and performance. For example, the Securus three-way call detection feature has been proven to be more accurate than the same feature offered by competitors. Independent testing by an outside research and testing company proves it. Similarly, our voice biometric feature leads the industry in accuracy.

The voice quality available on our call platform provides near perfect fidelity. Customers have used information heard through background conversations to prevent and solve crimes.

Our quality control does not end with our system design but continues all the way through site installation. Securus and each customer develop a defined quality checklist to install the system in a manner that meets their unique operating requirements. As described and included with our installation plan, Securus uses quality control checkpoints for each phase of an installation:

- Quality Control Checkpoint 1 – Provisioning: After customer provisioning is complete, Securus technicians submit a quality control review to the Engineer, Project Manager, and Account Manager for the project.
- Quality Control Checkpoint 2 – Pre-Installation: While on-site, Securus Field Service Technicians complete a checklist to ensure that the physical installation characteristics meet or exceed Securus standards.
- Quality Control Checkpoint 3 – Equipment Testing/Functional Validation: Technicians complete test call scenarios and phone labels, call durations, on/off times, administrative terminals, and verify other customer configurations.
- Quality Control Checkpoint 4 – Acceptance: The Securus Project Team provides copies of all quality control documents, equipment inventory records, and

network diagrams. The Securus Project Team will host a review of these documents with CDOC.

These tools are used to verify that work is completed properly before moving to the next step in a process. Customers must indicate their satisfaction with a sign off moving to the next step in a process.

Internal Controls

Finally, Securus has developed the best internal controls in the industry to make sure we follow our processes and that our information is accurate and ensure its security. Securus access controls for all systems are internally audited for compliance with the Sarbanes–Oxley Act of 2002 (SOX), which set new or enhanced standards for all U.S. public company boards, management, and public accounting firms. This internal audit ensures CDOC will get accurate and timely reporting from Securus.

Securus also employs an internal audit team that constantly reviews and audits our systems and security procedures and verifies our performance compared to our standards.

B. Quality Control Plan Submission and Review

The Offeror will provide and maintain a comprehensive Quality Control Plan (QCP) acceptable to CDOC. To facilitate CDOC's QCP review process, the Offeror is responsible to submit its QCP:

i. The Quality Control Plan is negotiable and will be subject to approval by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Upon contract, Securus will work with CDOC to develop a comprehensive Quality Control Plan that is acceptable to the CDOC. That plan will be negotiable and will be subject to approval by the CDOC.

Elements of that plan are described above in Section 9, "Quality Assurance Program," A, "Quality Control Plan".

ii. Preapproval of any substantive changes in the Offerors quality control plan must be submitted in writing no later to the CDOC Principle Representative. A substantive change is defined as any change that directly affects the Offerors operations or quality management system. Examples of substantive changes include:

a. Significant changes to Offerors business operations,
b. Significant changes to the company's key management structure,
c. A new business operating system,
d. Significant changes to an existing system impacting operations,

e. A new process or procedure that considerably alters the way business operation are performed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All substantive changes to the plan, as listed in (a) through (e) included above, will be submitted to the CDOC for prior approval.

iii. An updated Quality Control Plan is due 30 days before each extension term.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide an updated Quality Control Plan 30 days before each extension term.

10. EMERGENCY PREPAREDNESS

A. To support continuity of operations during an emergency, including a pandemic, the Offeror is responsible to provide a plan for maintaining operations for an extended period of time. The plan should describe the Offerors strategy for providing critical services to the state in the event of such an emergency and put contingencies in place to provide needed goods and services.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus Disaster Recovery Plan is designed for rapid response with unmatched service and support in any circumstance. Our goal is to prevent or minimize down-time and remove your administrative burdens. Securus takes care of communications and technology while you take care of your population and facilities.

- Robust network architecture designed to mitigate issues before they occur
- Field service team readily positioned close to your facilities and on-call 24/7
- A plan for escalating issues, adding resources, and recovering quickly

If a natural disaster or other significant adverse event occurs, CDOC has the full support of the Securus Network Operations Center, the Securus Technical Support Team including engineering resources, and the Securus Field Service Team, including over 290 Field Service Team members with an average of seven years tenure, supported by a centralized field dispatch team. **Our Field Service Technicians are fully trained in our disaster recovery plan and processes**, and they are strategically positioned to support your ongoing maintenance and fast response in emergencies.

Response operations begin as soon as personnel safety is assured, and all emergency recovery operations are prioritized by critical facilities and equipment locations. For situations that are expansive in nature, we prioritize maximum-security sites and facilities with high offender phone usage.

Securus' Three-Tiered Approach to Disaster Response and Recovery

1. **Facility-Specific Emergency Response Checklists**
   For every facility, Securus develops an emergency response checklist to protect equipment and personnel in the event of an emergency. These procedures may be as simple as using sandbags to stabilize equipment and placing tape on windows exposed to high winds. Your checklists will focus on mitigation and recovery with contingencies for extreme conditions such as earthquakes, flash floods, power outages, etc. Each checklist will be coordinated with CDOC for consistency with your policy and procedures.
2. **Systemwide Disaster Response Plan**
   Securus works with you to declare emergencies for situations that are

catastrophic and may impact a localized area or wide-spread region. Recovery plans are triaged based on the extent of impact and recovery operations may last a few hours, days, or weeks. Securus prioritizes recovery of premise-based equipment by facility type and equipment location. The Securus Local Recovery Team will continue recovery operations until operations are restored. Retrospective reports are completed for all declared emergencies to advance our emergency recovery planning efforts for the future.

3. **A Foundation of Network and Equipment Preventative Measures CDOC avoids many communications-related disasters because we are prepared:** Securus provides a network and infrastructure tested to withstand adverse conditions, minimize outages, and protect your data. We research what works and then we implement continuous improvements. Securus adds layers of redundancy at the local and national level to our core network and operations centers. We stock your facility and our Field Service Team with spare parts. We back up your data at three geographically diverse Securus data centers and layer redundancy throughout each component of our network. Information is routed through geographically diverse and route-diverse network paths, all while we monitor operations and communications 24x7x365.

Additional details on the Securus Disaster Recovery Plan and our preventative measures are outlined on the following pages. It's difficult to contemplate every contingency, but with 30+ years of experience providing communications and technology services to the corrections industry, **Securus has the experience to take care of CDOC even when the unexpected occurs.**

CDOC Emergency Condition Declaration

If you encounter a catastrophic adverse event or disaster at your facility, immediately call the Securus Emergency Numbers that you are provided. Your call will be answered 24x7x365. Then with your Securus Account Manager you will request that Securus General Manager declare an emergency condition. Operations management then establishes an immediate conference bridge with the appropriate participants to gather information substantiating that an emergency status is warranted and determines the Disaster Level.

Securus classifies disasters on a Disaster Level Scale of 1-3:

- Level 1 Disasters are catastrophic events that are extremely wide-spread and affect many facilities and many customers.

- Level 2 Disasters are high-impact and affects a more wide-spread area than Level 3.
- Level 3 Disasters are moderate impact disasters typically affecting a localized area or specific facility with consideration that elevation of level may be needed.

A single event trouble ticket is used to track all recovery efforts. The Securus Technical Support Team will open a new trouble ticket in our ticket tracking system, indicating the declared condition level and the date and time of the declaration. All open tickets pertaining to the ongoing emergency recovery effort will be linked so that all recovery efforts are tracked as a single incident to facilitate complete resolution. This is critical for efficient and complete resolution in situations of extended recovery.

If needed, Securus will deploy and pull resources from our nationwide network and engage our vendors to supply additional resources, equipment, or manpower.

Securus Emergency Response Disaster Levels

Disaster Level 1

Securus provides a full-headquarters response and may deploy a Headquarters Response Team to the region to coordinate and assist local recovery efforts. Securus Local Recovery Team activated, and your Account Manager will work with you to initiate a Command Center, including Securus Leadership. Necessary skill levels and geographic proximity are matched to your site's needs; additional personnel are dispatched as needed.

Disaster Level 2

Securus Headquarters Response Team assists Securus Local Recovery Team as needed; onsite technician requirements assessed, and additional personnel dispatched as and when needed.

Disaster Level 3

Securus Local Recovery Team coordinates all recovery operations. Headquarters assistance beyond standard Network Operations and Technical Support Teams likely not required.

Risk Mitigation and Proactive Monitoring

The Securus Network Operations Center (NOC) continuously monitors all data centers, infrastructure components, platform systems, and network/communication systems using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.



The Securus NOC also monitors real-time video surveillance and environmental alerts for the Securus data centers. In the event there is an issue at the Securus Network Operations Center, Securus maintains a fully redundant backup Network Operations Center at a separate physical location.

The Securus Technical Support Team monitors all facility-based equipment and connectivity 24x7x365 including firewalls, integrated access devices (IADs), visitation phone monitoring (VPM) units, routers, switches, on-site systems, wireless access points, user interfacing kiosks and terminals, and uninterrupted power supply (UPS) systems.

The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. In addition to real-time monitoring and alerting, Securus Technical Support also leverages network performance monitor tools to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. This ongoing, proactive, in-depth analysis of your systems' performance enables our Technical Support Team to prevent and mitigate facility issues.

Data storage redundancy is a key component of Securus' Risk Mitigation and Disaster Recovery Plan. Securus maintains three data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.995% availability.



Securus' data centers meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier III, with some Tier IV (highest level) attributes, for data centers including:

- ability to withstand a 96-hour power event
- multi-layer physical security
- multiple power delivery paths

Each data center has redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity.

Securus' data centers are staffed 24x7x365 for immediate physical assistance inside the data center.

Data is no longer susceptible to loss due to an individual drive failure or issues at your location: The Securus communication platform uses technology that is much more advanced than traditional local onsite storage. Securus uses a mix of Storage Area Network (SAN)—a high-speed sub-network of shared storage devices—and Network-Attached Storage (NAS). This architecture avails all storage devices to all servers on Local Area Networks (LANs) or Wide Area Networks (WANs). Data is stored in Redundant Arrays of Independent Disk (RAID) formats, spreading the data across multiple drives, which provides additional protection. Accordingly, this architecture provide facilities with the ultimate protection against single drive or server failures, as well as increased security. **Securus maintains hardware replacement inventory on your site, in our Field Service Team vehicles, and at centralized locations.** In addition, we have distribution agreements with our vendors so that in the event of disaster recovery efforts, we can get replacement equipment to your facilities quickly.

Localized Event Affecting Only Securus Facilities

In the event of a disaster impacting Securus, the local Securus Network and systems, or NextGen SCP, Securus immediately assembles a team of engineers to investigate and

restore services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and a list of third-party vendors to engage if needed. Our priority is fast resolution and minimal downtime. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Upon confirmation of a service-impacting event, the Network Operations Center will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

The Securus Executive Team and the Securus Account Management Team receive SIRs and communicate with you directly. In addition, the Securus Technical Support Team may communicate a service-impacting event via a splash screen on the NextGen SCP user interface introductory page. Securus updates you regularly throughout resolution. Securus investigates every service-impacting event, completes a root-cause analysis, and provides the analysis to you upon request.

Securus – A Case Study in Swift Recovery

In 2015, weeks of thunderstorms impacted the Dallas metroplex where two Securus data centers are located. Lighting struck a Securus data center and damaged the equipment cooling units. Normally, this would have been restored within minutes, but the roads leading to the data center were closed due to flooding and caused an extended recovery response time. The equipment in the data center rapidly overheated and began to fail. More than a quarter million dollars of components suffered fatal damage and needed replacement. Even with this compounding event, calling services were restored the same day for most facilities, and there was no loss of customer data, investigative data, or recordings.

B. Offeror is expected to include proposed emergency preparedness plan with their proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has designed and implemented a robust network architecture that provides for emergency preparedness and quick disaster recovery, minimizing downtime for the Securus platform and its customers. Securus has demonstrated its ability to recover efficiently under extreme circumstances, restoring service to our customers with no data loss.

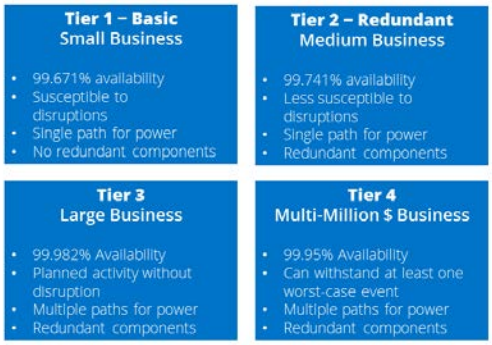
Risk Mitigation

Securus has implemented a platform and infrastructure designed to minimize potential outages and protect customer data. Multiple data centers, diverse network paths, redundant platform systems, and proactive monitoring mitigate the majority of risks.

Data Centers

Securus maintains a presence in three data centers in three geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.95% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier IV (highest availability) data centers including:

- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security
- Multiple power delivery paths.



TIA-942 Infrastructure standards for data centers
Telecommunications Industry Association

Also, Securus data centers have redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity. Securus data centers are staffed 24x7x365 for immediate physical assistance inside the data center.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in; dual-door authentication (card and biometric); and a mantrap (interlocking door controller) at the data center suite entrance.

Redundancy

Redundancy is a key component of the Next Generation Secure Call Platform (NG SCP). While operating on a single platform, Securus' NG SCP runs on duplicate environments in separate data centers in Atlanta, Georgia, and Dallas, Texas. Each component has N+1 redundancy, meaning that a failure of any one component does not result in downtime because there is a backup available to resume its function. In addition to the inherent redundancy of SCP, Securus has also designed redundancy into all support systems, either through N+ 1 configuration, database clusters, virtual machines, load balancing, or other failover methods. All network transport has redundant network equipment and routing to allow traffic to reroute in the event of a failure.

The NG SCP platforms in Dallas and Atlanta were designed and built to the same specifications. This standardization allows re-homing of systems from their primary data center to an alternate data center in the event of a failure.

All circuits coming into Securus data centers use multiple diverse carriers, including the interconnections between data centers. In the event of a failure, traffic will reroute across a redundant circuit or path. In addition, Securus uses multiple carriers for offender calls from the NGSCP platform. Calls to family and friends will immediately reroute upon failure of any carrier.

Securus uses multiple methods of storage to minimize the risk of data loss. All critical systems and data are backed up at regularly scheduled intervals and stored offsite for retrieval, if needed. In addition to offsite storage, Securus replicates voice clips, call recordings, and validation data between the data centers.

Securus uses industry-leading vendors for all platform and network hardware, including Dell, Cisco, Oracle, EMC, Big IP, and Intel. In addition to the redundancy designed into the platform and network, Securus also maintains a spare parts inventory onsite at each of our data centers to expedite repair of a failed component. Securus also maintains premium-level support contracts with each vendor that define stringent service level agreements in case of a failure.

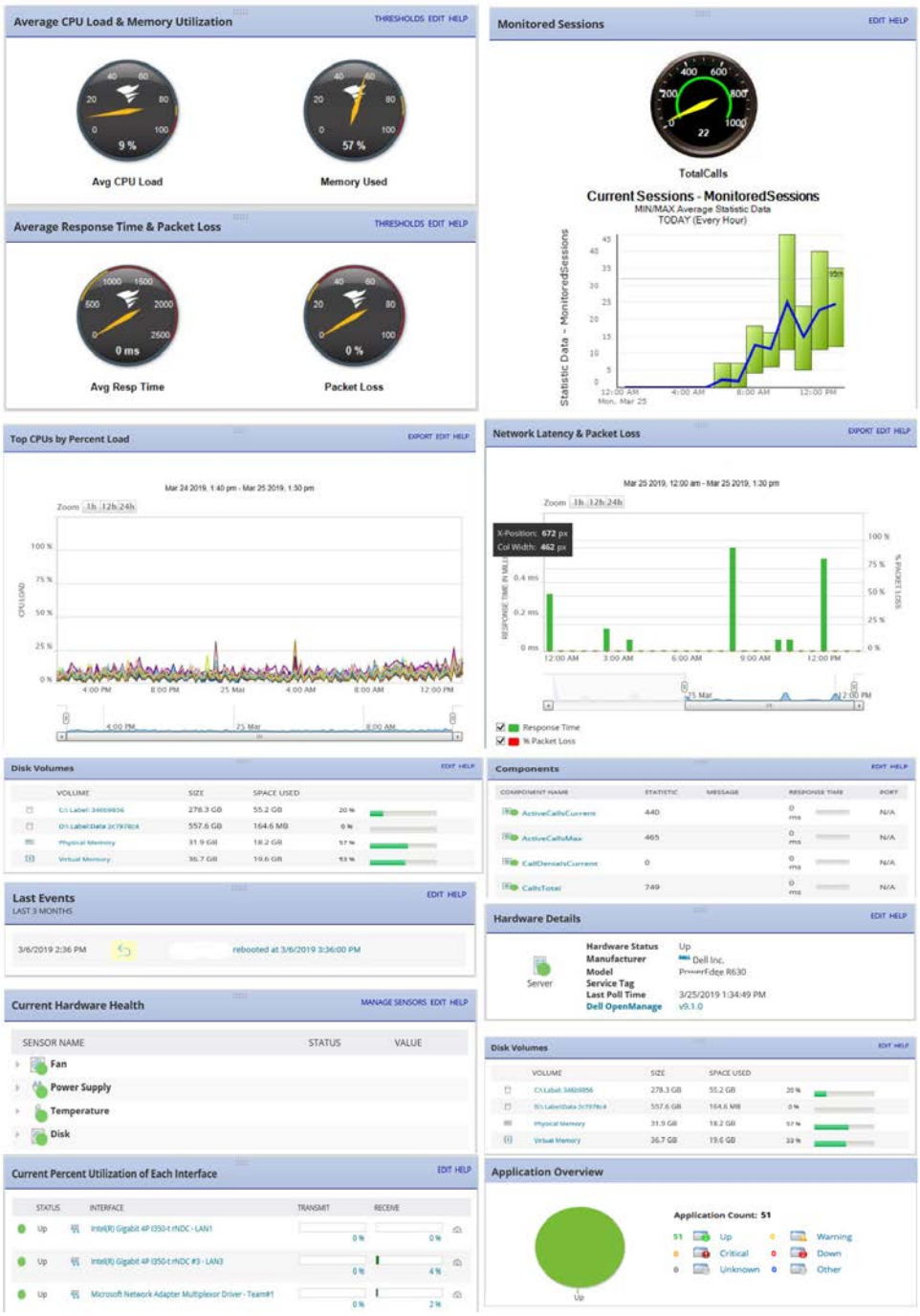
Securus maintains an inventory of spare parts for our facility-based components at our headquarters in Dallas, Texas, and has distribution agreements with multiple vendors to provide expedited national delivery service. The corporate headquarters maintains a standardized emergency recovery package of frequently used spare parts and equipment that will be available for shipment to support restoration efforts at our customer sites. Our technical field representatives located throughout the country also carry an inventory of the most commonly needed spare parts. With spare parts on board our service vehicles, most facility-based equipment malfunctions can be resolved with a single site visit.

Proactive Monitoring

Data Centers and Network

Securus continuously monitors all data centers, infrastructure components, platform systems, and offender telephone systems (OTS) using the SolarWinds® suite of network performance monitors. The SolarWinds performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including SCP, network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system- and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.



SolarWinds® Typical Monitored System and Application Elements

Securus Primary Network Operations Center

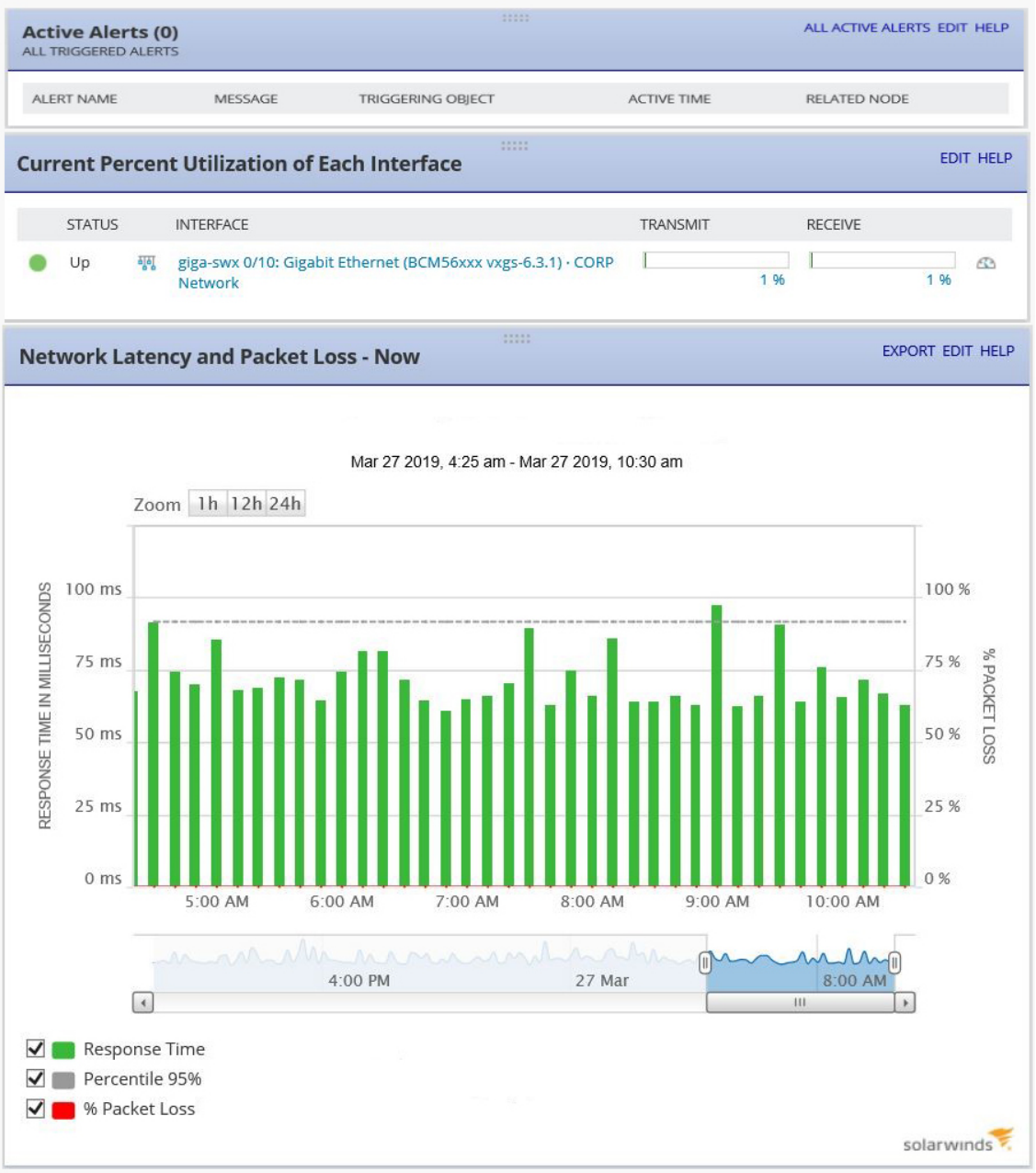


Securus Network Operations Center



Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including integrated access devices (IADs), visitation phone monitoring (VPM) units, switches, and uninterrupted power supply (UPS) systems. The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.



SolarWinds® Device Monitoring Example (Bandwidth & Network Latency)

In addition to real-time monitoring and alerting, Securus technical support also leverages the SolarWinds network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the technical support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Restoration

Platform and Network

In the event of a disaster impacting NG SCP or our network, Securus immediately assembles a team of engineers to begin investigation and restoration of services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and will also engage third party vendors, if required. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Facility-Installed Systems

Securus prioritizes recovery of premise-based equipment by facility type and equipment location. Maximum-security institutions and institutions with high offender phone usage receive priority. Prioritization also considers customer requirements and preferences. Securus has developed procedures and checklists to protect personnel and equipment in the event of an emergency situation. Securus will combine headquarters and field staff efforts to expedite service recovery wherever possible. Securus coordinates each checklist to ensure compliance with each facility's guidelines.

Securus has a field support department with more than 165 field service associates supported by a centralized field dispatch team. The Field Service Technicians (FST) are strategically located to support ongoing maintenance, as well as any disaster recovery situations. The FSTs are supported by senior technical support resources and engineering to expedite repairs and minimize customer downtime.

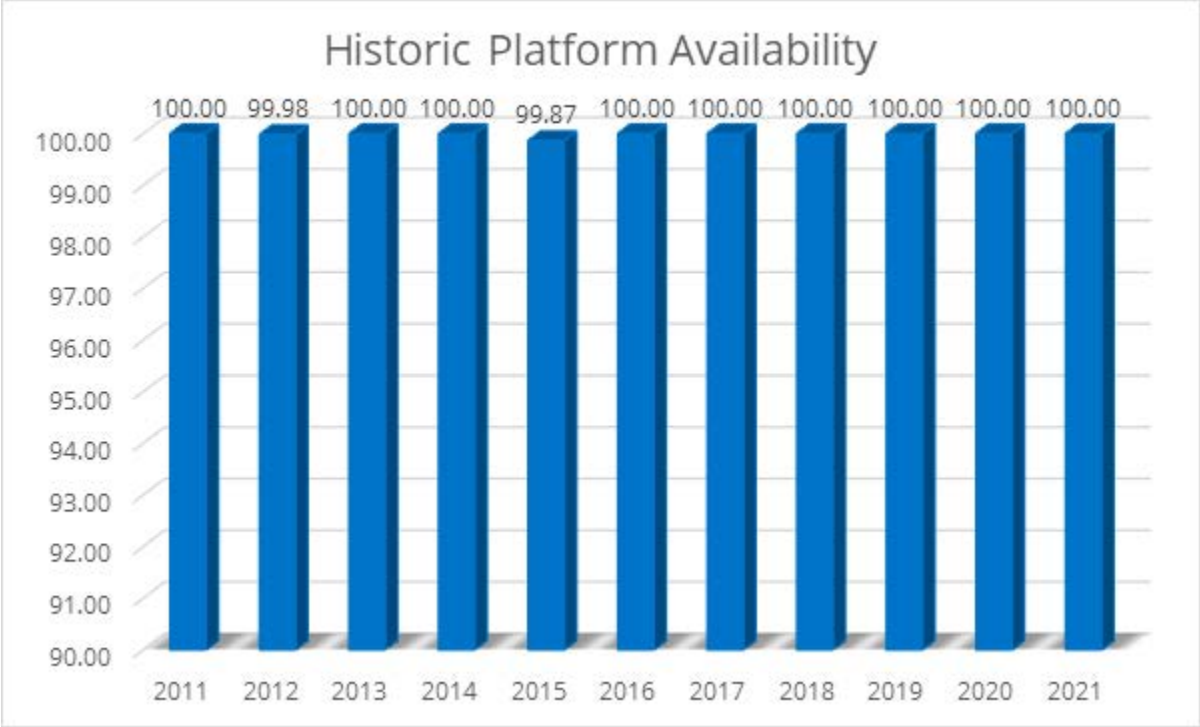
Reporting

Upon confirmation of a service-impacting event, the NOC will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

Customer contact personnel receive SIRs, so they can communicate with customer facilities proactively or reactively as required by the facility. In addition, technical support may communicate a service-impacting event via a splash screen on the SCP user interface introductory page, whenever possible. Regular updates ensure that the information provided is always current. Securus executives also receive all SIRs, so they are aware of all customer-impacting events.

The NOC will issue a final SIR upon issue resolution. Securus investigates each incident and completes a root-cause analysis (RCA) following all service-impacting events. After the root cause is determined, Securus makes RCA documents available to customers upon request.

Performance



The NG SCP is one the most stable calling platforms in the industry, with nearly perfect, 100% availability. Through design, proactive monitoring, and rapid-response procedures, Securus minimizes customer-impacting outages. Data storage with multiple layers of redundancy minimizes the risk of losing critical data and recordings.

When disasters strike, Securus responds quickly and methodically to ensure the fastest restoration of service possible. And we have been tested.

In the spring of 2015, the Dallas, Texas, area, home to two Securus data centers, was impacted by weeks of significant storms, resulting in 27 deaths and more than one billion dollars of property damage due to flooding. Early one morning, lighting struck a Securus data center, damaging cooling units. Normally, this cooling would have been restored within minutes, but the roads leading to the data center were closed due to flooding, which caused a longer response time for service technicians. Securus' equipment rapidly overheated and began to fail. More than a quarter million dollars of components suffered fatal damage and needed replacement. Even with this once-in-a-lifetime series of compounding events**, calling services were restored the same day** for most facilities, and **there was no loss of customer data, investigative data, or recordings**.

C. CDOC anticipates meeting with the Offeror twice a year to review the Offerors emergency preparedness plan and develop contingency plans.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will meet with the CDOC twice a year to review the Emergency Preparedness Plan and develop contingency plans to take in local and current concerns.

11. DELIVERABLES

CDOC anticipates the deliverables listed in section XXXVI, Table of Contract Deliverables will be due under the contract. In addition to the official designated in Table Under "Deliver to," the Offeror will submit a copy of each deliverable to the CDOC Principal Representative in the contract. CDOC anticipates Offerors to propose other applicable deliverables to be negotiated.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus agrees to support the deliverables listed in section XXXVI, Table for Contract Deliverables, and will work with authorized CDOC personnel to ensure they are included in the final contract.

12. PERFORMANCE MEASURES

A. The performance measures agreed to during negotiations and accepted by CDOC will apply to the services provided under this contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will comply with all performance measures stipulated under this contract.

B. At a minimum, the Offeror is expected to maintain the baseline rate for the performance measures.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will maintain the baseline rate for the performance measures.

C. The contract may be amended, in subsequent years, by mutual agreement of the parties to add additional performance measures to the Contract, amend existing performance measures, or discontinue performance measures where they are deemed to be no longer necessary.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands that the contract may be amended, in subsequent years, by mutual agreement of the parties to add additional performance measures to the Contract, amend existing performance measures, or discontinue performance measures where they are deemed to be no longer necessary.

D. The Offeror will submit a Performance Measures Report with their proposal, and each quarter as required by section 6 of the contract, Reporting – Notification, paragraph A, Quarterly Reports.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will submit a quarterly Performance Measures Report that complies with the measurements and deliverables agreed to in the contract.

We have included a sample Quarterly Performance Measures Report in **Securus Attachment No. 7, Sample Quarterly Performance Report.**

E. Corrective Action Plan

i. Upon request of the CDOC, the Offeror is responsible to prepare and implement a corrective action plan (CAP) within 30 calendar days for each metric that falls below the target or threshold.

ii. CDOC anticipates CAPs will be provided in a standardized format throughout the contract and specify the following information:

a. Compliance criteria

b. Percent of compliance
c. Specific description of deficiency
d. Timeframe for corrective action
e. Owner responsible for corrective action
f. Completion date

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus looks forward to working closely with CDOC personnel to ensure complete satisfaction with the services we offer. Upon request of the CDOC, Securus will work with your personnel to prepare and implement a Corrective Action Plan (CAP) within 30 days for each metric that falls below the target or threshold. We understand these CAPs will follow a standardized format throughout the contract and will contain the following information:

a. Compliance criteria
b. Percent of compliance
c. Specific description of deficiency
d. Timeframe for corrective action
e. Owner responsible for corrective action
f. Completion date

13. KIOSKS

A. Kiosk Types

i. Turnkey Kiosks – all hardware and software necessary to provide any related services the Offeror provides. Should include locked down operating systems, security patches, remote monitoring and software upgrade, network security, application hosting on dedicated cloud services and secure data center.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All hardware and software necessary to provide any related services Securus provides will be provided by Securus at no cost to the CDOC. This includes locked down operating systems, security patches, remote monitoring and software upgrade, network security, application hosting on dedicated cloud services and secure data center.

ii. Hardware Only Kiosk – all related hardware as needed to implement the kiosk solution. Kiosks should contain a touch screen; however, a durable security centered keyboard will also be considered, especially supporting disabled offenders who could not access the kiosks.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will include all related hardware needed to implement the kiosk solution. The kiosk hardware, including screens, are designed for a corrections environment will be capable of supporting disabled offenders.

a. If proposing this type of kiosk, the Offeror is responsible for the work, with a sub-contractor(s) as needed to complete the installation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. Kiosk Applications Email/Secure Messaging

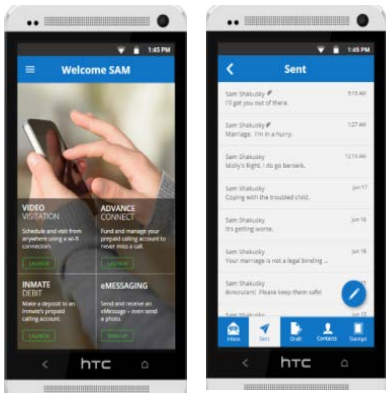
i. Electronic mail service, including restrictions of senders and receivers

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus eMessaging™ is the most widely used messaging platform in the corrections industry. CDOC has control of who uses the system and what messages are permitted.

- Facilitates electronic communication at **no cost** to the CDOC
- Increases investigative data and analysis with all digital review
- Implements easily with existing facility network connectivity and hardware
- Prevents offenders from sending messages to other offenders at your facility or any other facility

Inexpensive, user-friendly options to maintain connections without sacrificing security: Securus eMessaging™ is an easy way for friends and family to stay in touch using the free Securus App or on the Securus website. Both provide a high-level of security for communication entering your facility. Friends and family purchase stamps that are used to send eMessages with the option of using an additional stamp to attach an eCard, photo, or video.



- **Stamp Packages** may be purchased by an offender using their Securus Debit Account and by friends and family using a credit or debit card. Once the Stamp Packages are purchased, they may be used to send messages, transfer stamps to an offender for their use, and to pre-pay for a return message from an offender.
- **Snap n' Send™** gives friends and family a tool to send just a photo for one stamp. It's an easy way for friends and family to share photos from their phone or photos snapped at family celebrations, kids sporting events, or just because.



- **eCards**, like traditional greeting cards, celebrate life events and holidays with pre-worded, uneditable messages. An offender or friends and family may send eCards for the cost of just one stamp.
- **VideoGrams** are a convenient way to send 30 second videos from the Securus App for Android and iOS mobile devices. The Securus App automatically crops longer videos with no extra steps.

Friends & Family Access

The faster way to write an incarcerated individual. For staying in touch, nothing beats the speed and convenience of email. Securus eMessaging™ service is a fast, feature-rich way to correspond with your incarcerated loved one. Depending on the facility, offenders may be able to respond electronically, view and print your message, and view photo attachments.

Mail made easy Securus eMessaging™ correctional email service is faster than regular mail, with individuals usually receiving emails within 48 hours. Each email requires a "Stamp," often available at more affordable rates than traditional postage, and can be purchased online.

Functionality you can use In many locations, you can attach a photo to an email, or even record a 30-second VideoGram to send along with your letter. With these popular and convenient services, Securus eMessaging™ is using technology to keep you and your friend or relative connected throughout the duration of their incarceration. The email interface for the offender is as familiar as the email program you use at home, and just as easy to use.

Helping you stay connected, we know that getting that letter from your loved one in your inbox is one of the best feelings in the world, and we want you to have that feeling again and again.

eMessaging Facility Portal

Reduced administrative burden: Securus eMessaging™ is an advanced, digital investigation option that reduces offender administrative burden while increasing your control over communication and content. Our centralized, proprietary platform is managed wholly within the United States and can be configured to match CDOC goals. The Securus eMessaging™ Facility Portal is where you choose the level of review by choosing security controls. Then as eMessages are processed, if none of your security controls are triggered, the eMessages "Auto Release." If your security controls are triggered, then you have an opportunity to review the flags and approve/reject the message. Each eMessage that is rejected generates an automatic, free message to the offender or family and friend sender advising that their message was not forwarded with a stated reason.

Offender Access

Using a Securus Tablet or the ConnectUs eMessaging module on the Securus ConnectUs Terminal, an offender can retrieve eMessages sent by friends and family. At log-in, there is an indicator that shows an eMessage is available and once opened it clearly shows if there is a photo, eCard, or Video attached. The offender can reply to the sender by using a stamp they purchased using their Securus Debit Account, a stamp that was transferred to them, or a stamp that was paid for by the sender and attached to the incoming eMessage.

All eMessages, photos, eCards, and VideoGrams are displayed on the terminal or tablet in an eMessage inbox with no paper distribution. There is no Draft folder for the offender and the Sent folder may be deactivated by CDOC.



Since 2010, Securus' subsidiary JPay has partnered with CDOC to provide communications services that kept loved ones connected, so there is familiarity with both the Friends & Family interface and the Facility interface.

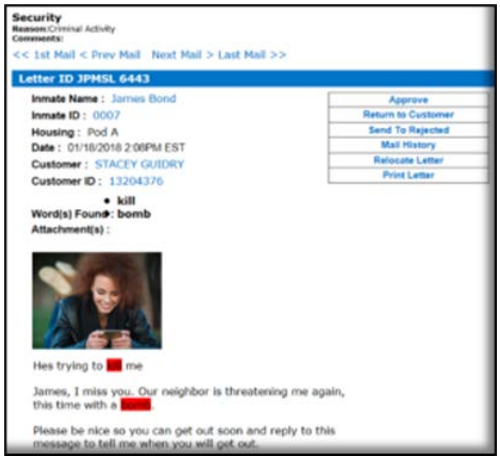
ii. Keyword search capabilities on both incoming and outgoing messages.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Minimize time and maximize results with automated screening: The Securus eMessaging Facility Portal allows you to view and analyze the complete mail history of any sender. Intuitive reporting and views provide a complete message history by offender, and the ability to search messages by offender, family and friend, date, specific message, and word filter list. Use this tool for timely identification and evaluation of big-picture communication issues so you can proactively address.

All messages and photos are retained for the term of the contract, even if they are rejected or deleted by recipients. An additional benefit--as electronic communication increases, you can redeploy mailroom resources to other agency tasks.

- **Photo Review:** Photo Review is efficient using the Facility Portal's Photo Review Folder. If photos are outside CDOC photo policy, you may remove them (individually or as a group) from the message while allowing the message and acceptable photos to be delivered. The sender receives a notification that a photo was removed. All photos that were removed remain associated to the message and are accessible to CDOC. The Facility Portal logs capture both the date and the staff member for each removed photo.



- **Word Watch:** The word watch filters automatically screen and flag for review all incoming and outgoing messages that include a word on the CDOC Word Watch List. The flagged words will appear in red at the top of the message for fast review. You may modify the Word Watch List at any time to align with trends in coded speech phrases or buzz words.
- **Watch Lists** allow CDOC to flag for review all communications from designated individuals in your population and/or their friends and family. You may modify the Watch List at any time.
- **E messaging Suspension:** This feature allows you to stop all communications to any individual using the system. Pop-up notifications alert senders if they are suspended or if the intended recipient is suspended. Each suspension and reactivation action for an offender is logged with staff name, date, and reason for the status change; suspensions may be modified at any time.

iii. Keyword search may be edited at any time.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With Securus, Agency administrators can create, maintain, and modify keyword searches through Word Watch and Watch Lists via the admin portal. These customizable keywords and lists can be modified at any time to capture the agency's current investigative trends.

iv. Capability for the CDOC to manage email approvals at either a facility level and the State level.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Determining whether email approvals are managed at a facility level and/or State level is a CDOC policy that Securus is able to accommodate.

v. Incoming photo messages/attachments

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Family and friends can send only a photo to their incarcerated loved ones through Snap N' Send™ or family and friends can send photos as an attachment to an E-message. To ensure safety and security, the agency can review and approve all photo messages received through Snap N' Send™ and E-messaging.

vi. System may allow for separate viewing of messages and photos as well as the ability to reject/accept any combination of messages and photos.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As is the case with Securus photo and messaging services, CDOC can customize some video message settings to meet policy requirements.

vii. Incoming video messages/attachments

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Family and friends can easily send a 30-second video to their incarcerated loved one through VideoGrams.

viii. System may allow for separate viewing of messages and videos as well as the ability to reject/accept any combination of messages and videos.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Messages and videos allow for separate viewing as well as the ability to reject/accept any combination of messages and videos.

ix. Offender email is expected to be storable by Offeror and accessible by the CDOC network.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The CDOC can access historical emails for the length of its contract with Securus.

x. Offeror to describe estimated impact of email/messaging on the CDOC network.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

We install a Securus-owned and maintained network to support all the products and services we provide. Therefore, there is no impact to the CDOC network.

What's more, our hassle-free services go beyond reducing the impact to the CDOC's network. Our digital messaging services have a downstream impact by reducing the amount of physical mail a facility receives. In turn, this lowers the chances of introducing contraband to your facilities.

xi. Provide a plan for data lines should capabilities at the facilities be limited as a result of this implementation, at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus implementation will be supported by Securus owned and maintained network. Site profiles will provide guidance to ensure no data lines will be limited as a result of this implementation.

xii. Offeror to describe file size limitations, if any.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

We want offenders to have easy access to their digital communications. That's why we support large file sizes. Here's a look at how we handle file sizes:

- eMessaging – message length is configurable by the agency.
- Attachments – system utilizes compression and/or conversion of the attachments.

Even though we support large files sizes as part of our standard offer, we know that some Agencies might prefer to limit those capabilities. That's why we allow agencies the ability to customize the length of emails based on their preferences. We'll work together during implementation to apply any desired messaging limitations.

xiii. Offeror to provide both electronic viewing of messages and the ability for CDOC to print messages and photos. For printing, the Offeror is to supply printers and consumables including toner and paper at no additional cost.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Another great thing about Securus' digital communication services is that emails can be viewed and accessed through a tablet or via the admin portal at any time. This digital access to communication reduces the need to print hard-copy messages. Not only does this decrease the administrative burden for Agency employees, but it also saves time and is more efficient.

For Agencies who still wish to print hard-copy messages, Securus will provide one (1) printer per facility at no additional cost. This printer and Securus provided toner and paper is reserved for the printing of messages rendered from Securus services only.

xiv. Offeror to describe the process for CDOC to order printing supplies.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with authorized CDOC personnel to incorporate the inventory, storage, and ordering of printing supplies.

xv. Offeror to submit a plan on how the toner will be recycled.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with CDOC personnel to follow CDOC guidelines on toner recycling and ensure recycling policies and laws are followed. This plan will be developed in conjunction with CDOC personnel.

xvi. The Offeror will describe the ability for CDOC staff to track, research and investigate messaging history by various factors including, but not limited to, send date, sender, recipient, etc.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Identify trends, investigate suspicious activities, and manage usage: The NextGen SCP retains communication detail records on all communication attempts and events. NextGen SCP has a report writer that provides investigative information based on the communication detail records. CDOC may search and analyze details on all communication events through NextGen SCP and then run reports to identify communication trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

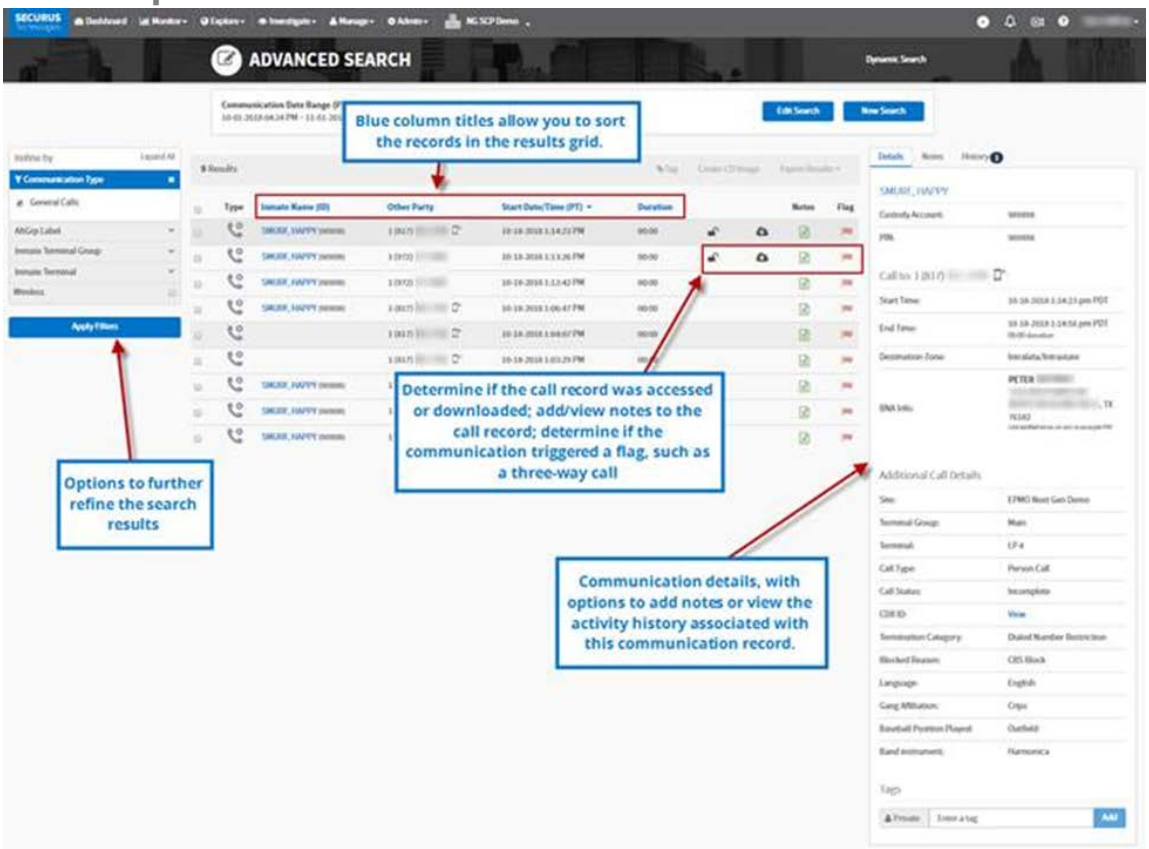
Custom and standard searches worth sharing: NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on an extensive list of criteria options. CDOC also may create customized reports by changing search criteria. After search results are generated, you can sort based on any of the communication event details. Then, with a single click, the data exports to Excel, CSV (Comma Separated Values), or Adobe PDF format and may be saved, printed, or emailed to others.

NextGen SCP™ Report Criteria Fields
▪ Date Range
▪ Identifier (ID, PIN, Name)
▪ Continuous Voice Identification
▪ Communication Type (Calls and Video)
▪ Communication Status (Complete or Incomplete)
▪ Prepaid Account Number
▪ Destination Number (Partial or Full Number Entry)
▪ Call Type
▪ Three-Way or Remote Call Forwarding Detected
▪ Watched Status
▪ Wireless Indicator
▪ Visitor and Visit Type (SVC)
▪ Visitor Contact Number
▪ Visitor Identifier (ID, Name, Email)
▪ Phone or Terminal Location
▪ Number Restriction and/or Status Assignment

NextGen SCP™ Report Criteria Fields

- Broad Search with No Data Entry
- Suspected Fraudulent Call Activity
- Destination Zone (Local, Interlata, Interstate, Intralata, International)

Sample Communication Detail Results Screen



xvii. Offeror will provide technology to restrict offender to offender communication.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Offender-to-Offender communication is a long-standing problem of which the frequency and severity has been nearly impossible to determine. Correctional facilities understand this problem, but have no means to solve it. Others believe the problem doesn't even exist. The reality is: **offender-to-offender communication is real, happening all over the country, and can now be identified**.

Every day, we learn about instances of major crimes being solved because of the increasingly cooperative efforts among state and federal agencies that are beginning to share case-critical data around the United States. In the world of offender phone calls, we offer cutting-edge technology based on state-of-the-art, patent-pending, call-matching technology that identifies Offender to Offender communications even when it's between two different correctional facilities across the country.

Although illegal Offender to Offender events are identified in this scenario and details are provided to each agency regarding their leg of the call, the details of the other agency's event, such as names and telephone numbers, remain confidential unless both correctional facilities agree to share such information on an event-by-event basis. This unique information-sharing model ensures data remains secure while also providing enhanced information when needed. Securus serves more than 1,200 correctional facilities around the country where ICER events can be identified, and we have identified ITIC events within all 1,200 facilities.

Offenders are continually finding creative ways to speak to each other using the offender phone system, and ICER listens to and identifies all of these illegal communication events. Whether two offenders are calling an accomplice on the outside who is verbally relaying messages, or the accomplice has two speakerphones to coordinate gang conference calls, ICER identifies all of these scenarios and proactively notifies all authorized corrections staff of the event and provides details that can quickly and easily be traced back to a specific call. This call can then be listened to through Securus' industry-leading platform.

The Threat

Offenders have been and continue to communicate with each other over the telephone systems that have been provided for their controlled contact with the outside world.

Before ICER, Offender to Offender communications were essentially undetectable due to no practical technology or uniform networking capability to identify such communications.

Highlights of the offender-to-offender communication threat include:

- Offenders use a variety of methods to go undetected when communicating with an offender, whether that offender is in a neighboring pod, a separate facility within the same state, or in a different state. Offenders exploit conference bridges, Google Voice™, and other forms of modern telecommunications technology. In addition, they rely on called parties to bridge the calls, place three-way calls, or put two speaker phones in proximity to one another, so that offenders can talk to other offenders without being detected.

- Until recently, Offender to Offender communication events were only found when accidentally stumbled upon by correctional staff. Events are known to occur with much greater frequency than previously known.
- These illegal communications enable criminal activities to occur, including coordinating gang-related murders, human trafficking, drug trafficking, racketeering, and offender disturbances at multiple correctional facilities around the country.

How ICER Events Occur

ICER events can occur in any of the following ways:

- Three-way calling
- Manually bridged calls
- Automatic bridges
- Speaker phones
- Relaying messages in real time
- Using Google Voice

Common Element: Called Party Involvement

How ICER Works

ICER uses advanced voice analysis technology to generate a call signature—a representation of the call that does not involve any of the original audio—for each completed offender telephone call. Call signatures are then automatically encrypted and transmitted to the central data center for analysis. Because none of the original audio is used in a call signature, the ICER system is in full compliance with state laws regarding the transmission of call recordings. Under normal operations, call signatures are created, transmitted, and received at the data center for each completed call. Upon arrival, the call signature is immediately analyzed and checked against other call signatures. If an Offender to Offender communications event is detected, it is logged in the ICER system database and investigators from the participating corrections administration are automatically alerted via email to log into the ICER system for the detailed report. To protect certain elements of offender data from being displayed to participating agencies, both parties must provide online consent before details of the full report are made available. The ICER system doesn't require correctional facilities to transmit audio files and each agency is always in complete control of the level of sensitivity of any data transferred.

xviii. Offender Commissary

a. Place canteen orders on the ITS utilizing interactive voice recognition technology with the capability to automatically transfer data between CDOC's Canteen management system and the Offerors system.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus Commissary Order by Phone product allows offenders to order items from commissary vendors by using the same offender telephones they use to place calls to friends and family members. This product saves facility staff the time processing commissary orders and handling order complaints. Commissary Order by Phone frees your staff to focus on important activities like safety and security. Your facility will see an increase in sales of commissary items by offering an additional point of sale.

Offenders can place orders at the time and frequency needed, using Commissary Order by Phone. The ordering process is convenient, easy, and accessible, and does not require facility staff. To place an order, offenders go to any offender telephone and dial a designated number. The call then connects to the commissary vendor's IVR where the offender places their order by following the voice prompts and pressing keys on the phone keypad.

Commissaries also benefit from Commissary Order by Phone—it provides another point-of-sale that increases commissary revenue and improves inventory turnover.

ConnectUs Commissary Ordering

ConnectUs-enabled devices continue to be of great use even when telephone and video session hours have passed. Offenders can place commissary orders from the same devices they use to place a call or view the offender handbook. Securus has multiple integration options to display a third-party vendor's application or integrate directly with your jail. Publishing a commissary application can have an immediate impact on your bottom line. Securus works with any willing commissary company to enable the access through our terminals. We have active agreements with many commissary companies.

ConnectUs Home Page



Benefits

- Eliminate the need to have multiple types of offender terminals or kiosks
- Increase efficiency by fully automating the commissary ordering process
- Maintain control of the integration and ensure that offenders are not able to access unsecure IP addresses once in the third-party application

b. View commissary account balances

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Commissary account balances are provided by the commissary provider, who is tied into the agency trust/banking and they would provide the current balance of funds. As such, the display of that would be provided by the commissary provider. Securus' integration allows the offender to see information provided by the commissary.

xix. Video Visitation

a. Expectations for data transfer for video visitation are as follows:

b. System will be able to manage visits of various types (i.e., video, face-to- face, contact, etc.).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Video Connect™ (SVC) is a web-based visual communication system that allows friends, family members, and attorneys to schedule and participate in video sessions with an offender—from anywhere with internet access—using a smartphone, tablet, or PC with internet access. Remote video communication provides family and friends with limitless opportunities to connect with a loved one by sharing everyday events like celebrating birthdays, reviewing homework, watching cartoons with their kids, attending a concert, and opening presents on Christmas. Many studies show a link between individuals maintaining relationships with their loved ones and reduced recidivism rates.

This advanced solution provides multiple benefits, including:

- Allowing offender to participate in video via terminal or tablet
- Allowing family & friends to enjoy video sessions in home or other mobile situations
- Allowing more family members to be involved in a video session, providing a much better alternative for children
- Providing additional convenience to stay connected across distance
- Providing more options for video sessions at times that are convenient
- Improving communication with legal representation, bail-bondsmen, family, and any other persons authorized by CDOC administration
- Increasing Offender and guest morale with increased opportunities to communicate.

Remote Video Sessions

This method allows remote video guests, such as family and friends, bail bondsmen, probation officers, and attorneys to communicate with offenders from outside the facility via a broadband internet connection on Android and Apple mobile devices.

Remote video guests access SVC services through the Securus mobile application or the www.videovisitanywhere.net website. Remote users need only a tablet, Android or Apple mobile phone, or a computer with a webcam, microphone, and speakers/headset.

Family and friends sign up for a free Securus Online account and add the video product to their accounts. Then, the user requests video access to the facility, which requires submitting their picture and driver's license to the agency for approval.

From the mobile app or website, guests select the offenders with whom they would like to communicate and then can:

- Create, reschedule, and/or cancel a video session
- Pay for the scheduled session with a credit or debit card
- Join a video session—no officer intervention is required



How It Works: Remote Video Sessions



An offender's family, friends, and others—such as attorneys—can access the SVC service through the mobile app or by going to www.videovistanywhere.net using any standard internet browser on a computer or mobile device. This website allows users to establish an account, schedule and pay for a remote video session, and view account activity.

When a user logs on to the website or mobile app, they select the facility and offender with whom they wish to see. The system shows the available dates and times from which they can pick; through an integration with the jail management system, the

application automatically schedules sessions according to the individual's housing location, available terminals at that location, and available video time slots. Remote video sessions are charged on a per-session basis or subscription rate, and friends and family can pay using a debit or credit card.

How It Works: On-Site Video Sessions

Onsite video allows guests to engage at the facility in a video session at a touch-screen terminal. When the guest arrives at the facility, they are directed to the designated terminal area after passing through security. At the terminal, they enter a PIN unique to that video session to validate the appointment and enjoy a video session with the offender. The PIN is provided to the guest when scheduling the session and is also emailed to the guest separately. Video guests can schedule their onsite video session in three ways:

- Securus mobile app: Schedule an onsite session using the Android or Apple Securus mobile app
- Onsite terminal: Schedule using one of the touch-screen terminals configured for scheduling within the lobby
- Securus Online Website: Schedule online at www.videovisitanywhere.com

The facility's needs dictate the scheduling process. By default, onsite sessions are subject to the same scheduling rules as remote video sessions.

When prompted, the offender identifies themselves on the terminal using single- or dual-password authentication and the session starts automatically, requiring no officer intervention.

Efficiency-Driving Services

The SVC service is just one of many applications available on Securus' ConnectUs platform. ConnectUs is the offender user interface on the terminals. ConnectUs provides limitless opportunities for offenders to self-perform tasks that reduce facility involvement and to help automate facility processes. These opportunities include:



- Making phone calls
- Reading PDFs (i.e. Offender handbook)
- Listening to MP4 videos (e.g. PREA)

- Displaying dynamic facility notifications

Frequent Technology Updates

The SVC service receives regular feature upgrades to keep up with advancements in technology and within the industry. The Video Connect system is accessed through NextGen SCP™, providing the facility control over the system. Securus enables new features and modules through the centralized system, even after installation.

SVC Summary

The SVC platform is a **100%** web-based video communication solution specifically designed for correctional facilities.

Our SVC system provides Securus clients the best video system to facilitate communication between the offender and their family and friends. Securus maintains the SVC system so family and friends will not be directed to a third-party site to create or manage their video sessions. The system is operational 24x7x365, so that the CDOC benefits from fast, accessible, and secure service.

c. System will provide intelligent video visitation technology to reduce unwarranted visual images and explicit content.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Background Privacy blurs the background in a range of six (6) feet or so behind the participant on video sessions using facial detection (not facial recognition).

d. System will allow the facility to manage visitation hours, time slots, scheduling and monitoring.

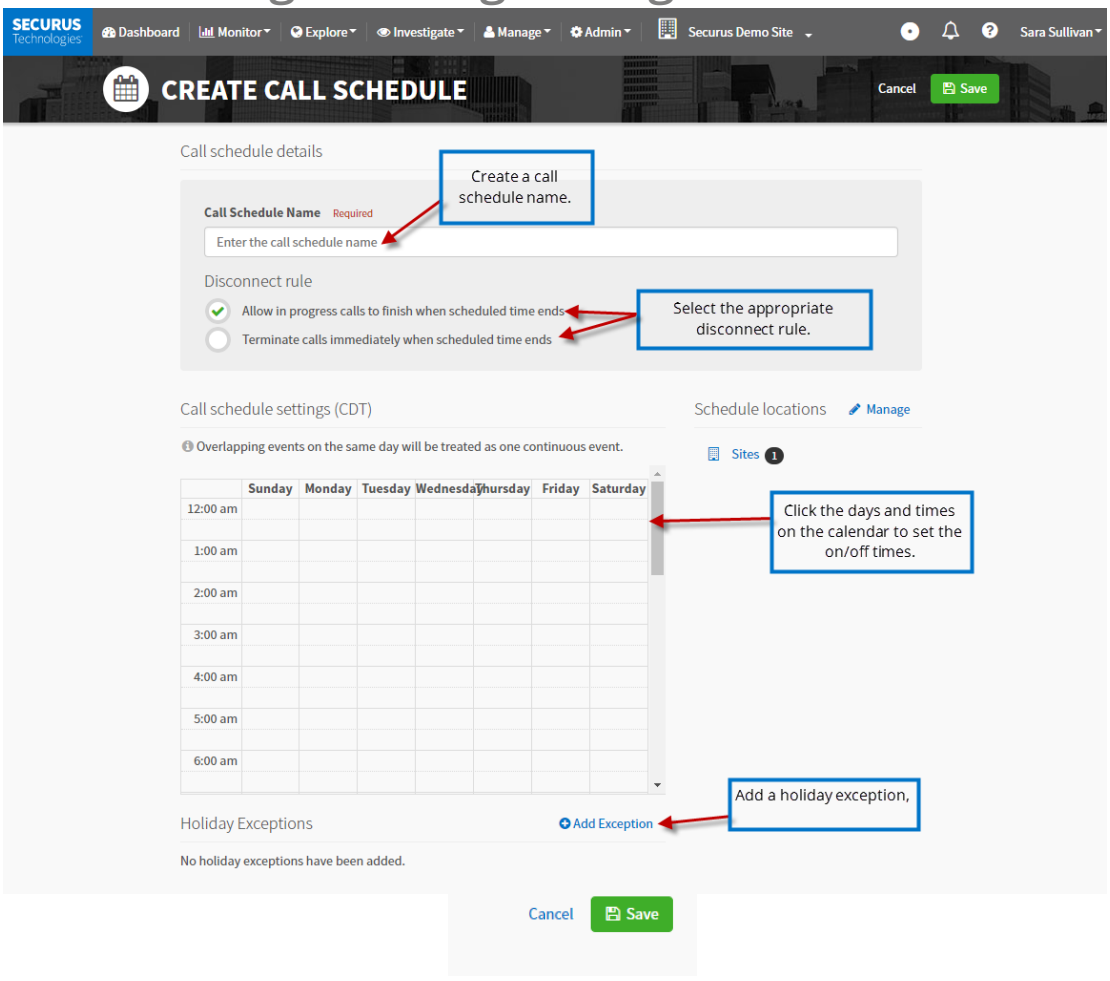
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen Secure Communications Platform™ (NextGen SCP™) calling services has an automated calling schedules feature that allows the system to enforce the scheduling policies of the facility without staff intervention. Calling schedules are used to turn on and off the phones during designated times throughout the day or night.

Calling schedules are flexible and configurable allowing the facility to have multiple on and off times during the day, within a week and by day of the week and then be applied to individual telephones, groups of telephones, individual offenders and/or globally.

Also, holiday overrides can be preset to accommodate anticipated exceptions to the set schedule.

Programming Calling Schedules



Programmable calling schedules are responsive to and overridden by both the manual cut-off switches located within the facility and the Call Settings Disconnect Rule.

e. System will provide video visitation resolution rated at 720p at 30 frames per second or better.

SECURUS HAS READ, UNDERSTANDS, AND WILL PARTIALLY COMPLY WITH THIS REQUIREMENT.

SVC supports up to 15 frames per second of high-quality video at 200+ Kbps.

f. System will have the ability to record visitations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The integrated calling services recording application works independently, so integration with a third-party is unnecessary. This allows your facility to deal with a single vendor if any issues arise. NextGen SCP also shows if the call was accessed, available call notes, or if the call is flagged. Clicking on a call will open a side-bar and any associated details for the communication event, such as the billing name and address (if available), phone location details, call type, call status, CDR ID, termination category, cost of the call, and the call prompt language selected. This side-bar provides an easy method for downloading the call recording, extending the expiration retention period date for a call recording, a note capability for he CDR, and access for viewing the recording historyall with a single mouse click.

NextGen SCP writes all recorded calls to a Network Attached Storage array (NAS) in our primary Data Center. Each NAS array is also replicated to the secondary Data Center for redundancy and failover. All recordings created on the platform reside in at least two of our Data Centers. Recordings are stored online for immediate access per contractual agreement. NextGen SCP can also be used to copy the recording and call detail information to a digital file that can be transferred to CD or DVD for additional back up, if necessary.

The calling service records all calls simultaneously and allows personnel to listen to previously recorded calls while active calls continue to be recorded. The system records the entire conversation from call acceptance to termination.

Remote Access to Recording and Monitoring

With integrated recording and monitoring applications, other agencies, such as local police departments, can also access these functions. Any user that CDOC approves can access the recording and monitoring function of offender calls from any computer or device with internet access. Securus has tested and certified call playbacks and live monitoring on:

- Operating Systems/Devices
  - iOS
  - Android OS
  - OS X
  - Windows
- Browsers
  - Chrome

Security of Call Recordings

Video recordings are stored in Securus' centralized Disaster-Resistant Carrier-Class Data Centers located in Dallas and Atlanta. The Data Centers house commercial-grade, high-performance, managed video systems built to the latest technology standards. These centers manage all of the hardware and software controlling fraud detection, investigative features, session processing, session records, and actual recordings of sessions. They are managed under the direct supervision and immediate hands-on maintenance by trained data center personnel. In addition, all equipment used to store recordings is monitored by the Securus' fully staffed Network Operations Center 24 hours a day, 7 days a week, and 365 days a year.

Securus records all video sessions to two separate Storage Appliances, using two separate connections to the different Appliances. The Securus Data Centers are carrier-class data center that haves some of the most comprehensive security measures in the telecommunications industry. Multiple layers of security control physical access to the Securus network facilities.

Security personnel maintain the following procedures for allowing entry into the data centers:

- Security personnel are on premise 24x7x365
- Cardkey reader (electronic badge) access for entry
- All persons having a business need to access company premises must carry identification badges at all times
- Man traps at each entry and exit point in the data center. Man traps use two sets of doors that both require electronic badge entry. The first set of doors must close before the second can open.

Other companies may try to convince you that a second-rate method of storing video recordings – such as storing them in video terminals accessible by offenders – is adequate. Do not be fooled. With Securus, you can be assured your video session recordings will be secure. No other company in the industry provides this level of security.

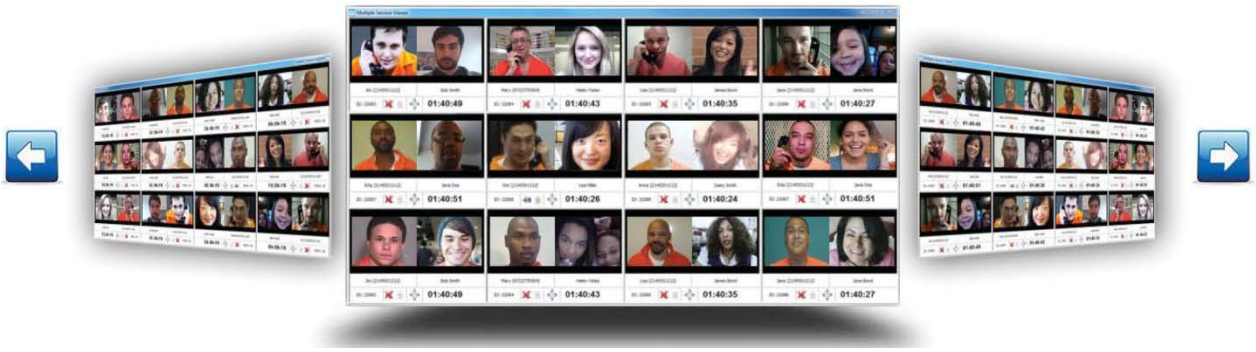
g. System will have the ability for designated CDOC staff to monitor real-time visitation and terminate the visit as needed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus offers Multi-Session Live Monitoring (MSM) through the NextGen Secure Communications Platform™ (NextGen SCP™). The Securus Video Connect™ (SVC) service MSM allows facility administrators to view a "slideshow" of all active video

sessions. Up to 12 simultaneous sessions can be seen on the screen at one time—more than any other video provider. If there are more than 12 active video sessions at one time, the system will scroll through all active sessions, providing CDOC management and control over inappropriate and suspicious behavior.

Multi-Session Monitoring Window



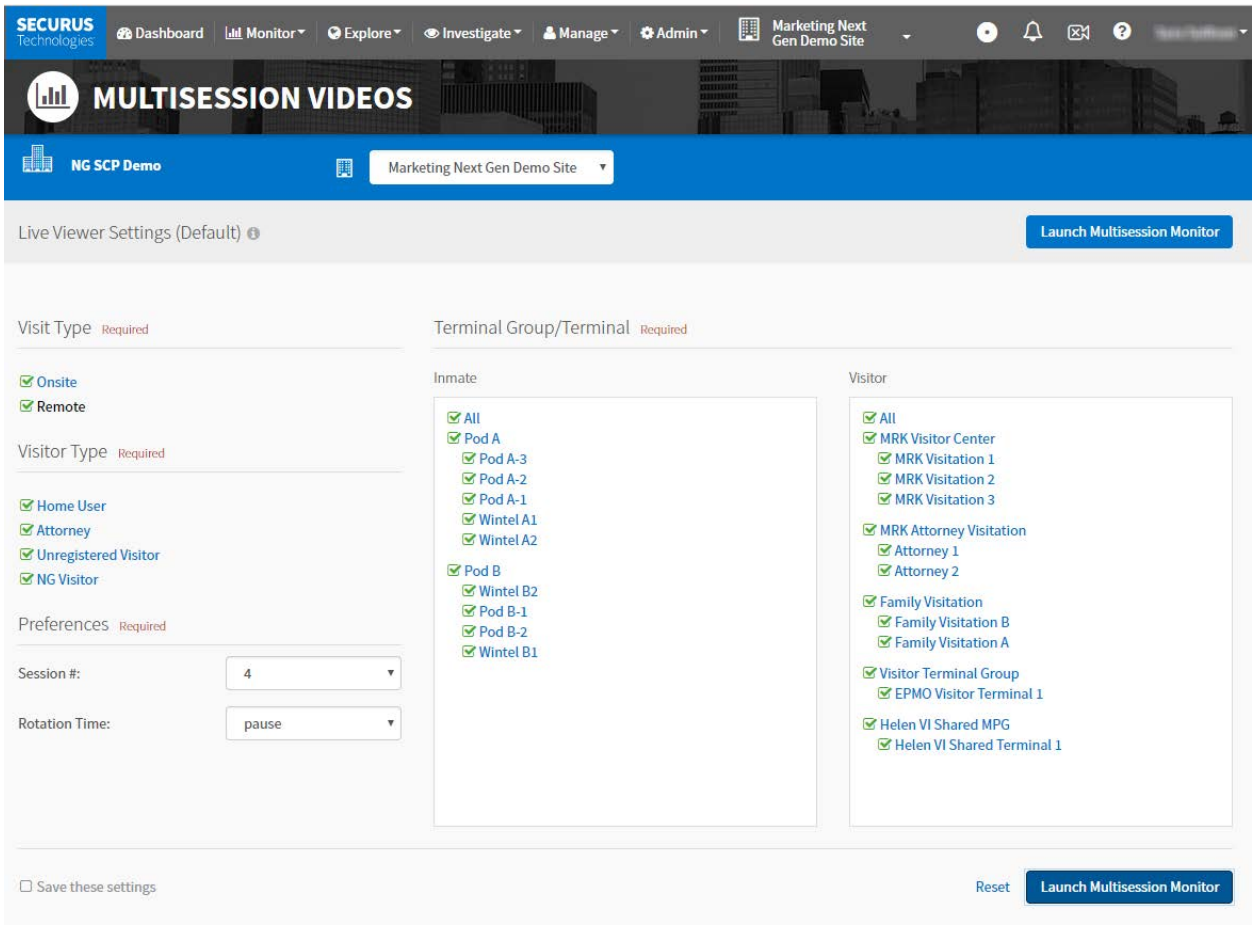
How it Works

MSM streams multiple, in-progress video sessions to allow the authorized user to monitor multiple sessions at the same time, which is ideal for facilities with a centralized monitoring room with multiple concurrent live visits.

A CDOC user can configure the parameters to view all live visits according to their access credentials and preferences. The available parameters include:

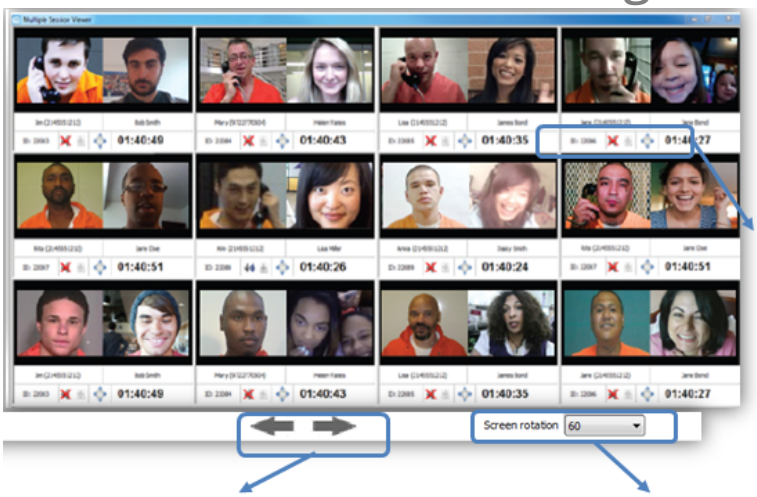
- Visit type
- Visitor type
- Offender terminal group or individual terminal
- Visitor terminal group or individual terminal

Filter Parameters



Sessions are displayed in the order in which they began, beginning in the upper left corner. For example, if a CDOC facility has 12 sessions all scheduled to begin at 1:00 p.m., the first session in the upper left of the MSM window will be the visit where both the visitor and offender joined first.

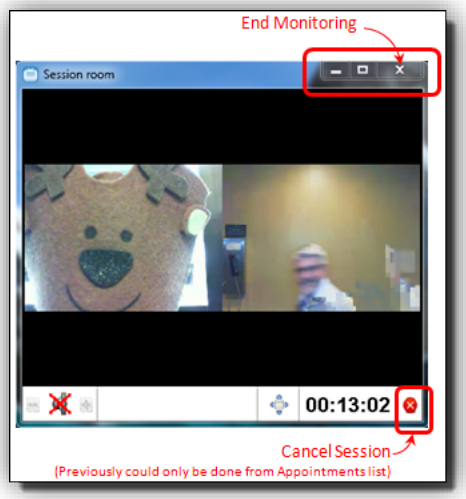
Multi-Session Monitoring Window Details



Multi-Session Live Monitoring Zoom-In Window

Authorized CDOC users can zoom in on an individual video session, allowing for even more capabilities, such as listening to the audio, barging in or immediately disconnecting a session. After zooming in, a user can stop monitoring that specific session or cancel the session by selecting the icon in the lower right of the screen.

Zoom-In Window

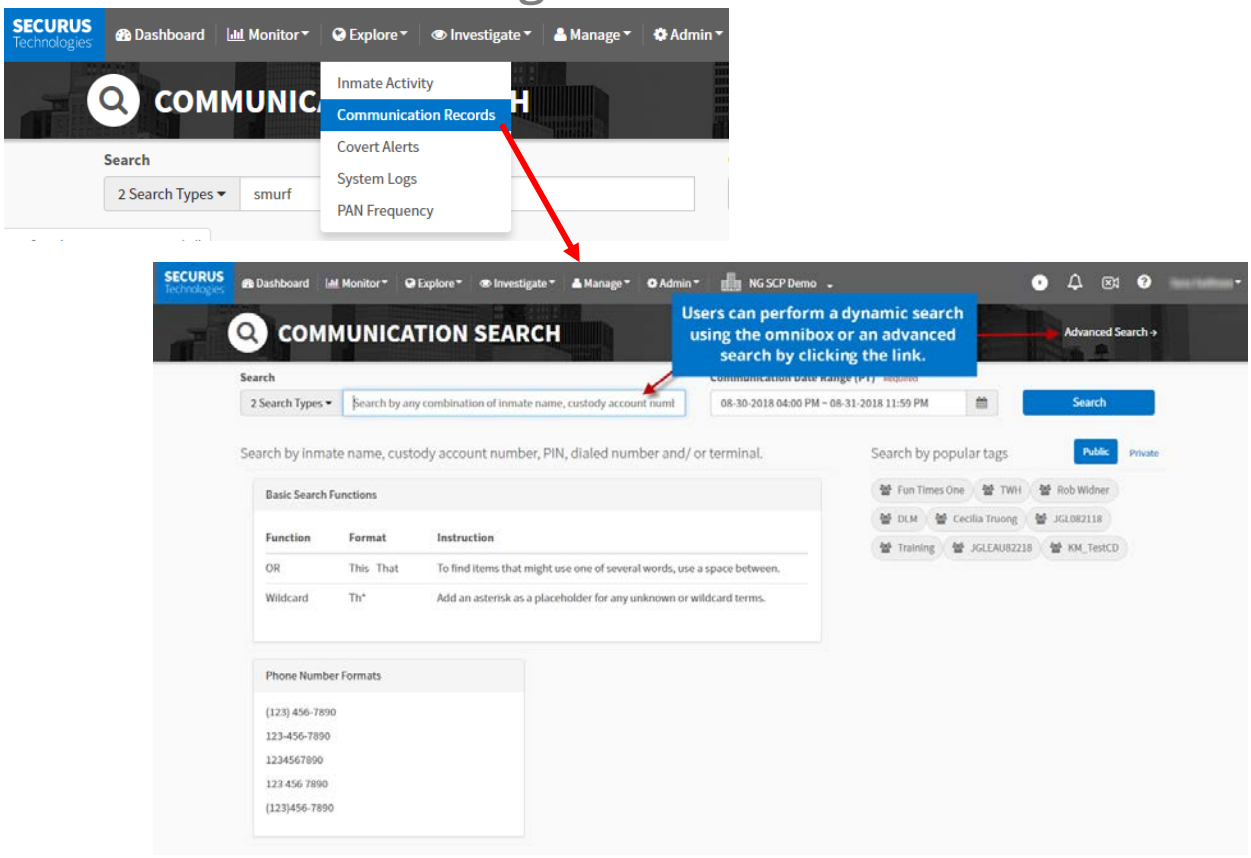


h. System will provide video visitation technology to access recording, detailed reports, scheduled offender visits, etc.

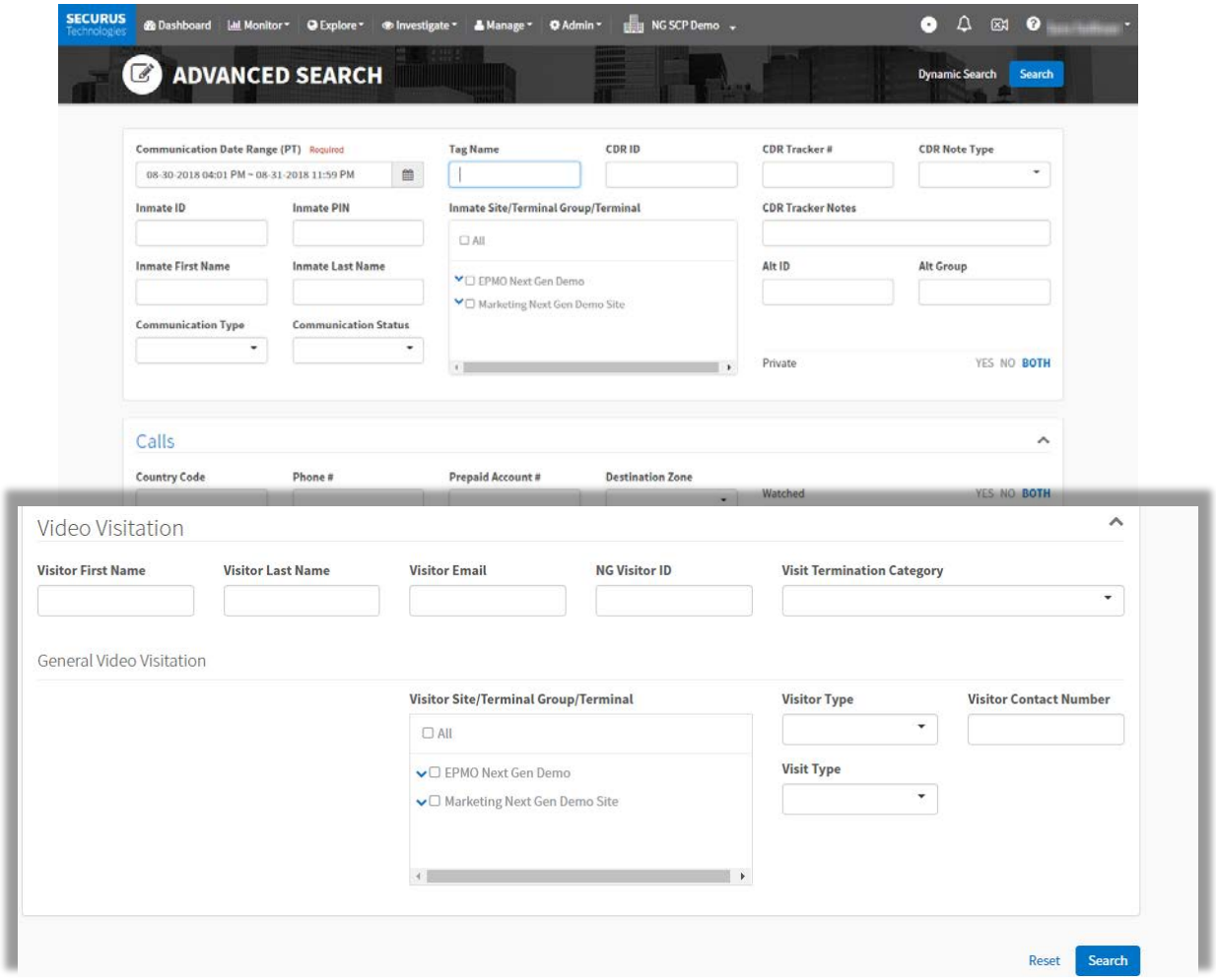
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Authorized CDOC users can generate communication reports on all Securus Video Connect™ (SVC) events through the NextGen Secure Communications Platform™ (NextGen SCP™) user interface. CDOC users can perform a dynamic search using the single-input omnibox or an advanced search.

Searching for SVC Events



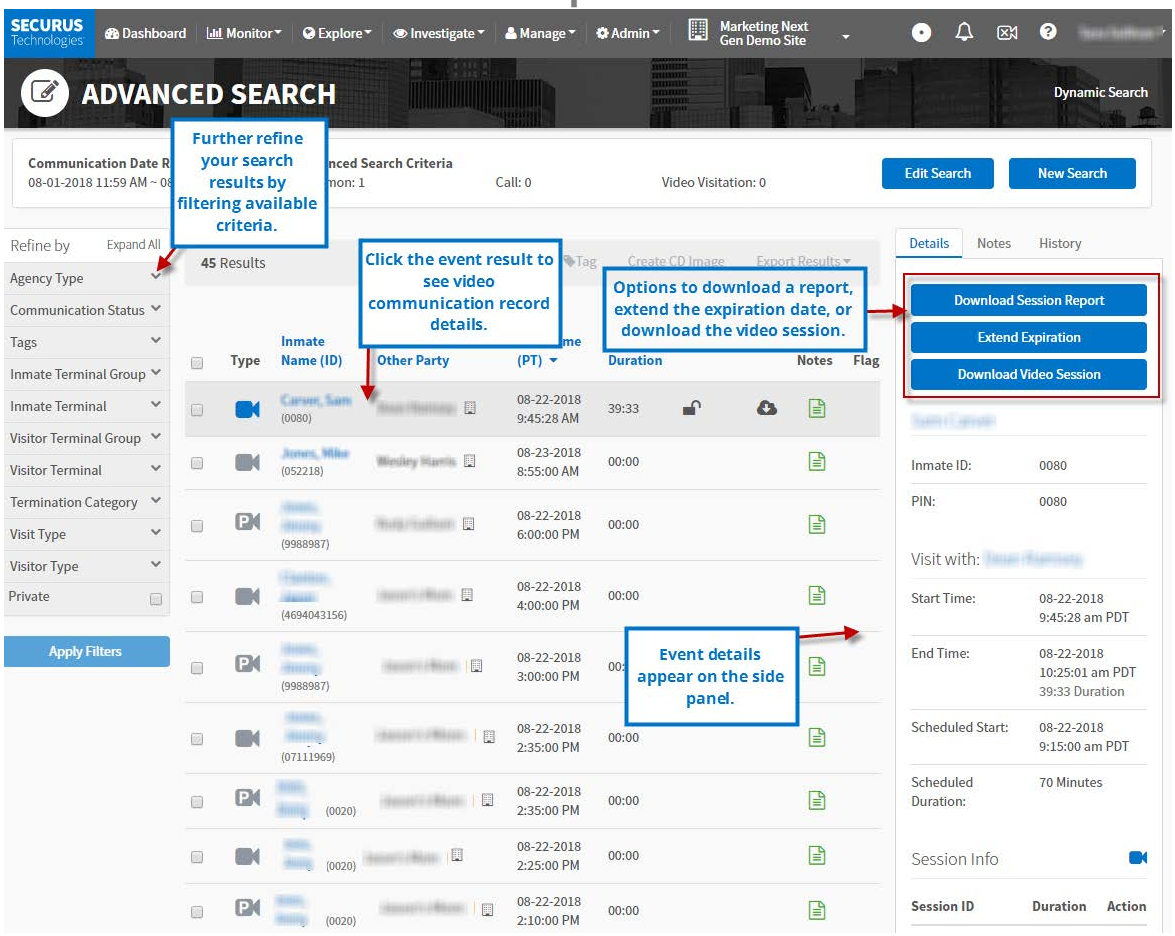
Advanced Search for SVC Communication Records



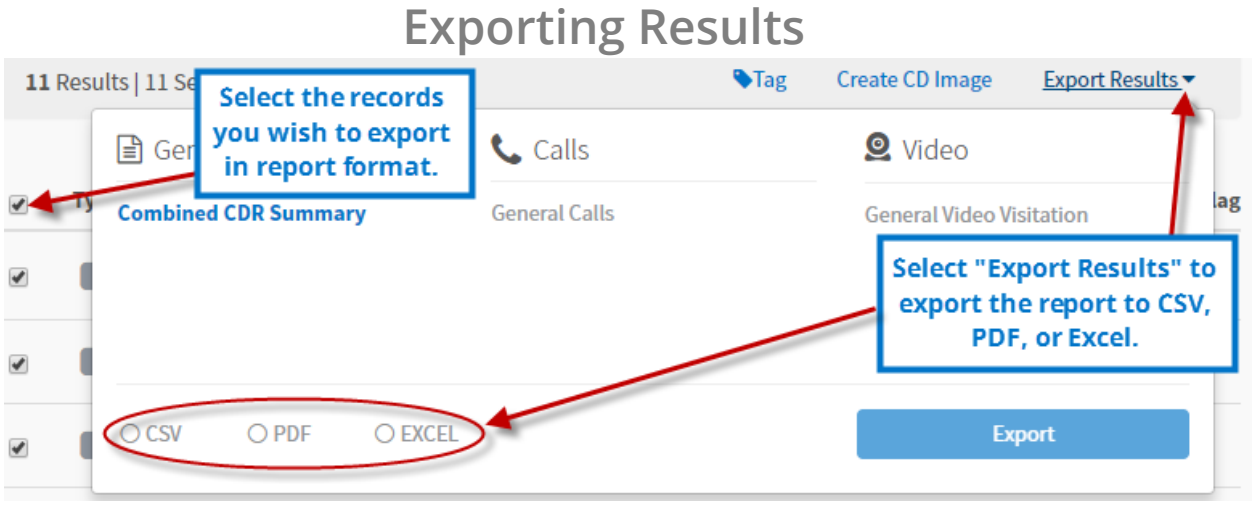
NextGen SCP presents the search results in such a way that further action can be taken from this same page to further refine search results, download recordings or data, or export report results without navigating away from the search results page. The left-hand side of the page offers filtering based on the results and shows only the filter options that are present in the results.

Clicking on the event in the results pane opens the communication event detail pane on the right-hand side of the page. This pane provides additional detailed information about the event and allows the user to download the session report, extend the recording expiration date, download the video session, or play the session recording without downloading it to the user's computer.

Securus Video Connect℠ Communication Detail Report



Communication detail results can be exported to CSV, PDF, or Excel.



xx. System will include an option for Video Relay Service (VRS) separate from video visitation for hearing impaired/offenders. Capabilities for video visitation should include, but not be restricted to:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus uses ZVRS/Purple for our VRS solution. There are major differences in how vendors provide VRS service. The Securus offering is very unique compared to other vendors in that it is fully integrated into our NextGen SCP and does not require users to access a totally different system to complete VRS calls. **NO other vendor** has VRS fully integrated into their platform. The high level of integration between Securus VRS and NextGen SCP provides hearing impaired offenders with "equal access" to communication services while providing CDOC the ability to provide, manage, and investigate offender VRS calls in a manner consistent with traditional offender calls.

Video Relay Services offer unique challenges to the correctional industry due to its reliance on American Sign Language (ASL) which requires visual communication, the automatic insertion of an ASL interpreter when needed, and adherence to FCC regulations which prohibit VRS Service providers from interfering with or recording the communication. Securus VRS addresses all of these challenges so as to provide CDOC with a VRS solution which does more than meet the requirements of ADA compliance.

Securus VRS supports both types of VRS Calls:

1. Offender VRS Phone to VRS Phone:
2. Offender VRS Phone to Standard Non-Video Phone:



Offender VRS call to F&F VRS Device



Offender VRS Call to Non VRS Phone Number



Controlling Which Offender May place VRS Calls

Authorized CDOC users can set whether an offender is eligible to use VRS from the offender custody account profile page. For CDOC, we will configure the Securus VRS application to require offender login. Then, the offender must have "VRS Allowed" setting on the offender profile set to "yes" before they are allowed to login to the application.

The Securus VRS ConnectUs application will require offenders to enter both their designated offender ID as well as their issued calling PIN before being allowed to place VRS calls. To accommodate the needs of the hearing impaired, Securus VRS can be configured in designated booking and/or intake areas to not require the use of offender PINs to place VRS calls through Securus VRS. By these controls, CDOC is provided both security over VRS calling as well as flexibility to allow VRS calls in situations where detainees have not yet been issued a PIN.

Call Controls

Our VRS is fully integrated within the NextGen SCP network, allowing for standard NextGen SCP policies, such as PAN list control, call recording, time limits, remote printing of the call contents, redial prevention, and more. Securus VRS highly leverages the standard offender call management control structures used by NextGen SCP for traditional offender calls, including the following:

- Calling Schedules
- Max Call Duration controls
- Calling Restrictions
- Calling Velocity
- Specific called party phone number controls both globally and on offender PAN lists

- Control over which calls to record

VRS Call Monitoring and Recording

The nature of our relationship with Purple, along with the proprietary integration of technologies, allows NextGen SCP to record VRS calls while still remaining compliant with FCC regulations. If a VRS call is in progress, the GDC user will be able to click and see the video call in progress. Further, because of the full integration of VRS with NextGen SCP, call recordings are searchable within the platform and will appear in the Call Detail Record. This is a feature that **our competitors do not possess** because their video relay solutions are not in integrated to the same level.

Securus VRS call recordings include the visual component of the offender call for both the offender and the other end of the video portion of the VRS call. The other end of the VRS call might be the offender's called party (if they are a registered subscriber to the public VRS service) or the VRS interpreter (if the called party is not a registered subscriber to the public VRS service). Since the public VRS service automatically bridges in a VRS interpreter when necessary, Securus VRS fully accommodates the various scenarios the public VRS service may encounter. These scenarios include the potential that a VRS Service provider supports Voice Carry Over (VCO). When VCO is supported, the Securus VRS call recording will include the audio component of the VRS call.

Recorded VRS calls are available for download in MP4 format and can be put on a CD for investigative purposes.

a. Integrated into wall-mounted kiosks.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus VRS works through the ConnectUs interface on the standard wall-mounted offender kiosks.

b. Option for VRS application to be available to specific users based on offender PIN.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus VRS is integrated with NextGen SCP to allow the CDOC to designate which offenders are allowed to place VRS calls. Offenders must then enter their designated offender ID and their calling PIN before placing a VRS call.

To accommodate the needs of the hearing-impaired, Securus VRS can be configured to work without PINs in areas that the DOC may designate. With these controls, the DOC has security over VRS calling as well as the flexibility to allow VRS calls in situations where offenders have not yet been issued a PIN.

c. Automatically route VRS calls through a VRS interpreter for calls placed to a non-VRS registered phone number is expected to have the capability of making a direct connection to a called party without the need for an interpreter when calling a VRS registered phone number.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus VRS is integrated with the NextGen SCP and automatically routes VRS calls through a VRS interpreter for calls placed to a non-VRS registered phone number. The system can make a direct connection to a called party without the need for an interpreter when calling a VRS registered phone number. The public VRS service automatically bridges in a VRS interpreter when necessary, Securus VRS fully accommodates the various scenarios the public VRS service may encounter.

d. Allow offenders to choose English or other language speaking video relay interpreters.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Offenders can select English or another-language speaking VRS interpreter.

e. Allow option for Voice Carry Over.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

When VCO is supported, the Securus VRS call recording will include the audio component of the VRS call.

f. Have an automated announcement to the called party/interpreter to inform the called party that the call is from a correctional facility and that calls may be monitored and recorded.

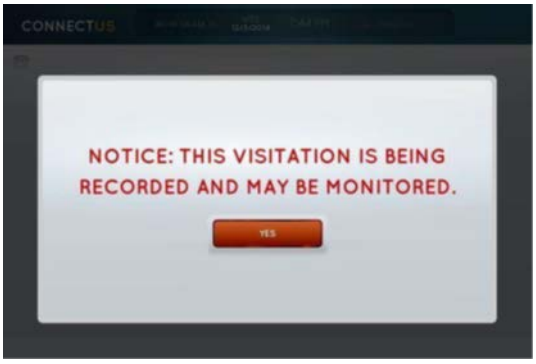
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus provides an announcement to the called party/interpreter to inform the called party that the call is from a correctional facilities and that they may be monitored and/or recorded.

g. Display an on-screen message to the offender that VRS calls may be monitored and recorded.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

When participants join a visitation, a warning screen will pop up advising that video call may be monitored and recorded and will require the participants to acknowledge the warning before the session can progress.



h. Prevent 3-way calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

i. Prevent incoming calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

j. Prevent 911 calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

k. Will not display a call history or call log to offenders.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

l. Have live monitoring of VRS calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

m. Record VRS calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.



Securus' NextGen Secure Communications Platform™ (NextGen SCP™) provides support for hearing-impaired offenders through both Video Relay Service (VRS) and TTY/TDD. The Securus VRS solution is a complete solution for correctional-grade VRS services that incorporate FCC regulations, as well as the offender call controls, management, and investigative abilities expected for offender calls.

VRS offers unique challenges to the correctional industry due to its reliance on American Sign Language (ASL), which requires visual communication, the automatic insertion of an ASL interpreter when needed, and adherence to FCC regulations that prohibit VRS service providers from interfering with or recording the communication.

Securus VRS addresses all of these challenges so as to provide CDOC with a VRS solution that does more than meet the requirements of ADA compliance—Securus VRS meets these challenges through a high-level integration with NextGen SCP. The high level of integration between Securus VRS and NextGen SCP provides hearing-impaired offenders with "equal access" to communication services while allowing CDOC to provide, manage, and investigate offender VRS calls in a manner consistent with traditional offender calls.

Securus VRS provides equal access by allowing CDOC to:

- Provide VRS-capable offender call devices that fully conform to the rigorous needs of the correctional environment
- Manage VRS calls using the same controls as are used for traditional offender calls
- Record VRS calls in accordance with the same recording controls that govern whether or not to record traditional offender calls
    - Securus VRS can record VRS calls due to the fact that Securus is not a "VRS Provider". Instead, Securus is partnered with ZVRS/Purple to be the "VRS Provider". The nature of this relationship, along with the proprietary integration of technologies, allows NextGen SCP to record VRS calls while still remaining compliant with FCC regulations.
- Include VRS call recordings in investigations including inclusion in CD images and individual downloads.

Securus VRS call recordings include the visual component of the offender call for both the offender and the other end of the video portion of the VRS call. The other end of the VRS call might be the offender's called party (if they are a registered subscriber to the public VRS service) or the VRS interpreter (if the called party is not a registered subscriber to the public VRS service). Since the public VRS service automatically bridges in a VRS interpreter when necessary, Securus VRS fully accommodates the various scenarios the public VRS service may encounter. These scenarios include the potential that a VRS Service provider supports Voice Carry-Over (VCO). When VCO is supported, the Securus VRS call recording will include the audio component of the VRS call.

Securus VRS uses the same standard offender call management control structures as for traditional offender calls, including the following call controls:

- Calling schedules
- Max call duration controls
- Calling Restrictions
- Calling Velocity

- Called party phone number control—both globally and on offender PAN lists
- Call recording
- Collecting VRS calls in offender calls for investigations and evidence

This level of integration between Securus VRS and NextGen SCP means that CDOC can set offender calling policies that apply equally to all offender calls, including VRS calls, or set unique policies for VRS calls.

Offender access to Securus VRS is provided as an application available through ConnectUs—the controlled offender interface provided on offender kiosks. ConnectUs can be configured to present numerous applications to CDOC offenders, which allows offenders to use the same multi-function terminal for Securus VRS calls as for standard offender calling, Securus Video Connect, Offender Forms, and more.

Because VRS calls are required by the FCC to be free, all offender VRS calls will be provided at no cost to the offender. To ensure CDOC can prevent the unauthorized use of Securus VRS to place free calls, the Securus VRS is also integrated with NextGen SCP to allow CDOC to designate which offenders are allowed to place VRS calls. The Securus VRS ConnectUs application requires offenders to enter their designated offender ID and their calling PIN before placing calls. To accommodate the needs of the hearing-impaired, Securus VRS can be configured to work without PINs in designated booking and/or intake areas. With these controls, CDOC has security over VRS calling as well as the flexibility to allow VRS calls in situations where offenders have not yet been issued a PIN.

Securus VRS represents the ultimate solution for accommodating conformance to ADA compliance and FCC regulations, and the necessary call controls and investigative abilities to ensure safe communications.

xxi. Offeror to describe estimated impact of video visitation on the CDOC network.

a. Provide a plan for data lines should capabilities at the facilities be limited as a result of this implementation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

SVC operates on a separate network from the CDOC secure network. Securus installs all necessary cabling, networking and equipment and will not require or interfere with the agency's network.

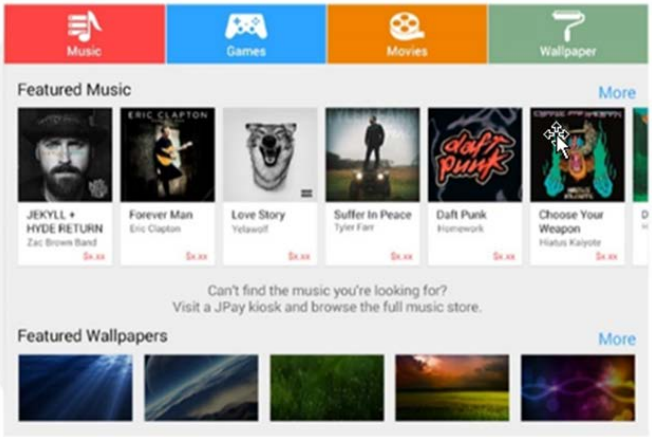
xxii. Music

a. Offer subscription-based media and/or streaming music available for a fee. The CDOC will decide on the fee structure for the streaming music model.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

From the Media Store app on the Unity Tablet, offenders have access to over 35 million songs from several genres. Offenders can search for their favorite artists, songs and albums, discover the latest music. Thirty (30) second previews are available so offenders can listen to a sample of the audio, before they buy it.

Securus can offer both an ala carte purchase model and subscription-based music structure.



Music App

The Music application allows offenders to listen to the music that they have purchased and downloaded from the Securus Media Store. Users can download their favorite tunes to their tablet and create a customizable playlist for more enjoyable listening.

Music Subscriptions

With Securus' music subscription service, offenders have access to millions of tracks through a tiered subscription model for a recurring monthly cost. Several subscription package options are available to meet a variety of consumer preferences and budgets.

We have partnered with one of the largest music distributors in the world to bring offenders music subscription access to an evolving selection of titles – new music is added catalog daily!

And unlike other competitor providers who use automated algorithms to provide 'customized' content, our music is expertly, and personally curated based on data derived directly from the facility. Our playlists and suggested artists are population-specific, created by our music professionals.

Best of all, there is no additional administrative hassle for the agency. All subscription packages are purchased and managed independently by the offender through the Personal+ tablet media store. And in efforts to expand access to music to as many incarcerated listeners as possible, we periodically run sales and promotions making subscriptions an attainable option for your incarcerated population.

A-la-carte music will continue to be available through the media store for offenders who are not interested in a subscription package option.

b. Offer a large variety of titles and genres available for subscription-based streaming.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus Media Store and Music App offers a large selection of corrections appropriate, industry sanitized music with over 35 million tracks. The music catalog is updated daily and includes several genres such as Folk, Jazz, Blues, Rock, Alternative, Electronic, Dance, Music from Soundtracks, Classical, R&B, Hip Hop, Gospel, Soul, World, Latin Country and Reggae.

c. Offeror is expected to be able to customize the music catalog for approval by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

While individual customization is not available, Securus will work with CDOC personnel to remove music from the catalog, and music provided is suitable for the corrections environment.

d. Offeror is expected to provide expected download/data retrieval times.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Downloads should be complete in as little as five seconds, but times are variable since they are dependent on wireless network load.

Programs, movies, educational content, and games are accessed and downloaded to Unity Tablets from Securus' Tier IV data centers. There are no bandwidth or location issues as there are when streaming from an outside internet service/source, and the security of the offender' access to data, sites, and information is protected by the firmware within the Unity Tablet.

e. Offeror to describe theft prevention features.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All tablets on Securus' Unity Platform are equipped with a custom lock screen that allows the CDOC to easily identify the device type and who it belongs to. The lock screen will have a screen that will show the user's first name, last name, ID, customer name, housing location, time, date and the Wi-Fi strength and battery percentage.

Tablet content can only be accessed using the credentials of the offender to whom the device is assigned. Unity Tablets requires an offender to log-in prior to use with their unique account ID and PIN, which is the same credentials used to make phone calls or sign into other Unity Applications. There is a limit on login attempts. If the

predetermined number of attempts is exceeded, the tablet will be locked for 10 minutes.

For all tablet and media transactions, the offender is required to input and confirm their credentials before the transaction may be completed.

Securus Unity hardware is only functional within the correctional facility. In the event it was removed, it would no longer be functional and could not be accessed.

f. The Offeror is expected to have contractual rights to distribute digital media from major music labels or other entertainment fields to provide a reasonable volume of acceptable media content.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has the contractual rights to distribute digital media from out content providers. We have worked hard over many years to build relationships with providers to get diverse content at reasonable prices. This work has resulted in a music catalog of more than 35 million songs from all major record labels. The music catalog is updated daily and includes several genres such as Folk, Jazz, Blues, Rock, Alternative, Electronic, Dance, Music from Soundtracks, Classical, R&B, Hip Hop, Gospel, Soul, World, Latin Country and Reggae.

C. Kiosk technical environment

i. The Offeror will provide its application(s) that will run on an operating system, mutually agreed upon by the Offeror and the CDOC that is capable of being upgraded at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide its application(s) that will run on an operating system, mutually agreed upon by the Offeror and the CDOC that is capable of being upgraded at no cost to the CDOC.

ii. Offeror is expected to ensure that the operating system is no more than (N+2) revisions behind the publicly available kernel.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

We focus on overall security solutions for tablets and kiosks. Securus will ensure all Tablets and kiosks are up-to-date with an operating system version no more than two versions removed from the vendor's current version provided it passes our hardware compatibility, security, and quality control standards. Securus delivers software upgrades and systems updates to all customers multiple times per year with no

downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry.

iii. The Offeror is expected to provide following technical support services for all hardware equipment and software for services provided including but not limited to:

a. Updates and upgrades;

- **Security-related updates to their proposed solution, which may be called updates, upgrades, patches, service packs, hot fixes, and workarounds.**
- **All upgrades, bug fixes, enhancements to the software and hardware will receive prior approval by the authorized CDOC staff.**
- **The Offeror will provide a test environment to allow authorized CDOC staff to verify the upgrade, fix and enhancement is compatible with the current operating environment.**

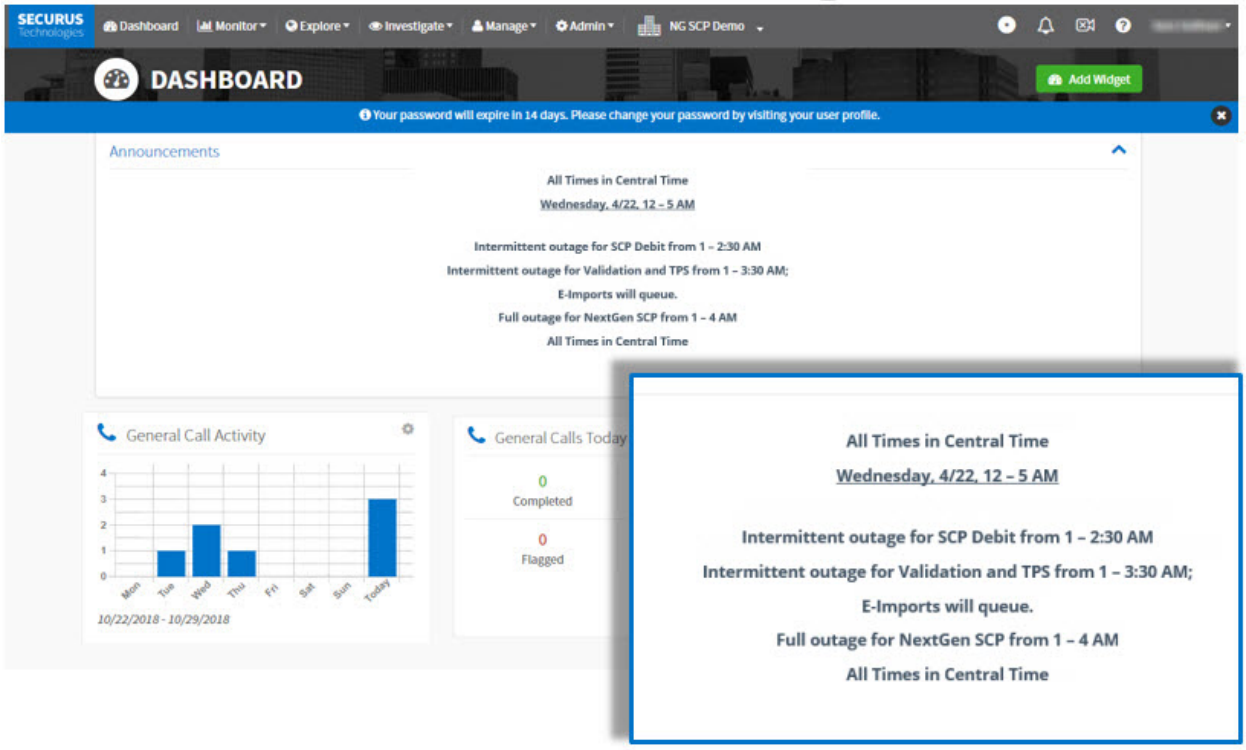
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

System updates, bug fixes, enhancements, patches and workarounds are executed as described below.

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCP™ software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



Securus will provide production-ready software enhancements and upgrades three to four times per year.

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Patches

System patch management: After system deployment, Securus uses the Patch Management Program to ensure that systems are updated with the latest patches.

Software Development

The Securus use of information technology (IT) best practices, industry standard quality measurement tools, and strict environmental controls ensure the highest system functionality and availability. The Securus development team uses the Waterfall Software Development Lifecycle (SDLC) to ensure high-quality deliverables. The feature/functionality enhancements process stages are:

- Analysis
- Design
- Development
- Quality Assurance
- Implementation
- Post Implementation Support

Each phase has specific deliverables and gates (controls) to ensure high quality and to minimize rework. During the lifecycle phases, software changes include an accompanying change control document that identifies, at a minimum:

- Version number
- Description of the change
- How the change was initiated
- Person or customer requesting the change
- Person responsible for the change
- Date and time of the change

Securus uses the following distinct system environments in conjunction with our SDLC:

- Development – Used by IT Development to create and unit test new enhancements
- Quality Assurance – Used by Quality Assurance Analysts to test and certify new enhancements and bug fixes
- Pre-Production – Used by Production Support to validate hot fixes for production, and for final validation and mock deployment of major functionality releases
- Production – Used by all Securus customers and accessible by only Securus Production Support and Tech Support

Each environment has access controls, and we use source code control systems to ensure the proper promotion of code and as a document repository.

Securus uses industry-standard HP Quality Center for defect tracking and follows a rigorous test cycle including:

- Verification of New Functionality – Ensures a feature is working as designed
- Load Testing – Determines the upper threshold or breaking point of the component or feature

- Performance Testing – Determines the expected user experience
- Regression Testing – Ensure all existing functionality still works as designed
- Exception Testing – Tests boundary conditions and unexpected usage scenarios

New releases typically create new functionality. Upon completion of the Quality Assurance stage, the code changes are packaged and deployed into our pre-production environment for the final end-to-end quality check, and to optimize the implementation. This effort enables Securus to minimize the maintenance window related to system changes.

Both IT and business stakeholders review and must approve all scheduled changes to production in two change control meetings to safeguard the stability of the production environment.

Upon implementation of new code into production, Securus Production Support and IT Development monitor changes closely to minimize the impact of any adverse or unexpected system behavior.

This attention to detail allows Securus to build feature functionality that leads the industry in quality and performance.

Our quality control does not end with our system design but continues all the way through system upgrades and training.

Our notification of changes is provided in the form of a splash screen upon log-in to the NextGen SCP user interface, or through an official Release Notes document. The Release Notes provides the following details:

- Version number, if applicable
- Description of the change, including whether it is a minor update or a major update
- Contact information for additional information or training
- Date and time of the change

Pilot sites

Securus uses customer sites as pilot sites to test-in and verify updates and upgrades in a customer environment to verify field adoption of the changes.

b. Hardware Expectations

- **Offeror is expected to describe the capability for the development of future applications and implementing these applications on the proposed hardware configuration.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is constantly developing its system to accommodate technological progress. When hardware is necessary to system growth, it is added within the terms of the contract. Scalability and growth is built into Securus' system with storage growth is described below.

All of Securus' systems are completely scalable with the ability to increase server number and size to accommodate changes and increased workflows.

Scalability of our Central Processing System and Network

Securus communications system, encompassing telephone, video and tablet service, is a centralized system which provides centralized management services at the Securus data center for all of the telephones, kiosks and tablets within the customer facility.

The network for our communications system maintains twice the capacity of normal calling volume to prevent blocking of outbound calls and busy signals and also maintains twice the capacity of normal video volume to prevent blocking of inbound video and support the quality of the audio/video streaming.

The central processing system and its network capacity can scale to many times their current capacity within the current architecture and design. Securus monitors system 24 hours per day, seven days per week, every day of the year. When concurrent telephone call volumes and video session volumes consistently cross 80% of the available capacity, additional infrastructure is added to our central processing system to augment the capacity. Securus adds additional circuit bandwidth to each site and the central data center when necessary.

The on-site tablet servers and network equipment are scaled to provide sufficient capacity and network bandwidth to accommodate expected tablet usage for all tablets within the facility. The central data center is designed to scale beyond the current capacity based on the needs of our customers. When concurrent tablet traffic consistently cross 80% of the available capacity (either at the customer site or at the central data center, additional infrastructure is added to augment the capacity. Since the system capacity is managed to keep ahead of the usage of tablets as well as additional features and services on the tablet, the customer has the flexibility to increase the number of tablets and services enabled at a facility as needed.

Scalability of Storage

Securus stores call recordings in centralized, disaster-resistant, carrier-class data centers. The NAS architecture of our data centers delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network.

The Securus NAS has more than seven petabytes of storage space in each carrier-class data center and is continuously monitored and managed through automated processes and storage policies. When these very large storage systems approach designated thresholds, Securus expands capacity to ensure all authorized communication records and recordings are retained in secure, disaster-resistant locations.

- **Offerors to describe in detail the ability to provide the electrical equipment to operate on a regular 120-volt, 60 hertz, AC power and be "UL" or equivalently listed and be certified by a Nationally Recognized Testing Laboratory to be compliant with the FCC regulations.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All Securus hardware operates on regular 110-120 VAC, 60 Hz electrical power. All components are UL listed and compliant with FCC Part 15 or Part 68, as applicable.

D. Kiosks to support communications via:
i. Cable;
ii. Fiber;
iii. Wireless; and
iv. Other.
v. Offeror is expected to provide a sufficient infrastructure to allow offenders to utilize all the available communication solutions at the same time.
vi. Offeror is expected to allow kiosks to be linked throughout the Department.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The kiosk accepts any type of communications connectivity, whether it is cable, fiber, or wireless. Securus typically installs Ethernet cabling throughout a facility when implementing a network but will work with the CDOC to accommodate other methods if needed.

E. Kiosk Enclosure
i. The successful Offeror will provide a kiosk design to be of standalone style for inside/outside locations. The kiosk enclosure/housing needs to be self-contained, rugged and secure. No crevices that can enable offenders to damage or spill into the enclosure and damage the kiosk.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.



The sPhone XL kiosk is standalone style for inside/outside locations. They are a correctional-facility grade, tamper-proof steel enclosure. The kiosk is a wall mounted unit equipped with a built-in shatter resistant touch screen, a high- resolution video camera with integrated lighting, and tamper-proof, heavy molded plastic handset with an armor-reinforced cord for audio communication, and surge protection. The kiosk does not have any crevices that can enable offenders to damage or spill into the enclosure and damage the kiosk.

Design features:

- A detention grade hardened steel enclosure
- One detention grade audio handset per terminal for the incarcerated individual, and two detention grade audio handsets per terminal for the public
- A shatter resistant LCD monitor with integrated camera
- Enclosures which prevent spills from entering
- Terminals that do not have any openings exposed to the user, including all wiring and ventilation holes
- Terminals without any external hinges
- Rounded tops and corners
- Terminals with built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes and/or disables during all other functions
- Terminals with multiple mounting methods: wall, table, pedestal or cart. All mounting options use standard industry or better methods
- Sealed: Dust and Liquids Resistant, spill-proof (accidental or deliberate).
- Assembly elements are hidden: No screws or hinges can be removed and used to manufacture weapons. No doors/compartments that can be opened in the front or on the sides of the unit.
- Rounded edges that reduce the risks of accidental or intentional injuries.
- Abrasion and chemical resistant; the unit can be cleaned using commercial cleaning agents.
- Humidity and corrosion resistant
- Magnetically activated pushbutton for on/off power

- Built-in heat sink mounted to the back for heat dissipation
- Built-in protection device against voltage variations

ii. Outside Kiosks - located outside and able to withstand weather and the elements; rain, snow, wind, sun, etc. Kiosks should withstand temperatures from -20 degrees to 110 degrees with up to 100% humidity.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our kiosks are designed for durability. Additionally, Securus normally installs outside kiosks under an awning or other covering to help prevent excessive exposure to extreme precipitation and sun.

a. This requirement is not mandatory and will be determined by the type of kiosk proposed. If there are no enclosures, Offerors are to explain in detail the plan for mounting and security and protection of the hardware.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has multiple mounting methods for our kiosks, which include wall, table, pedestal, or cart. All mounting options use standard industry or better methods. Our installation team will perform site surveys and work with the facility to design an optimal plan for mounting of the kiosks.

iii. Kiosk enclosures may have, but are not limited to, the following:

a. Heavy duty locking mechanisms, hinges, door mechanisms capable of resisting offender tampering and vandalism. Hardware is expected to be contained in the kiosk enclosure.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All kiosk hardware is contained within the kiosks hardened steel casing, which uses heavy- duty hinges and security locks that are easily capable of withstanding use in a corrections environment, including tampering and attempted vandalism.

b. Kiosks will have floor and/or wall anchors. The Offeror will ensure that each kiosk can be easily unsecured from the floor or the wall by authorized CDOC personnel.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

c. The kiosk enclosure is expected to be of a neutral color and easily cleaned/sanitized.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The kiosks' stainless steel shells are powder-coated a neutral gray color and are easily wiped clean using a damp cloth. If needed, common cleaning sprays can also be used for stubborn stains.

d. When applicable, the Offeror is expected to ensure that all openings are secured with detectors where entry might be forced. It is necessary that the Kiosk alarms is expected to be:

- **Manually set to ring for a period of time with shrill alarm;**
- **Capable of activation and deactivation of a remote location designated by the CDOC and proven not to provide false signaling regarding remote alarms.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with the CDOC to install kiosk alarms as necessary.

e. The Offeror will include battery replacement when required.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

f. Kiosks will have sealed opening(s) for power and phone lines as needed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus kiosk has sealed openings and the phone line is not accessible unless unlocked.

F. Kiosk Monitors

i. Kiosk monitors is expected to be Energy Star Compliant with a minimum level of EPEAT Bronze. Monitors is expected to be a minimum of 17" in size across the diagonal, having an associated graphics control board with video drivers.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus kiosk monitors are Energy Star compliant and UL complaint.

ii. Touch screen monitors is expected to be secure, safe and capable of withstanding heavy usage in a correctional environment. It is expected to be scratch and shatter resistant. Offeror is expected to provide any special care required to keep the screen clean, and prolong the viewing and usage life expectancy.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our kiosk includes a built-in LCD with hardened shatter resistant touch screen. The touch screen is UL-60950 and CSA 22.2 No. 60950 ball drop test compliant. The touch screen meets:

- IEC: 60529

- IP: 544
- NEMA: Type 12

iii. Touch screen monitors will not be of the "overlay" or "membrane" type. If a "surface acoustic" or "capacitive" technology is not utilized, the Offeror is expected to provide an explanation of why another technology is being proposed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

iv. Touch screen monitors will reduce the ability to read the kiosk screen when viewed from the side to prevent others from viewing displayed information.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our kiosks have an integrated privacy screen built in to reduce visibility from the side of the screen. The privacy film is built into the screen so that offenders cannot peel or tamper it.

This is screen is beneficial for high traffic areas as it works to keep confidential and private information secure. The screen only allows persons directly in front of the monitor can see the data on screen.

v. Describe proposed solutions for offenders with disabilities (i.e., large print options, text reader options for the blind, and assistive key-stroke functionality for paralyzed offenders).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is well versed with the 2010 ADA Standards for Accessible Design and Securus' installation team will work with the DOC to install our physical equipment to conform to the necessary accessibility requirements. Securus offers a variety of mounting options for the sPhone XL terminal, including wall mount, floor pedestal mount, booth or enclosure, flush mount, and outdoor weatherproofed mountings. The installation team can mount the unit at varying heights to ensure there is sufficient approach, toe, and knee space, taking into consideration all possible reach ranges. The variety of mounting options along with the varying heights will accommodate those with the need for accessibility for mobility impaired or wheelchairs. The sPhone XL kiosk has a movable camera. The standard version allows 30 degrees of variance on the vertical axis. If a greater variance angle is required, this can be accommodated during installation.

Further, Securus can offer cordless phones, hands-free phones or telephones mounted on a roll-around carts for incarcerated individuals with physical challenges.

Securus will provide screens large enough to accommodate the increased text size needed for visually impaired individuals, along with zooming capabilities where appropriate to allow individuals to see text clearly.

Securus has a keyboard with braille keys that can be provided at designated kiosks for use by visually impaired users.

Securus equipment is designed to accommodate hearing impaired users by providing volume controls and assistive listening capabilities.

Tablet Accessibility Features

Securus provides various accessibility features and settings on tablets to meet the needs of offenders. Securus has removed any setting or ability that could impact the safety and security of the facility or the tablet.

Accessibility features include:

- Mono/stereo audio options
- Volume controls
- Modify sound settings
- Hearing aid compatible headphones
- Visual alerts (where applicable)
- Text to Speech
- Screen magnification (zoom in/out)
- Increase/decrease font size
- Ergonomic on-screen keyboard
- Optional clear silicon plug-in keyboard
- Set screen rotation preferences
- Modify screen brightness
- Spell checker

Certain applications have additional customizable settings that can meet various accessibility needs of offender, such as the Movies and Video applications which include closed captioning for many titles in the library.

Securus will provide Closed Captioning where available, adjustable volume controls, hearing aid compatible headphones and visual alerts where applicable. In addition, we will provide headset options that support the Hearing-impaired population that allow for noise cancelling and volume increases.

vi. Kiosks is expected to have a touch screen video display (optional, available if needed) monitor capable of displaying digitized photographs, graphics, and videos, etc.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. Kiosk Configuration

i. Offeror will ensure kiosks are maintained on the most current version of the Offerors operating system, with no more than two versions at any one-time across all kiosks.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

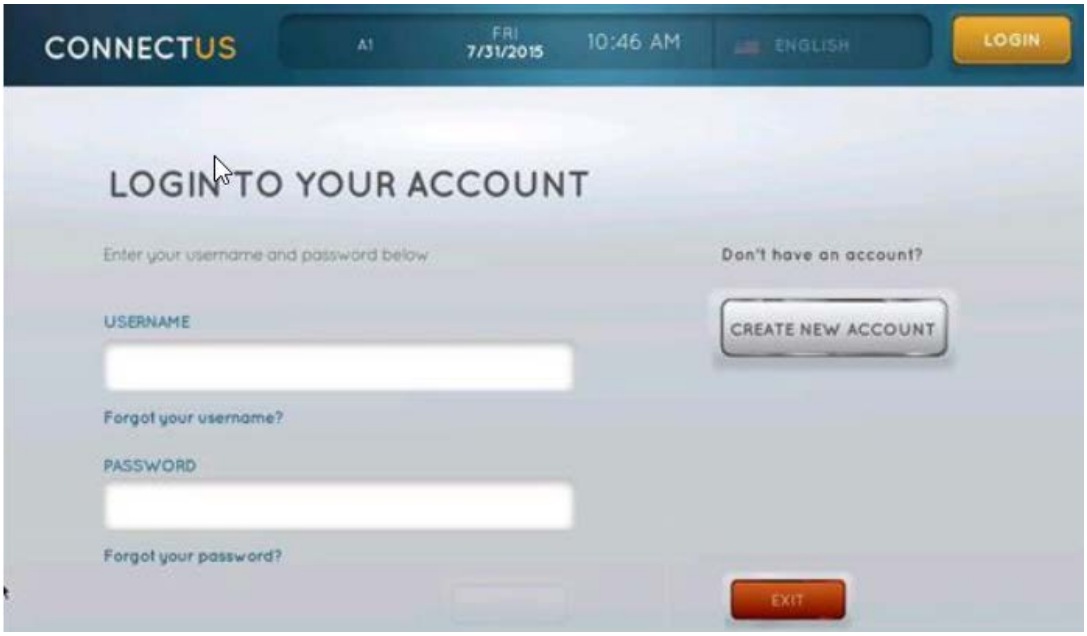
Securus will ensure all kiosks are up-to-date with an operating system version no more than two versions removed from the vendor's current version. Securus delivers software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry.

ii. Offeror will provide a method of ensuring offender ID security. Methods may include fingerprint scan or other biometric possibilities, ID card scanning (magnetic or barcode), PIN numbers, facial recognition, and/or voice options.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our kiosks can be enabled to require offender login to ensure ID security. Offenders create their own personal account for the ConnectUs kiosk, to include key information elements such as username and password, credentials, security questions, and offender photo. The offender's custody account number and PIN are also captured as part of this account creation to allow the account to be tied to the NextGen SCP database.

Before an offender can access their information, services, and applications on the kiosk they will be required to login.



Once logged in, the offender can access any Securus service and application. When the offender logs out, all open services and applications are closed automatically.

iii. Specifications, pictures, artist renderings and drawings of the proposed kiosk design will be included with the proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Technical specifications of the XL Terminal are included in **Securus Attachment No. 8, XL Terminal Technical Specifications**.



iv. Kiosks will comply with the most up-to-date ADA standards for accessible design to ensure ease of access for individuals with disabilities.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide accommodations necessary to comply with the Americans with Disabilities Act (ADA). The Securus program for offenders who are deaf or hearing impaired allows those offenders to place outgoing telephone calls using a text telephone (TTY) device integrated with NextGen Secure Communications Platform™ (NextGen SCP™) or through Video Relay Services (VRS).

Securus is well versed with the 2010 ADA Standards for Accessible Design and Securus' installation team will work with CDOC to install our physical equipment to conform to the necessary accessibility requirements. First, Securus offers a variety of offender phone mounting options, including wall mount, floor pedestal mount, booth or enclosure, flush mount, and outdoor weatherproofed mountings. The installation team can mount the unit at varying heights to ensure there is sufficient approach, toe, and knee space, taking into consideration all possible reach ranges. The variety of mounting options along with the varying height will accommodate those with the need for accessibility for mobility impaired or wheelchairs.

v. Kiosks will have adequate ventilation to include fans if needed for components.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

vi. The kiosk will not bear company names or logos.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

vii. The operating system should allow CDOC the ability to customize the applications offered to offenders.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The ConnectUs operating system on our kiosks provides an "app store" environment where the applications available are customizable.

H. Remote Management

i. At a minimum, remote Keyboard/Video/Mouse (KVM) reset is required.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus maintains the systems so that the agency does not have to reset the mouse/keyboard. Securus has the ability to remotely reset any and all kiosks at the facility.

ii. Offeror to detail remote management capabilities. To include, but not limited to the following:

a. Monitoring;
b. Diagnostics;
c. Error resolution;
d. Software problem assistance;
e. Intelligence reporting;
f. Application and software updates and upgrades; and
g. Rebooting and controlling the remote kiosks from a central location.
h. Remote management should be set through a security access designation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

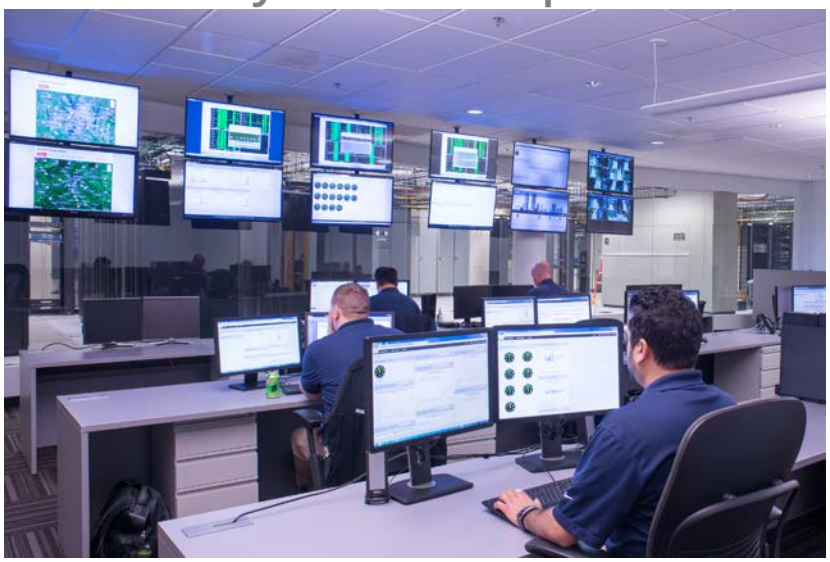
Our Network Operations Center (NOC) technicians continuously monitor and control all hardware, software, and system performance, including the ability to reboot kiosks remotely. This allows our dedicated personnel to diagnose and resolve issues, often before the CDOC notices a problem. If the NOC is unable to remotely resolve a software issue, technicians may be dispatched to conduct onsite repairs. If the team detects that a larger fix is required, Securus collaborates with the account manager and field technicians to resolve the issue. All application and software updates are loaded onto field equipment remotely. These upgrades are vetted by a Change Control Committee, then subject to a rigorous testing phase before being released into the field. JPay monitors and manages the entire process remotely, allowing for zero impact on CDOC resources.

Network Operations Center (NOC)

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring and proactively monitors our systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

Securus Primary Network Operations Center



Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment. The systems are polled every two minutes to ensure proper operation, and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. I

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

I. Offeror to describe how they will prevent any virus or malware from infiltrating the CDOC's system.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Protecting your data: Securus has developed a strong corporate Information Security Governance and Cyber-Security framework using the NIST guidelines, including 800.53 current version. Applications transmitting data across public networks support TLS 1.2 with AES-256 bit encryption. Sensitive data is encrypted both at rest and in motion. Securus provides support for TLS encryption at the application network layer. All web sessions and services are conducted via HTTPS using AES 256-bit encryption. Securus uses a gold-class vendor-provided certificate service for external and internal SSL connections.

The NextGen SCP user interface encrypts and decrypts user page requests, as well as the pages that are returned by the web server. Access to Securus server information is done through HTTPS—HTTP application layering with Transport Layer Security (TLS) as a sub-layer. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks (events where attacker secretly relays, and possibly alters, the communication between two parties who believe they are directly communicating with each other).

CJIS-compliant access: Securus uses an industry-recognized leader to provide remote access to Securus systems within state networks. This remote access system provides secure, encrypted, CJIS-compliant access to Securus systems. Securus also uses a state-of-the-art Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor and protect our network boundaries. Securus infrastructure servers and all workstations require anti-virus protection and receive regularly scheduled security patches and updates

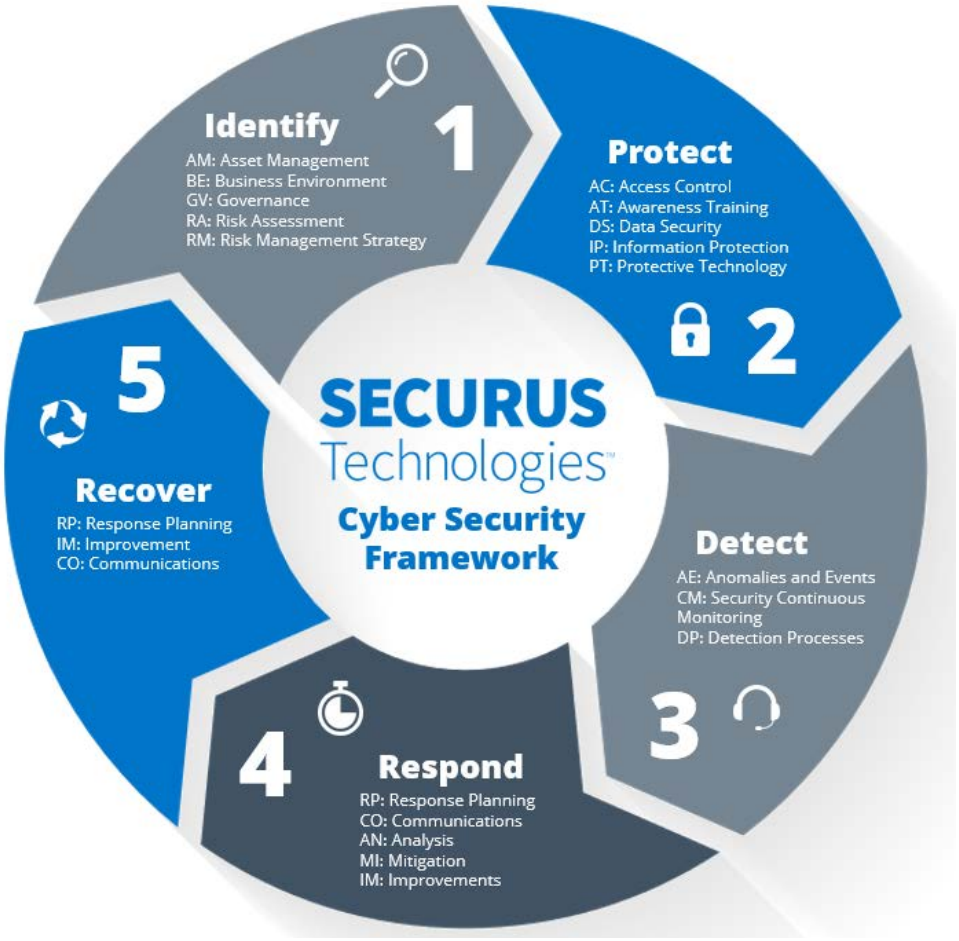
For your team, NextGen SCP can enforce strong password policies for individual with minimum password length, 30-/60-/90-day password expirations, case sensitivity requiring upper- and lower-case letters, and special characters (@, #, $, etc.).

Data Center Security

Comprehensive Security: Securus NextGen SCP is in a carrier-class data center with the most comprehensive security measures in the industry equal to appliable

regulatory and compliance standards. Applications that transmit data across public networks support Transport Layer Security (TLS), certificates, and encryption. Sensitive data is encrypted both at rest and in motion. Securus provides support for SSL/TLS encryption at the application network layer. All web sessions are conducted via HTTPS using AES 256-bit encryption. Securus employs both internal and external certificate authorities to support and secure communications throughout.

J.



Software Expectations

i. The successful Offeror will allow for additional applications to be added as determined necessary by the CDOC. Upon mutual agreement between the Offeror and the CDOC, additional applications can be added via change order to the device while this contract or its extensions are in effect, at CDOC's option.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide a system capable of additional applications to be added as determined necessary the CDOC. By mutual agreement additional applications may be added via change order to the device while this contract or its extension are in effect.

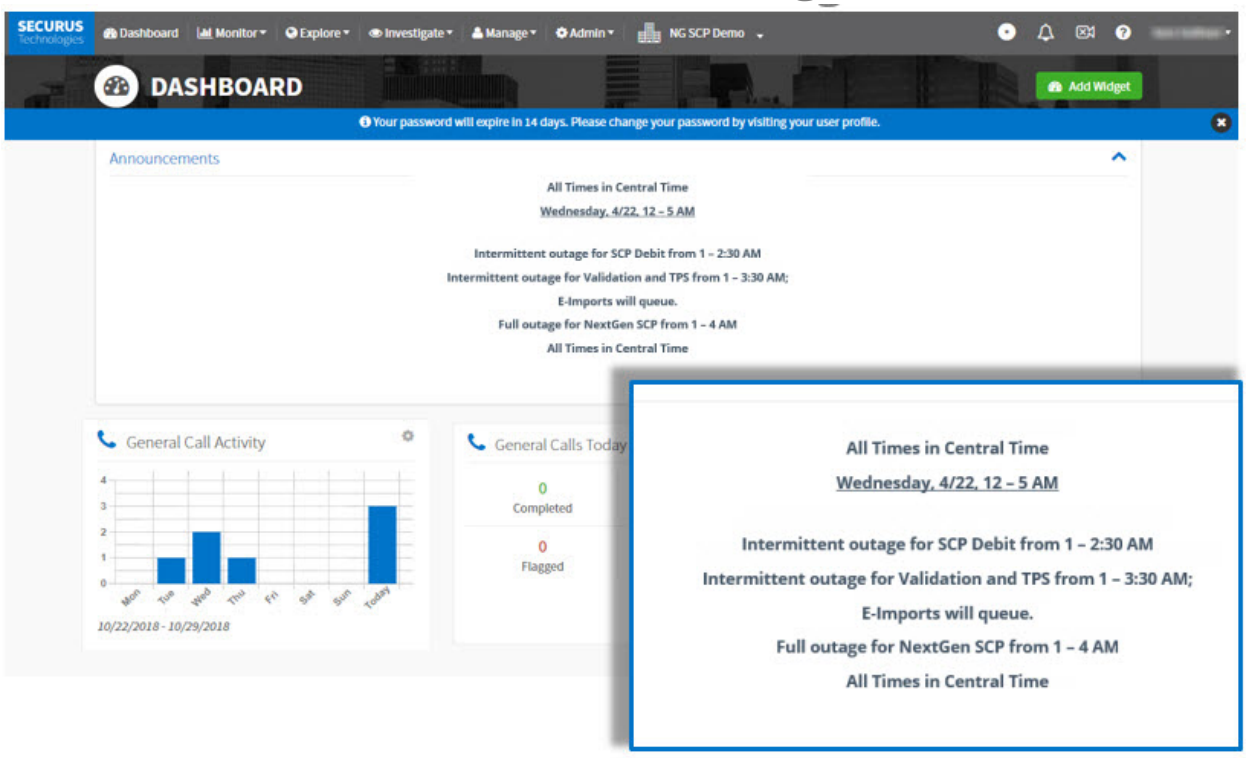
ii. Offeror is expected to provide any and all upgrades that become available during the term of the contract with prior approval from the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCPTM software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



iii. Offeror to describe how they will manage transferring any media including but not limited to streaming subscriptions and approved messages (i.e., text and photos) if new

devices are introduced during the life of the contract and/or if a new Offeror is chosen upon contract termination.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our proposed solution has offenders purchasing and renting media directly on their Unity tablets. If a new tablet is introduced during the life of the contract, all content is easily transferred. The offender will be given a new tablet, instructed to log into the tablet with their credentials to redeem the new tablet and reactivate their tablet subscription through the "Make Mine" process on the tablet. This tablet will now become their own Personal Tablet and their current subscription will continue. The offender will be able to access and download all their previously purchased content from the cloud.

From the Account Tab in the Media store, the offender can view and download all previously downloaded content. Any subscriptions the offender had in place would still be active. Any rentals would also be available as well. They can also download any books or podcasts he had previously downloaded through those respective applications.

Transferring Content to a New Vendor

Securus' content and customer agreements prevent us from transferring licensed content to other vendor devices. In addition, while it may be "technically" possible for Securus to copy previously purchased content onto a portable media device and provide that media device to the CDOC, Securus does not have a process in place to facilitate this today, and we cannot comment on, or guarantee, the legality, feasibility, technical difficulty or potential development effort required to load any such content onto a competitor's device.

We will provide the information you are requesting if we are permitted by the record labels and/or aggregators and if they provide such metadata to us.

iv. Third Party Acquisition of Software: Offeror will notify the Department in writing if its intellectual property, business, or all of its assets are acquired by a third party.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

v. Title of Software: Offerors submitting a proposal represents and warrants that it is the sole owner of the software or, if not, the owner, has received all legally required authorizations from the owner. Offeror to provide the following documentation:

a. Terms of software license.

b. Rights to computer software

- **Documented Interface API and tool kit ad.**
- **Custom changes to the Interface API.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus warrants that it is the sole owner of the software. All of Securus kiosk software is proprietary and built in-house, so no license or additional documentation is needed. For tablet-based software, Securus uses an Android Open-Source Project (AOSP) content license.

K. Interfacing

i. Offeror to detail their capability to interface Offerors applications to CDOC applications.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has extensive experience interfacing with both off-the-shelf and custom-designed CDOC (and outside vendor) applications. Securus has interfaced with hundreds of systems, large and small, and is more than capable of interfacing with any participating CDOC.

Integration

The Securus Integration Team works with 200+ vendors worldwide and 60+ independent, facility-owned systems, and shared databases. We make connections so that your communications, management, and banking technology works together.

Your Securus Integration Team designs, develops, tests, and integrates the Securus system with CDOC vendors and banking systems. This process is part of the overall Project Plan for the installation of the NextGen SCP™. Major milestones include:

- Collect preliminary needs/ requirements
- Have contract signed
- Finalized requirements
- Approve the Statement of Work
- Finalize design document
- Schedule customer implementation
- Develop custom integration solution
- Test custom integration solution
- Implement custom integration solution
- Customer approval and sign-off

Securus integration specialists consult with your IT departments or system providers to determine the best integration strategy for each specific application. **All integrations occur over secure connections** usually with the following technologies: SOAP Web

Services; HTTP; FTP push or pull of files in any textual format; JSON; XML-RPC; and TCP Sockets. Securus can modify your data format for migration into our platform, without costly code modifications.

ii. Data transfer in Offerors operating system. Offeror to include specifications for Extensible Markup Language (XML) or other standard interface options, to tie in a kiosk-based application with offender management systems.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus kiosks use web services to communicate with back office. Those web services can be used to tie in a kiosk - based application with offender management systems.

iii. Security and capability when interfacing to a CDOC application.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will integrate with the CDOC in a thorough, secure manner through multi-layered security protocols implemented at all levels of the network and its applications. Securus utilizes a defense-in-depth security strategy, architecting the network into security zones at appropriate levels, while protecting and segregating users, applications, and databases. We enact strong access control policies that restrict access-based roles and policies to data and systems. Securus enforces strong, complex passwords and multi-factor authentication (MFA) across our enterprise networks and systems. Securus deploys and manages next-generation firewalls configured with highly restrictive access control lists (ACLs) which limit network traffic to pre-approved systems, and prevent Internet access per Correctional industry guidelines and standards. The network is monitored for anomalous traffic twenty-four hours a day, every day of week and year (24x7/365). Deep collaboration between Securus' in-house Cybersecurity Incident Response Team (CIRT) and managed security service providers (MSSPs) provide continuous monitoring and rapid detection and response capabilities at all times. Securus monitors network traffic and changes to standard configuration settings for tablets, kiosks, and local download managers (LDMs). If a setting has been changed, or if there are attempts to bypass security controls in place, alerts are generated and reviewed by the Securus Cyber Incident Response Team, and action is taken on an as-needed basis.

L. Customer Interaction Messages

i. Messages are available in English and other languages as requested by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our kiosks have multi-lingual support. ConnectUs can display notifications, confirmations and labels in multiple languages based on an offender's user language selection.

ii. Provide application instructions to the offenders which are clear and to the point, with no large blocks of text.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide durable instructions in English, Spanish, and any other languages specified by the CDOC. These instructions explain the process in an easy-to-read manner for all offenders. As a security measure, Securus will use materials and techniques appropriate for the corrections environment.

Additionally, instructional documents and videos can be published to the kiosk to educate offenders on application use.

M. Scalability

i. Offeror to recommend number of offenders to kiosk ratio and how their system can adjust based on changing offender populations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus normally installs kiosks at a kiosk-to-offender ratio of 40:1 or better. However, depending on the facility's layout, Securus will work with a lower ratio. If a housing unit's population increases, or if demand is such that more kiosks are needed, Securus will install additional kiosks to meet the CDOC's need.

Immediately following contract award, Securus' deployment team will conduct site surveys of each facility to determine optimal placement for the offender kiosks. Considerations include access to proper connectivity as well as security and ease of offender movement.

ii. Provide all assumptions used to identify required computing power and/or hardware.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus installation team doesn't make assumption as to what is required to provide the proper computing power or hardware. Instead, Securus identifies the required computing power and hardware based on site surveys conducted upon award and our 30+ years' experience with similar installations. Securus can expertly size each

implementation accurately according to data gathered during site visits and discussions with CDOC representatives.

Securus conducts comprehensive site surveys to gather required information in order to implement our products and services. During these site surveys, our installation team determines, based on max bed count, the number of phones, video terminals, and Wireless Access Points (WAPs) required as well as Intermediate Distribution Frames (IDFs), cable paths, switch counts, UPS requirements, and other information to ensure a successful deployment.

iii. Offeror will ensure that the system architecture is scalable and designed to easily accommodate changes (future applications, etc.) resulting from CDOC rules and workflows.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All of Securus' systems are completely scalable with the ability to increase server number and size to accommodate changes and increased workflows.

Scalability of our Central Processing System and Network

Securus communications system, encompassing telephone, video and tablet service, is a centralized system which provides centralized management services at the Securus data center for all of the telephones, kiosks and tablets within the customer facility.

The network for our communications system maintains twice the capacity of normal calling volume to prevent blocking of outbound calls and busy signals and also maintains twice the capacity of normal video volume to prevent blocking of inbound video and support the quality of the audio/video streaming.

The central processing system and its network capacity can scale to many times their current capacity within the current architecture and design. Securus monitors system 24 hours per day, seven days per week, every day of the year. When concurrent telephone call volumes and video session volumes consistently cross 80% of the available capacity, additional infrastructure is added to our central processing system to augment the capacity. Securus adds additional circuit bandwidth to each site and the central data center when necessary.

The on-site tablet servers and network equipment are scaled to provide sufficient capacity and network bandwidth to accommodate expected tablet usage for all tablets within the facility. The central data center is designed to scale beyond the current capacity based on the needs of our customers. When concurrent tablet traffic consistently cross 80% of the available capacity (either at the customer site or at the central data center, additional infrastructure is added to augment the capacity. Since

the system capacity is managed to keep ahead of the usage of tablets as well as additional features and services on the tablet, the customer has the flexibility to increase the number of tablets and services enabled at a facility as needed.

Scalability of Storage

Securus stores call recordings in centralized, disaster-resistant, carrier-class data centers. The NAS architecture of our data centers delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network.

The Securus NAS has more than seven petabytes of storage space in each carrier-class data center and is continuously monitored and managed through automated processes and storage policies. When these very large storage systems approach designated thresholds, Securus expands capacity to ensure all authorized communication records and recordings are retained in secure, disaster-resistant locations.

iv. Provide the capability of producing reports, including but not limited to:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Identify trends, investigate suspicious activities, and manage usage: The NextGen SCP retains communication detail records on all communication attempts and events. NextGen SCP has a report writer that provides investigative information based on the communication detail records. CDOC may search and analyze details on all communication events through NextGen SCP and then run reports to identify communication trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

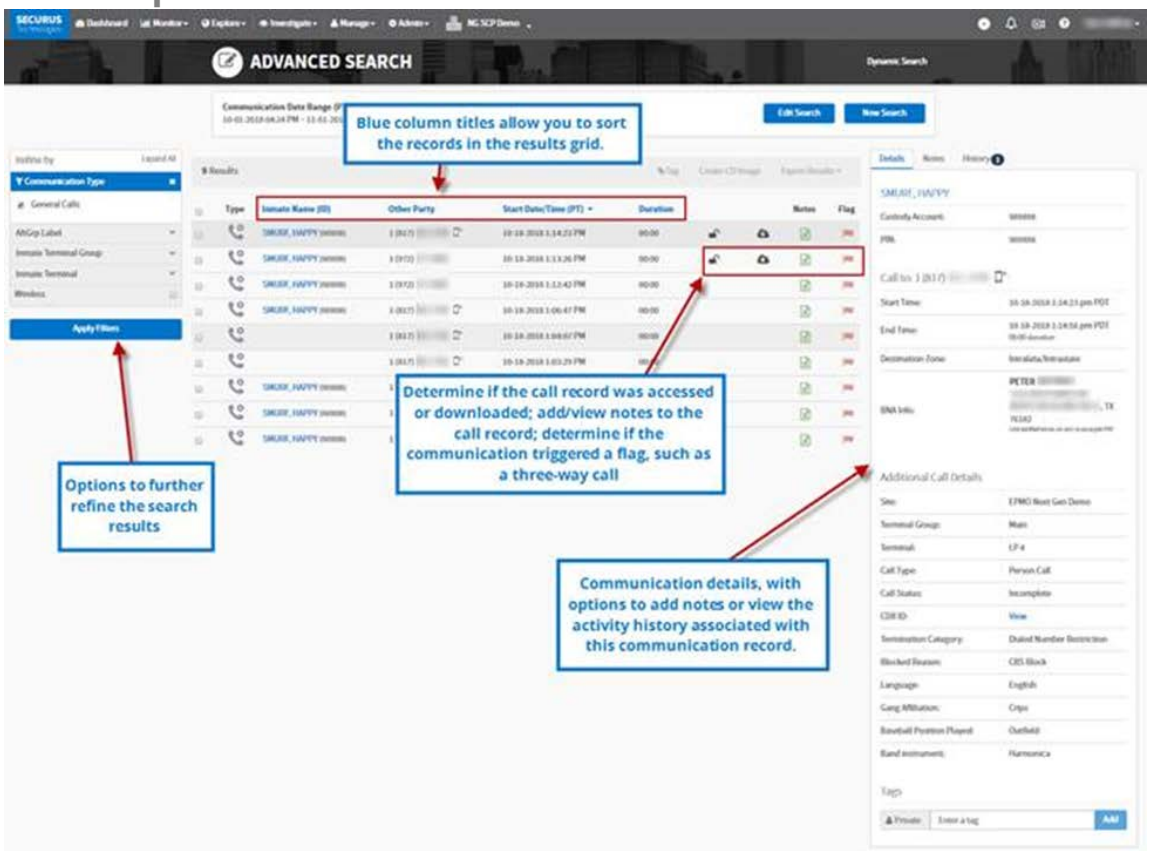
Custom and standard searches worth sharing: NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on an extensive list of criteria options. CDOC also may create customized reports by changing search criteria. After search results are generated, you can sort based on any of the communication event details. Then, with a single click, the data exports to Excel, CSV (Comma Separated Values), or Adobe PDF format and may be saved, printed, or emailed to others.

NextGen SCP™ Report Criteria Fields
▪ Date Range ▪ Identifier (ID, PIN, Name) ▪ Continuous Voice Identification ▪ Communication Type (Calls and Video)

NextGen SCP™ Report Criteria Fields

- Communication Status (Complete or Incomplete)
- Prepaid Account Number
- Destination Number (Partial or Full Number Entry)
- Call Type
- Three-Way or Remote Call Forwarding Detected
- Watched Status
- Wireless Indicator
- Visitor and Visit Type (SVC)
- Visitor Contact Number
- Visitor Identifier (ID, Name, Email)
- Phone or Terminal Location
- Number Restriction and/or Status Assignment
- Broad Search with No Data Entry
- Suspected Fraudulent Call Activity
- Destination Zone (Local, Interlata, Interstate, Intralata, International)

Sample Communication Detail Results Screen



a. Use and statistical reports by function.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen Secure Communications Platform™ (NextGen SCP™) is very flexible and easy to use and allows the user to create almost limitless reporting. Using the dynamic filters of our reporting tool, authorized users can refine search results to create the desired reports.

Should customized reports be needed, Securus will provide them to the CDOC at no charge except in those cases where the customized report would require a significant allocation of resources or material changes to Securus systems and procedures.

In the small number of instances where development is needed (e.g., capturing additional information from other systems), Securus will provide the development free of charge unless the request involves significant cost to Securus. In such cases the

CDOC will be given the option to pay for the additional services without markup by Securus.

b. Accounting reports;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

c. Kiosk Operational Statistics to include:

- **At minimum, internal operational software.**
- **Ability to look at up-time logging data and monitor kiosks.**
- **Full monitoring capabilities; KVM/Power.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Internal operational software is proprietary. Performance is monitored at all times by OUR Network Operation Center (NOC). Securus utilizes a VPN to control kiosk CPUs remotely, which allows the kiosk to be maintained, rebooted, and upgraded as needed. All events are recorded and easily audited.

- **Touch Screen buttons and font sizes large enough to be easily read by the majority of customers.**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The touch screen of the Securus sPhone XL kiosk contains all buttons and fonts large enough to be read easily by the majority of offenders. Aspect rations can be adjusted to increase font size if needed.

N. Offerors are to describe in detail the following:

i. Transaction processing messages;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Through the NextGen SCP user interface, authorized users have a window into all of an offenders actions and transactions performed not just on the kiosk, but across all of Securus' services statewide. The NextGen SCP UI provides the tools to see offender purchases, requests or forms submitted including grievances, communications, and more.

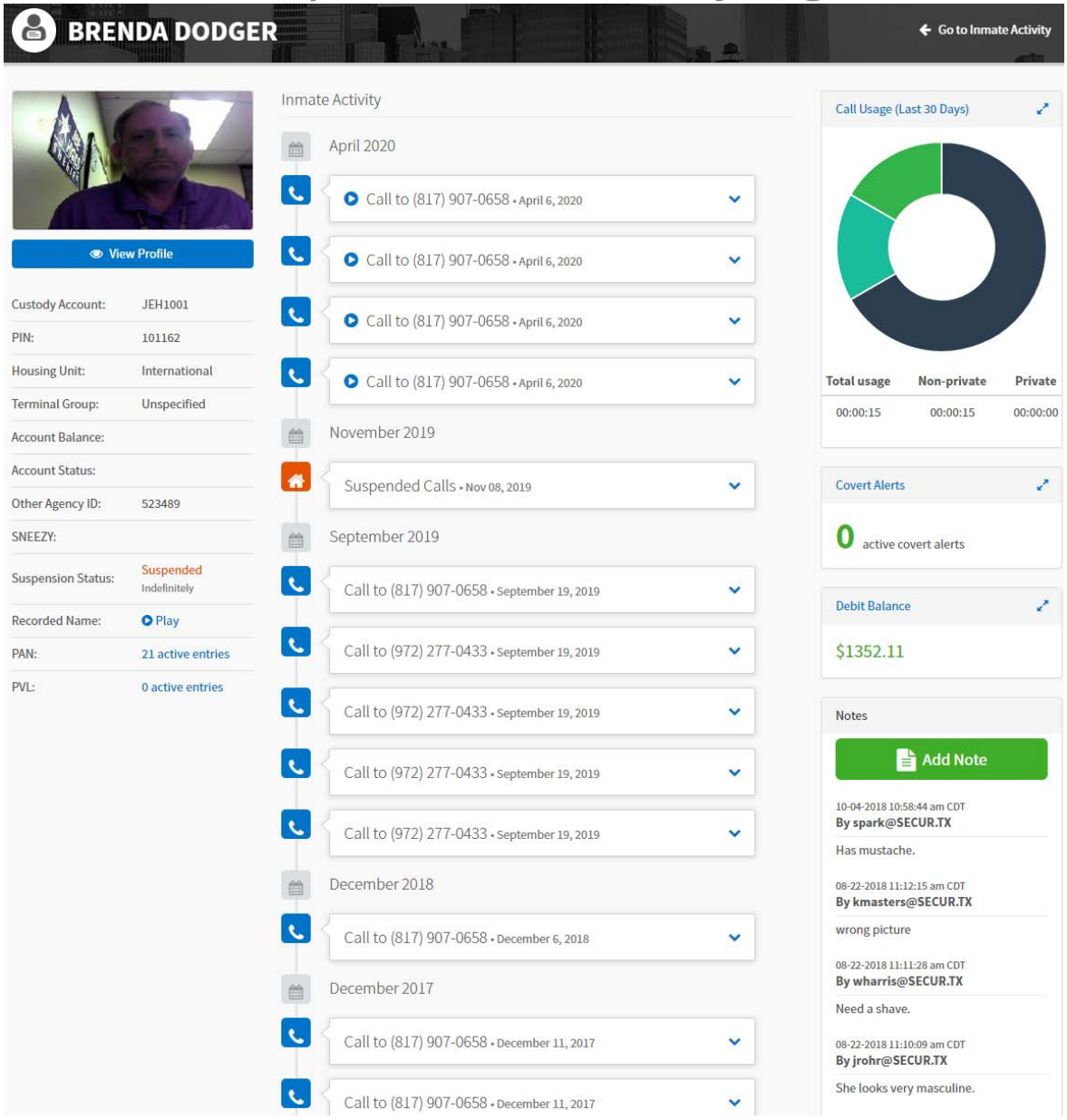
Offender Activity Page

The Offender Activity page allows the user to explore an offender's activity, calling and visitation details, and important information about a specific individual through an offender dashboard.

The offender dashboard compiles data from various sources that show the offender's communication activities—past, present, and future (scheduled)—in a single location.

Summary information for other offender activities and notes, along with tools to that allow for the easy management of restrictions, are also provided.

Sample Offender Activity Page



Debit Transaction Reporting

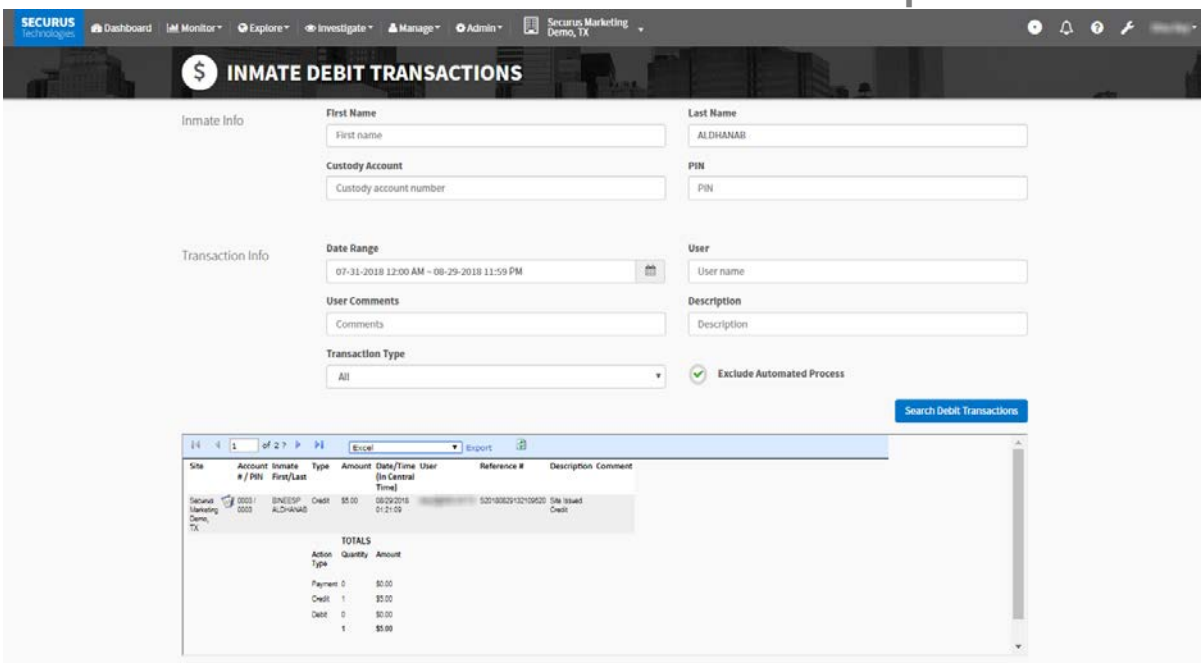
Authorized CDOC personnel have real time access offender account balances and purchase information through the offender debit balance report. The Offender Debit

Balance Report shows all offender debit account activity, including stamp and media purchases, and account balances.

The NextGen Securus Debit Report enables users to:

- Query Securus Debit call detail records (CDRs) by the user-specified criteria
- View all debits and credits that occurred during a specific period for a specific offender, for all offenders within a facility, or for all facilities

Securus Debit Transactions Report



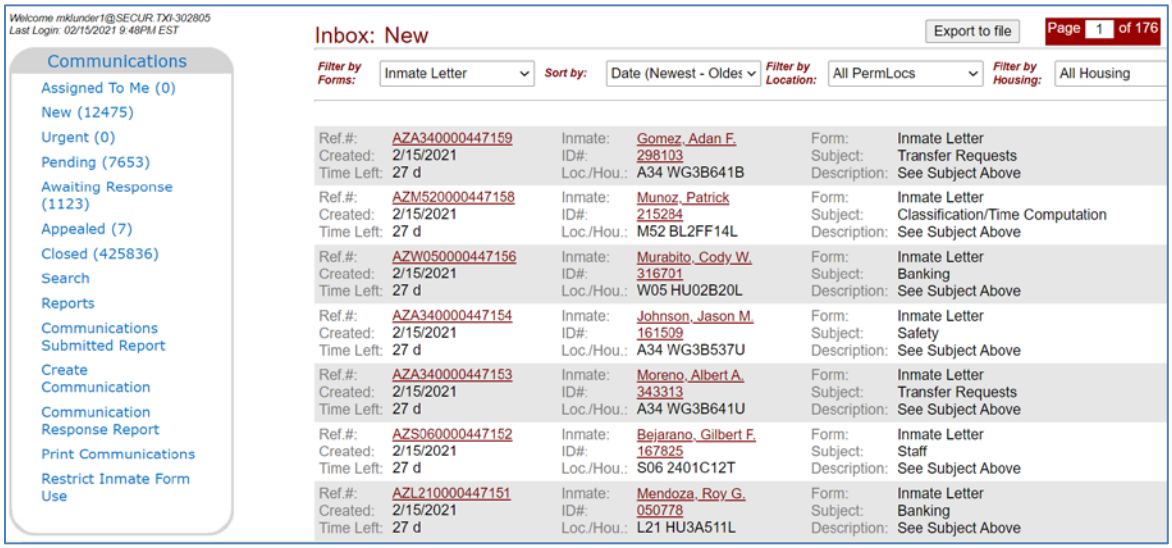
eMessaging Review

From the eMessaging facility portal, authorized staff can review all messages and attachments. The facility can also choose “Auto Release” if the message does not trigger any of the configured security controls. If your security controls are triggered, then you have an opportunity to review the flags and approve/reject the message.

Offender Requests Review

From the staff side, each user has individual access rights so that they can view and respond to the specific forms. Within the system there are also several specific functionalities unique to the staff, such as comments and categorizations not shown on the tablet, detailed search and reporting, and the option to add attachments.

Facility Grievances Interface



ii. What messages prompt the offender during their time on the OCS equipment;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

We designed our systems to be intuitive and easy to use, meaning that our kiosks use pop up boxes and messages to guide the offender through the use of our kiosk. The applications on the kiosk will only display information pertinent to the offender. For example, if an offender is trying to schedule a video connect session, they will only be presented with the available time slots for the terminal, or if they are using the forms and grievance application they will only be able to choose from the available forms and the onscreen key board only displays when there is an open entry box available. Other examples of prompts include but are not limited to:

- Popup messages warning the offender that the terminal has been reserved.
- Informational message of an upcoming even on the terminal
- Warning that a visitation is being recorded and may be monitored.
- Timer on the bottom of the screen indicates how much time remains in the offender's kiosk session
- Confirmation of submission of a form or other transaction

iii. Error message, can the error message be customized?

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Select error messages, on both the inmate- and customer-facing interfaces, can be customized to meet CDOC's specifications.

iv. Does functionality include instructional prompts?

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with the CDOC to configure the system to meet the facility's needs, including the appropriate prompts. Additionally, instructional information from the CDOC can be included on the kiosk through the video education application and inmate handbook application. The kiosks allow an inmate to use multiple applications at the same time, meaning they can use an application while reading some instructional material as well.

Securus' attention to detail is evident: the user interface is easy to use and self-explanatory. Securus provides an "Intro" video on every terminal to allow the inmate to view an instructive video explaining how to use the system. Instruction documents may also be published on the terminal for inmates to view.

14. WIRELESS TABLETS

A. Tablets is expected to be a corrections-grade device (i.e., tamper-proof seal to easily identify offender alterations). The Offeror will provide detailed specifications for proposed tablet(s).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides ruggedized tablet devices, designed specifically for corrections, that have been "locked down" to prevent access to unauthorized usage. Securus' Unity tablet is a customized Android 8.1 OS tablet. The Securus Unity Tablet hardware incorporates the following features and specifications.

Features:

- Ruggedized Casing
- High strength, impact-resistant security glass w/ integrated screen protector
- Barrel charge port
- Pogo pin connector
- Secure WiFi
- Built-in FM Radio Receiver



Specifications:

- Internal Storage: 32 GB
- CPU: MT8163 - Quad core cortex A53 Frequency 1.3G, 64bit CPU
- Resolution: 1280 x 800
- Dimensions: (L x W x H) 7.8" x 5" x 0.61"
- Weight: 17.2 Oz
- Battery: Lithium - 500 cycles, includes temperature sensor
- Dual WiFi Bands (2.4GHz and 5GHz)

Environmental Conditions:

- Operating Temperature Range: 50o F to 110o F (10o C to 43o C)
- Storage Temperature Range: -40o F to 150o F (-40o C to 65o C)
- Humidity: 95% RH (relative humidity), non-condensing

JP6S Ports and Physical Buttons



The following table lists the complete JP6S specifications.

Item	JP6S
OS	Android 8.1
CPU	MT8163 - Quad core cortex A53, Frequency 1.3G, 64bit CPU
GPU (Graphics Processing Unit)	Mali-T720 MP2 GPU
DDR	2G - 512*4
Battery	8000mAh
LCD	Resolution: 800*1280
Boot On - mA during boot on	500-750 mA (LCD on)
Stand by: Stand by current on main window	300-400 mA (LCD on)
Music: Listen to music w/ ear bud plug in	380-400 mA (LCD on)
Movie: Play movie w/ ear bud plugged in	450-550 mA (LCD on)
FM: Listen to FM w/ ear bud plugged in	300-400 mA (LCD on)
Back Light	380 mA

Item	JP6S
USB (OTG)	400 mA
Stand by time	About 22hrs with LCD on About 350hrs with LCD off
Play MP3	About 20hrs with LCD on About 140hrs with LCD off
Play Video	About 13-14hrs
Storage	32GB
Buttons	Power, volume up, volume down
5G	Dual support for 2.4G and 5G
Camera	2 Mega Pixel
POGO PIN	Yes – charging and mounting

B. Tablets will meet all NEMA and UL ratings for ADA offenders.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Tables meet all NEMA and UL ratings for ADA offenders.

C. Offeror will provide a minimum of 1:6 ratio of tablets to offender (Offeror to recommend number of offender to tablet/kiosk ratio and how their system can adjust based on fluctuating offender populations).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide a 1:1 ratio of tablets to offenders.

D. The tablet device will be secure for all corrections environments to access a secure Wi- Fi network within facilities and allow the use of applications including but not limited to:

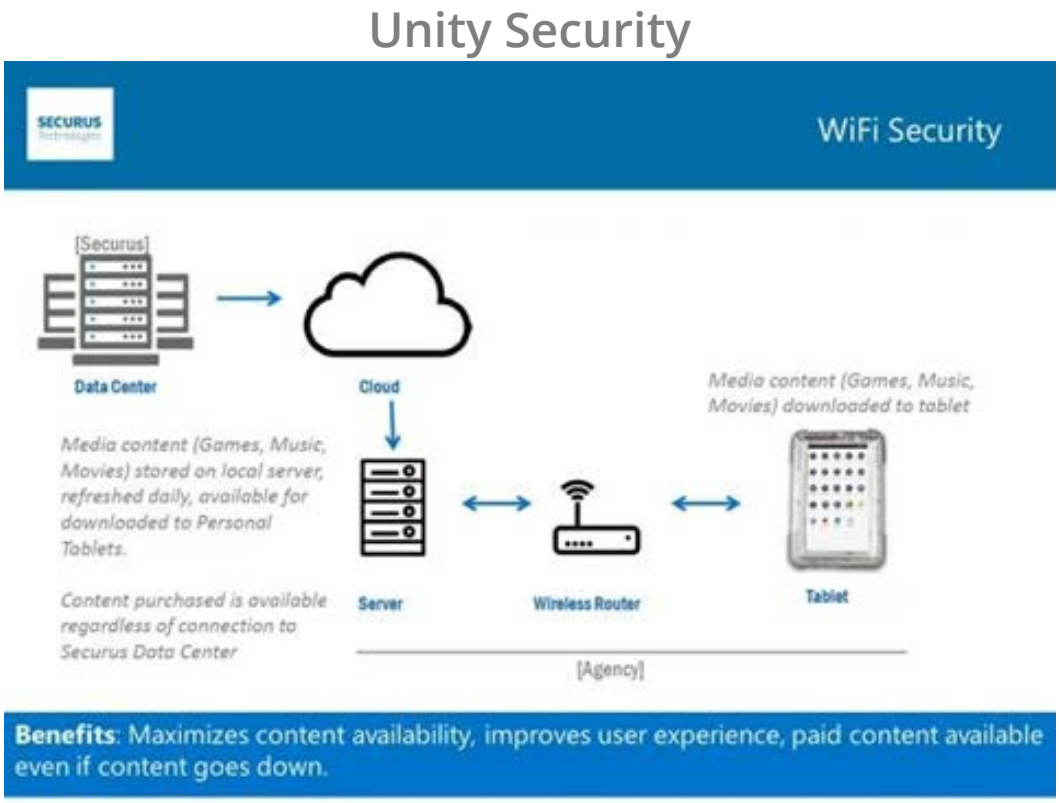
i. Education and self-improvement programs
ii. Email/Secure messaging, including photo attachments
iii. Video messages
iv. Video visitation
v. Offender commissary ordering.
vi. CDOC-initiated messaging services
vii. Media/Music subscription services
viii. E-books
ix. View account balances

x. **Law library access**
xi. **Games**
xii. **Podcasts**
xiii. **Newsfeed**
xiv. **Movies**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Both Unity tablet hardware and software have industry-best security practices. Internet access is restricted, ensuring users cannot surf the Internet or communicate through unauthorized channels with anyone outside of the facility.

Wi-Fi networks and on-premises equipment are monitored 24x7 to detect attempts to circumvent security controls.



Attempts are detected and responded to 24x7. Customers are notified of any unusual activity on tablets and kiosks as quickly as possible.

Securus provides multiple layers of security to ensure proper tablet usage and to prevent security breaches or tablet misuse.

Security Layer 1

Tablet Firmware

Securus Unity Tablets run a custom-developed proprietary firmware to harden their security and prevent any access to unauthorized content by the offenders. The customized firmware does not have any of the common apps that are found on consumer-grade tablets.

The following security measures have been taken to harden the firmware on these tablets:

- Browser, contacts, calendar, native phone, and messaging clients have been removed.
- The option to change configuration settings has been removed.
- Near-field Communication (NFC) and Bluetooth have been disabled, except for Wi-Fi (where applicable/approved).
- Authorized applications are pushed to the tablets through Securus' app state management process, thus preventing offenders from installing or un-installing apps.
- Tablets are prevented from accessing the public internet directly.
- Tablets are prevented from accessing third-party app stores.

Wi-Fi Access

The firmware only allows the tablets to connect to a Securus-provided network using a unique SSID (Service Set Identifier) for Wi-Fi. Security mechanisms prevent the tablet from connecting to any other Wi-Fi network other than the one provided by Securus for exclusive use by the tablets.

Securus uses Wireless Access Points (WAPs) that are customized only to broadcast the SSID to supported Unity Tablets.

Security Layer 2

Securus Local Platform (SLP)

All the WAPs are connected to a Securus Local Platform (SLP) running Securus' custom-developed proprietary software. These SLPs have components that inspect all the network packets and provide firewall, transparent proxy, DHCP, DNS, and routing services for the tablets.

The Securus Local Platform is essential to all tablet functions. The SLP is configured to govern what the tablets can access. The tablet cannot receive any content from a network that the SLP has not been configured to provide. The SLP inspects all tablets' traffic and ensures that access is granted only to authorized content.

Although a tablet can connect to the Wi-Fi network, it cannot obtain an IP address unless it is recognized as an authorized device by the SLP. If a tablet is not known by the SLP, it will *not* be granted access to the wireless network and will be rendered useless for applications that require network connectivity.

The SLP at the facility premise is connected to Securus' Data Center over an Internet Protocol Security Virtual Private Network (IPsec VPN) tunnel. The IPsec VPN service provides secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

Security Layer 3

Data Centers

Securus maintains a presence in two data centers in two geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.99% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier 4 (highest availability) data centers, including:

- Multiple power delivery paths
- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in, dual-door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Securus applies a high level of security to protect against cyber-attacks, and to secure its data. Applications transmitting data across public networks support SSL/TLS, Certificates, and 256-bit AES encryption. Routers, switches and firewalls are used throughout the network to protect Securus and our customers. All servers, laptops, and workstations require anti-virus and anti-spyware protection software and the latest operating system patches.

Sample Applications

Securus tablets offer a wide range of applications designed for multiple purposes—many of them focused on offender rehabilitee and preparedness for re-entry. Some of those are described below.

Access to Music, Books, Education, & Games

Securus partners with some of the largest content aggregators, publishers, and creators to deliver the largest library of officially licensed premium media content.

To ensure security levels appropriate to the corrections industry, Securus stores these materials in our Tier IV data centers, which deliver content to secure onsite content management servers. This model ensures that only authorized, approved content is available on Unity Tablets.

Unity Tablets run on a custom-developed proprietary firmware that prevents access to unauthorized content by offenders. The firmware on Unity Tablets provides multiple protections to maintain security and protect against offender abuse, including the following safeguards:

- Removing browser, contacts, calendar, native phone, and messaging clients
- Removing the option for the user to change the settings
- Disabling any access to NFC, Bluetooth, and cellular wireless radio, except for Securus' Wi-Fi
- Preventing users from installing or un-installing apps. Authorized apps are pushed to the tablets through Securus' app state management process.
- Removing access to third-party app stores

Wi-Fi Access

Unity firmware only allows the tablets to connect to a Securus-provided unique Service Set Identifier (SSID) to ensure that offenders only have access to authorized content and information.

Downloading

Programs, movies, educational content, and games are accessed and downloaded to Unity Tablets from Securus' Tier IV data centers. There are no bandwidth or location issues as there are when streaming from an outside internet service/source, and the security of the offender's access to data, sites, and information is protected by the firmware within the Unity Tablet.

Other tablet providers are known to have used unlicensed or standard consumer streaming applications. These applications lack filtering tools that are necessary to ensure only appropriate content is available and to maintain proper levels of security.

What to ask: *Ensure media content is appropriate by asking "do you have direct contracts with content providers or content aggregators that authorize you to filter and distribute music, books, education content, games, and movies?"*

The following list provides a summary of the applications and content available on Personal Tablets:

- **Phone** – Allows the tablet to function as a fully-integrated extension of the Securus' NextGen SCP™ platform. All features and restrictions of NextGen SCP will still apply.
- **eMessaging** – Two-way, corrections-grade digital messaging platform with facility regulated monitoring and control capabilities, as well as intelligence gathering opportunities.
- **Digital Mail Center** – Physically scanned mail delivered through tablets, reduces contraband entering the facility through the mail.
- **Media Store** – Modern premium media and entertainment options available at affordable prices.
- **Music** – Millions of songs available in multiple genres of music, such as, Country, Gospel, Rock, Pop, and more.
- **Games** – 850+ games and growing – a wide selection of titles at a low cost to offenders.
- **Movies** – Non-explicit content only and many popular movies and TV shows available.
- **Newsstand** – Digital news subscription service allowing access to information on current events.
- **eBooks** – The largest library available with access to over 50,000 titles.
- **KA Lite** – Self-paced preloaded educational platform with access to thousands of videos and exercises providing the complete education experience.
- **Lantern** – Full-service Learning Management System (LMS) that offers blended learning experiencing through interaction with educators and content providers.

- **Mental Health & Addiction Recovery** – Dozens of resources designed to assist with anxiety relief, depression assistance, guided meditation, thriving after addiction, alcoholism, opiate addiction, twelve-step programs, and much more.
- **Religion** – Access to Holy Books, sermons, teachings, and practices for a wide range of faiths and beliefs.
- **Job Search & Prep** – Daily updated job postings allow offenders to begin their search for employment following release. Additional programming is available to teach offenders important skills for finding employment.
- **Law Library** – Provides offenders with up-to-date legal information allowing them to perform comprehensive legal research.
- **Commissary** – Provide access to commissary ordering (with vendor agreement).
- **Forms and Grievance** – Fully automate the process of offenders submitting requests/forms via an easy-to-use interface with real-time access to both current and past forms and updates.
- **Viewer** – Display all facility documents and videos (e.g. Handbooks and PREA).
- **TYRO** – The Securus exclusive TYRO application provide access to programming that focuses on maintaining family bonds, life skills, and additional topics that assist in the re-entry process.
- **Services** – A staff to offender communication tool that allows administrators to post real-time notices, policies, procedures, and messages to one, a group of, or all tablets within the agency.
- **FM Receiver** – Provides the ability to listen to local corrections broadcasted audio.
- **Chasing the Dragon Movie** – A documentary developed as a resource to educate offenders on the dangers of opiate addiction and how it destroys lives.
- **Clock**
- **Calculator**

Descriptions of Available Tablet Applications

Job Search

Securus' Job Search application, **Jobview**, is specifically designed for use in the correctional environment. Jobview gives offenders secure access to over 2 million daily updated job opportunities. Each month, over a million job searches are conducted from the hundreds of correctional agencies where Jobview is available and being used today.

With Jobview, offenders have free and unlimited access to search for employment opportunities directly through their Securus Unity Tablet. The application's intuitive design requires no staff involvement, freeing up critical time and resources to focus on other needs of the correctional facility.



Screenshot of Jobview on Tablet

As an added benefit, Securus provides monthly reporting that tracks ongoing usage of Jobview allowing you to easily review the job search activity of the offenders at your agency.

Securus' exclusive secure job search app is already being utilized by hundreds of correctional facilities to allow individuals returning to society the ability to search for employment opportunities and prepare for a successful reentry.

Additionally, Securus Unity Tablets supplement the job search capabilities with free content that focuses on finding employment such as interview tips, how to create a resume and more.

Law Library

Through the Law Library application, offenders have secure digital access to millions of legal publications, documents, and resources at no cost. Federal and State materials are both accessible, using intuitive search capabilities that allow the user to pinpoint the information they are seeking. Providing access to Law Library through tablets can help you maintain compliance with legal and mandatory requirements to

provide offenders access to the courts (Supreme Court ruling in Bounds v. Smith (1977).)

Securus has worked directly with each Law Library vendor to ensure that the Law Library platforms are secure and locked down before being allowed on tablets.

Although Securus can enable the law library application for use by the vendor of your choice, **Securus is proposing the Casemaker law library solution (inclusive of licensing fees) at no cost to CDOC, saving the agency thousands of dollars a month in the current library expenses.**



Securus' tablet program can provide additional flexibility that allows your agency to have complete control over when the application is available on offender's devices. Through Securus' **Command & Control Officer Tablet**, agency administration can choose when and which devices have access to Law Library. Additionally, staff can be provided administrative access to the Law Library at no additional cost.

Podcasts

Securus' Podcast app provides access to a catalog of 600+ series and tens of thousands of hours of content that can be accessed through an offender's Securus Unity Tablet. Unlike other tablet providers that charge for access, Securus has recognized that podcasts deliver a significant amount of content that can improve the lives of offenders. Therefore, Securus allows this content to be accessible **at no cost!**

Securus has focused on providing a well-rounded catalog that is constantly growing with several new options each month.

Screenshot of Podcasts Landing Page



Offenders can access free programs that cover topics such as:

- Addiction Recovery
- Education
- Employment
- Mental Health
- Personal Development
- Personal Finance
- Religion & Spirituality
- And more!

Every podcast is screened and reviewed prior to being made available to ensure content and subject matter is appropriate for corrections.

Securus Originals – In addition to the hundreds of popular podcast series and thousands of episodes, Securus is working with corrections industries experts, success

stories and others to develop Securus Originals. These programs are designed and curated with the incarcerated population and are available **at no cost.**

Education

As an added benefit to the offenders, Securus has partnered with Ashland University, Prison Entrepreneurship Program (PEP), and God Behind Bars, to provide customized solutions.

These partnerships provide opportunities to create positive outcomes for post-incarceration. **Securus has included with our offer the opportunity to provide some of our premium services at no cost as a reward system to offenders who complete designated coursework.** We look forward to working with CDOC to build a program that maximizes utilization of the education content we provide.

KA Lite



KA Lite is a **user-friendly *offline* education application** that allows offenders to access more than 6,000 **K-12 educational content** options such as math, science, history, computing, and much more. KA Lite offers practice exercises, instructional videos, quizzes, and test prep. CDOC will have control over the subjects available to the offender.

KA Lite offers self-paced learning, suiting multiple learning styles and needs. Offenders can work at their own pace, allowing harder concepts to be practiced more efficiently. Offenders can plan their use around any schedule. Self-paced learning puts the ownership on the offender, forcing them to have internal motivation and learn time management skills. There is no cost to agency or offenders for this product.

Via a **personalized dashboard**, offenders can take courses, take practice exercises and quizzes, track progress, and explore real world applications. KA Lite provides an up-to-date educational curriculum based on **Common Core Standards**, offering thousands of instructional videos and interactive exercises.



Languages Available:

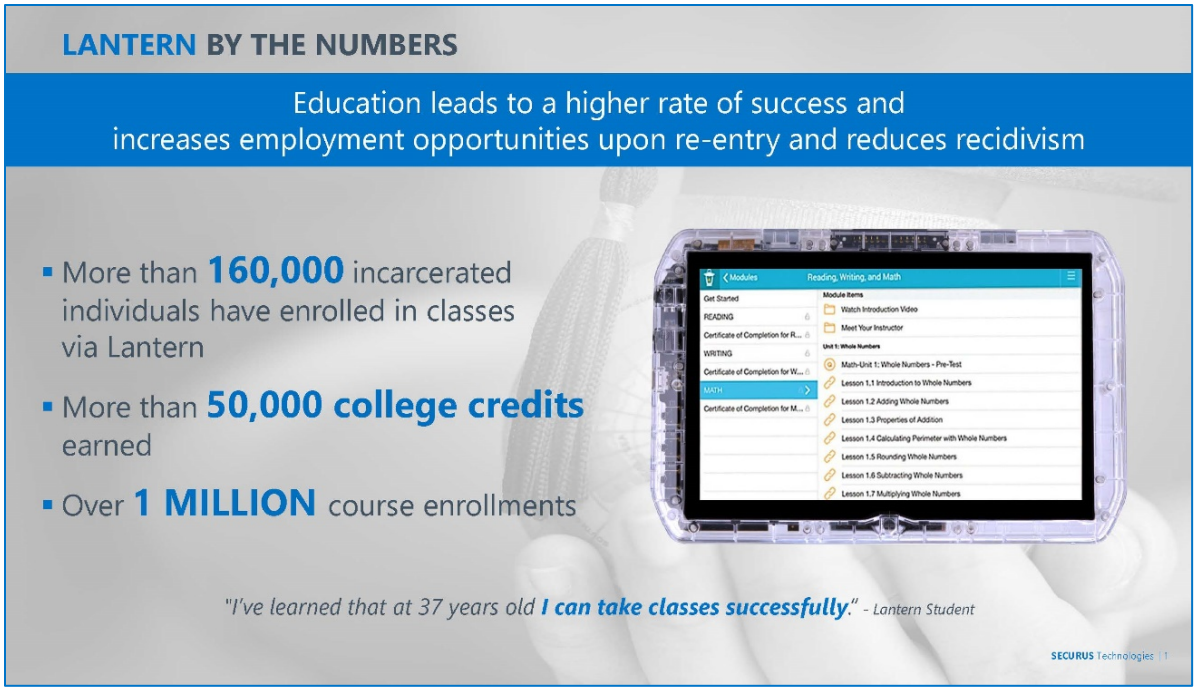
KA Lite via Securus has multilingual capabilities that support both English and Spanish. Some content is also available in French. **Closed captioning** is also available on a majority of the videos.

Unlimited Learning Opportunities with Lantern

Lantern is a Canvas-based Learning Management System (LMS). Canvas is used by multiple education agencies and schools throughout the nation, and Securus has modified this program to produce a **secure, corrections based LMS**.

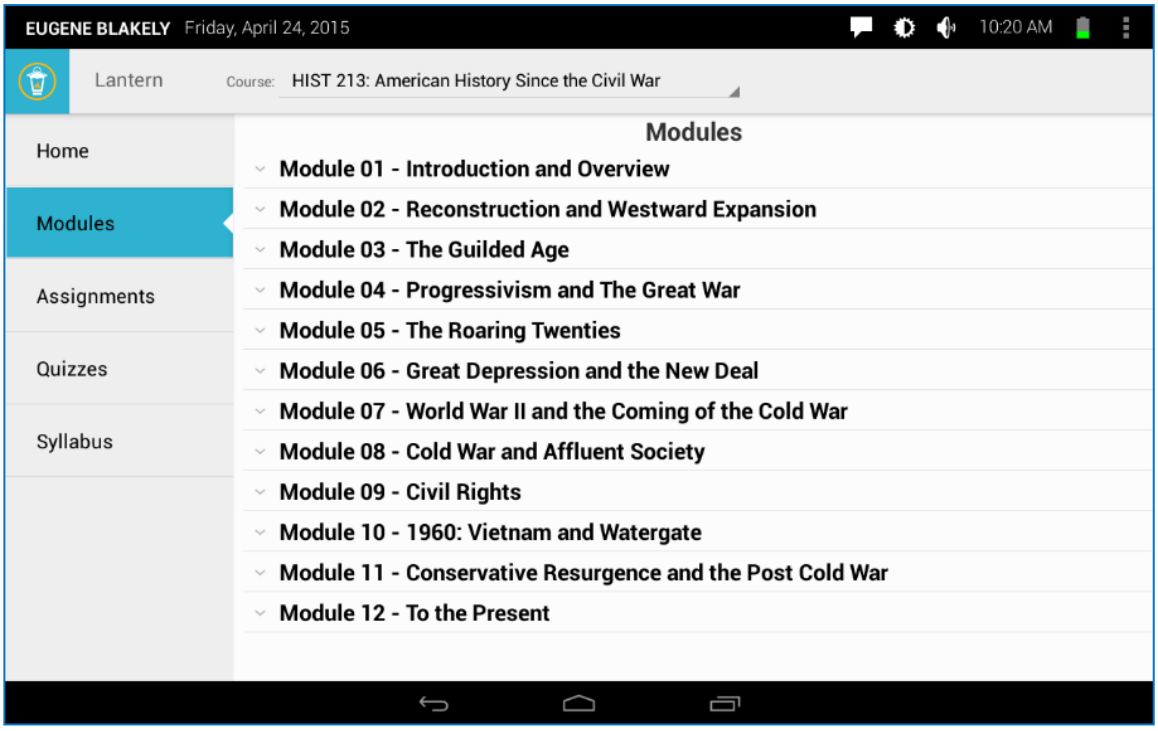
Securus' Lantern platform leverages secure tablet-based content delivery to increase the availability, scale, and variety of existing educational programs. Our open infrastructure platform is suited to building an education initiative from the ground up with courseware and educational partnerships. The education platform is a **free service** available on Securus' correctional tablets.

Lantern can be used to host facility-approved content, which is downloaded and consumed by offenders on their prison-grade Unity tablets.



Modules

Courses are split into multiple sections called modules, with each module consisting of approximately one week of coursework. Each module's course content is available on the tablet.



This may include, but not limited to, PDF files and ePub reading assignments, video lectures or voice-over PowerPoint presentations, and other downloaded content such as diagrams and audio files.

Within each module, students will also have assignments and quizzes to complete. The Unity Tablet also includes a customized, secure Mobisystems Office Suite product, so assignments can be completed using Word, Excel, or PowerPoint available directly from the Securus Lantern application.

Each course will also include a home page that displays the course objectives and overview for the student, along with a syllabus outlining the material to be covered and the due dates for each item.

All student coursework is completed and saved directly on the tablet. When a student syncs their tablet, all submitted coursework is uploaded to the Securus' LMS website for teachers/staff to access, grade and provide feedback. Once assignments are graded on the Securus' LMS website and the student again syncs with the kiosk, the students will receive all new grades and communications from their teachers. This allows module completion and coursework to be tracked on both the tablet and the Securus' LMS website.

Lantern hosts facility-approved content that offenders can access on their Unity tablets. Offenders have a real chance of equipping themselves with the education needed for success upon release.

Lantern is an adaptable system that allows instructors to upload coursework and correspond with students through a messaging option.

Functional Overview

- Screen elements are read aloud based on user touch on the tablet screen
- Screen reader reads aloud the navigational elements of the application as well as web view contents such as Assignments and Quiz Questions

College Credits through Ashland University

If your agency chooses to participate in offering college courses, Securus partners with Ashland University, an accredited university that offers free college courses to offenders using second chance Pell Grants. Securus and Ashland provide a turnkey solution, so no extra staff time is needed to support this education option.

Benefits of the Ashland University program include:

- Students enrolled in Ashland University courses access their courses from an Ashland University app on the tablet.
- The app launches a browser that only accesses corrections-grade Blackboard LMS site, or, alternatively, CDOC can choose our exclusive Lantern learning system.
- Students also use Mobisystems Office Suite, which includes Word, Excel, and PowerPoint, to create assignment files. This special office suite was customized for Securus to meet the security needs of our customers.
- All of this is exclusive to Securus' Ashland University partnership.

CourseShare



CourseShare offers a **no-cost solution** for agencies to **share educational curriculum** that can help offenders in any facility. Educational courses are proven to decrease recidivism by 40%; however, four out of five individuals in custody do not have regular access to educational content.

With CourseShare, agencies can give and receive custom courses created from respected agency peers across the U.S. through **Lantern, a Learning Management System that hosts facility-approved content.** Agencies can offer meaningful **rehabilitative programs** by leveraging educational content created from other agencies, saving time, money, and resources to create new course content. Offenders can access and download content directly to their tablets to begin their **path to successfully re-enter society.**

How CourseShare Works

STEP 1	STEP 2	STEP 3	STEP 4
Approval to share courses are granted. Appropriate content for sharing: • Basic Education • Life Skills • GED Prep, Post-Secondary/College • Substance Abuse • Vocational	A team of content specialists review the approved courses for appropriateness and external links. External links are removed if found.	Course content is imported to the new agency through Lantern.	Agency assigns new coursework to the students.



Google
Applied Digital Skills

CourseShare is now offering teachers and students access to **Google for Education - Applied Digital Skills.** The platform is a free, flexible video-based curriculum accessed by learners. The project-based units help students practice basic digital skills. With hundreds of hours of free lessons and instructional videos for 7th – 12th grade learners, lessons will equip them with the skills to be successful.

Mental Health Services



Mental Health services offered on Securus' tablets can help offenders combat depression, alleviate negative moods, reduce anxiety, and more to improve lives during, and following incarceration.

Securus Unity provides offenders with resources and programming that can meet a variety of needs.

Resources include:

- Anxiety Relief,
- Depression Assistance
- Relationship Guidance
- Guided Meditation
- Breathing Exercises
- Self-Reflection



In addition to Mental Health, **Addiction Recovery resources** are also available to aid their road to recovery and sobriety. These include:

- Alcoholics Anonymous
- Opiate Addiction
- 12 Step Programs
- Healing
- Thriving After Addiction
- Recovery Tips

Securus continues to expand the availability of Mental Health resources available through Securus Unity. Access to these critical Mental Health and Addiction Recovery resources are available to offenders **at no cost.**

Documents Viewer Application

Securus Unity allows the agency to make their own documents, as well as audio and video, accessible by offenders through the tablet. **The Department can easily add their own content to be available for offenders to access at any time for no cost.**

CDOC can add content through the Department's Document Manager or by providing content to a dedicated service technician to have added to the Viewer application.

Documents can also be set to require offenders to accept/indicate they have been viewed before gaining access to the device. This is ideal for agencies that wish to have offenders accept site specific rules, polices, terms or handbook before being able to use a tablet.



Reporting is available that tracks when these documents were accepted by each offender.

Video Applications



Offenders can access videos (in addition to Documents and Audio) at no cost directly on their device. The Agency can add videos directly to the tablets through the Agency Document Manager to be accessed through the FYI app or Securus can add this content on their behalf to the Viewer app.

Agencies today have used this functionality to add videos that provide information on PREA, video handbooks, educational and religious resources, health information and much more. This application is particularly important for offenders who cannot read.

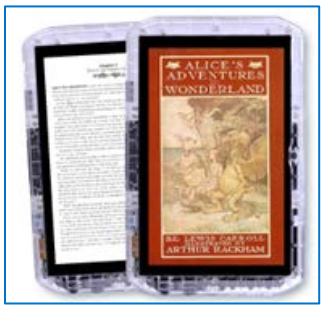
Music

Securus provides access to millions of songs, across every genre imaginable, through a constantly growing library. Offenders can easily browse the catalog, which is updated daily, preview songs, and make purchases, all over the Securus private network or downloaded when physically connected to a docking station or kiosk.

All Music and album covers are filtered in real time for questionable content.

FM Receiver Option: In addition to the above premium music offering, the Unity program allows offenders to utilize their Unity Tablet as an FM Receiver for local radio stations as well as access to the local corrections broadcasted audio. For agencies that broadcast television audio through an FM signal, this allows offenders to use their tablets to listen to the television which reduces noise and disruption in the common areas.

Books



Offenders have access to a catalog of **50,000+ free eBooks** available through the eBook Reader application that has been optimized for corrections. By allowing access to eBooks through a Securus Unity Tablet, offenders can access multiple books at the same time.

This large and expanding catalog is available to offenders at no cost allowing them to access their favorite titles, religious holy books, and more. Additionally, Securus also maintains a collection of free audiobooks that can be accessed by any offender at no cost.

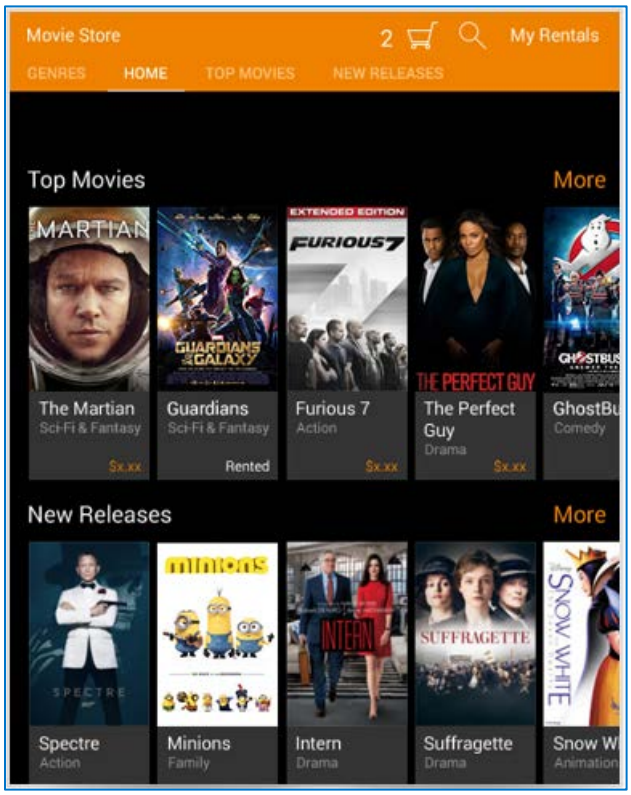
This application has several settings that can **help the visually impaired** such as **text-to-speech**, changing font size and various themes and backgrounds.

Games

Each Unity tablet also comes standard with **50 free unlimited usage Games**. In the Securus Media Store, offenders may purchase more than 850 games spanning popular genres, including education, puzzle, adventure, sports, strategy, and many more.



Movies and TV Shows



The Securus Media Store offers the largest catalog, featuring thousands of blockbuster Hollywood movies and hit TV shows available to rent. Every movie and TV episode has been reviewed to ensure it is appropriate for corrections. In addition, Securus will comply with the determination of the approved/unapproved list generated by the CDOC Review Committee.

Securus Unity Movies and TV Shows

Securus Unity provides access to the most extensive movie catalog available in corrections today, Offenders can use their tablet to access a catalog of several hundred movies that is constantly updated with recent releases and popular titles. Movies and TV Shows are available with a 30-day activation window and for 48 hours of unlimited viewing upon activation.

Upon rental, movies can be streamed and viewed instantly without needing to sync or download. Streaming avoids the need to have significant storage space available on the device. In doing this, the offender can have several movies available to watch from their device at any time without having to manage device storage or remove other content.

In addition to providing a first-class movie catalog, Securus also ensures that all movies meet the needs of the corrections environment. Securus utilizes a dedicated team of Content Review Specialists, in addition to automated filtering tools and resources, to perform a comprehensive review and evaluate content for appropriateness before it is available to the incarcerated population.

Reentry Assistance

CDOC can also have their own reentry content added to tablets through the FYI or Viewer apps to be accessible by offenders at any time.

Securus provides a large assortment of content that can be used directly by offenders to proactively prepare for reentry. Content is delivered in multiple formats (text, audio, and video) to meet the preferences of offenders.

Offenders can prepare for release by searching for employment in the Securus exclusive **Jobview** application. This easy-to-use application allows users to search for employment opportunities in the area where they will be living post incarceration.

Securus can exclusively provide content on tablets such as the **Academy of Hope** or **TYRO** that focus on success during and after incarceration. These programs cover important topics such as building support networks, interacting with family, communication, the change in technology and more.



Religious Applications

The Securus Unity Platform provides offenders with more access to their unique religious and spiritual beliefs than ever before. Securus provides access to religious content at **no cost,** allowing for the most access to **faith-based resources**.

Through Securus Unity, offenders can access their unique religious beliefs such as:

- Christianity
- Judaism
- Islam
- Hinduism
- Buddhism
- Asatru
- Baha'i
- Jehovah's Witnesses
- Latter Day Saints (LDS)
- Moorish Science Temple (MST)
- Rastafari
- Sikhism
- Wiccan
- And other spirituality

Spiritual and Self-Help Applications

As highlighted above, the Securus Unity Platform provides offenders with more access to their unique religious and spiritual beliefs than ever before. Securus provides access to religious content at no cost, allowing increased access to faith-based resources.

Securus Unity is the **only tablet platform in corrections that allows offenders to access the God Behind Bars application, Pando.** The application is available on every tablet and accessible by every offender at no cost.

Pando – God Behind Bars

Pando is a revolutionary new application from God Behind Bars that makes it possible for offenders to engage with their spirituality and improve their mental health in a whole new way. The Pando app delivers some of the best faith-based messages and other leadership content directly into the hands of the incarcerated population utilizing Securus Tablets.

God Behind Bars and **Securus** partnered to have the **Pando application** designed specifically for use in the correctional environment allowing us to deliver high quality content, while maintaining necessary security.

Offenders can identify their current spiritual and mental health needs for the application to recommend relevant messages, sermons, and other content automatically. The Pando application provides offenders with an additional avenue to engage with their spirituality and improve their mental health through high-quality, uplifting content.

What Does Pando Provide?

Pando provides 24-hour access to some of the best faith-based and leadership content in the world. God Behind Bars created the application for offenders to still be able to

stay connected with their faith while improving their lives. Through the content itself, offenders can learn, grow, and experience real life change.

The **Pando application** provides an enriching and engaging experience that allows offenders to receive critical spiritual growth, mental health, and self-betterment content.

This application features content in the form of sermons, leadership videos, bibles, and other self-help materials, as well as the ability to submit prayer requests.

High-Quality Streaming Videos



Utilizing Securus Tablets and private network, Pando delivers a “Netflix-like” experience for streaming faith-based content in corrections. Offenders can scroll & swipe through series of content based on their identified needs and interests.

Videos Include Topics Such As:

- Sermons
- Leadership Videos
- Topical Studies
- Prayer and Meditation
- Self-Help and Self-Betterment Material

Access to the Bible

The Pando app has multiple versions of the bible available within the application with additional tools that make navigation easy.

Prayer Wall

A unique feature of the Pando application is that it provides the ability for offenders to submit prayer requests or share wins with others. Users of the application are able to indicate that they are praying for the individual who submitted the prayer.

Pando utilizes a prayer auto-generation feature that creates the prayer on behalf of the offender so they cannot pass messages or input inappropriate text. All names on prayers are “Anonymous” as well.

Track Goals and Progress

“On September 22nd, 2013 we launched our first church service in a prison in Colorado. Today, we now have the honor to serve the least of these in four different prisons in the state of Colorado including Sterling Correctional Facility, Colorado Territorial Correctional Facility, Limon Correctional Facility, and Denver Women's Correctional Facility.

What does God Behind Bars Provide?
God Behind Bars takes a three phase approach that helps inmates get to know Jesus, grow deeper with Him, and live out walking with Him. We get them connected to the church through a weekly experience. The weekly experience is a high quality worship environment where they can hear some uplifting music backed by an encouraging message. We then encourage them to have their family watch the same service through our Pando app, so they can connect with their loved ones. In our second phase we help them grow deeper in their faith by gathering in small groups. They learn about overcoming their hurts, habits, and hang ups. In our third phase they live out their faith by learning what it means to serve others, and gain knowledge on leading a life centered around Jesus. Our hope for those reentering society is that GBB is a season of their life, and the Church is the rest of their lives.

Since 2013, we have seen some overwhelming success with our program in the state of Colorado. We have seen 64,000 inmates attend a GBB service. Over 5,500 inmates have made Jesus the leader of their lives, and 414 chose to get water baptized. We love our volunteers, and have gratefully seen over 3,100 volunteers serve inside of prisons in Colorado. Through the family reunification events we have seen (getting this number) families reconciled.

God has moved in the state of Colorado and continues to do so. Covid has brought some challenging times, but through that adversity a God idea was birthed and that idea is the Pando app. Let me introduce you to the greatest resource that has ever been given to inmates behind bars”.

The Pando application allows offenders to track their progress in the app based on goals set by God Behind Bars. Offenders can work towards earning bronze to platinum

status by completing goals that include praying for others, submitting prayers, and watching videos.

Self-Help

Using their Securus Unity Tablet and content that can be accessed at any time, offenders can improve their lives during and after incarceration. This includes education tools and content that provides inspiration, motivation and more that is available at no cost.

- Mental Health &Wellness
- Setting Goals & Productivity
- Inspiration &Motivation
- Meditation
- Overcoming Conflict
- Addiction Recovery & Sobriety
- Self-Paced Education
- Personal Development
- Securus continues to expand its catalog of Self-Help content and other content that can **enrich** the lives of the offenders utilizing the Securus Unity Tablets.

E. Ensure that all audio files offered to offenders are the industry-sanitized versions and appropriate for a correctional setting.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus Media Store and Music App offers a large selection of corrections appropriate, industry sanitized music with over 35 million tracks. The music catalog is updated daily and includes several genres such as Folk, Jazz, Blues, Rock, Alternative, Electronic, Dance, Music from Soundtracks, Classical, R&B, Hip Hop, Gospel, Soul, World, Latin Country and Reggae.

F. Ensure that e-books offered as a subscription and movies are in accordance with the Department's regulations regarding publications, to include the Publication Disapproved List (not all inclusive).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The eBooks application offers users unlimited real time access to 50,000+ unique preapproved books spread out multiple genres, available to read and download. Available genres include fiction, non-fiction, adventure, holy books and more. Via the

eBook Reader, offenders have the ability to download and read books with options to bookmark, zoom in and out, and utilize a table of contents.

Securus will work with CDOC personnel to ensure all e-books provided are in accordance with the Department's regulations regarding publications, to include the Publication Disapproved List (not all inclusive).

In addition to providing a first-class movie catalog, Securus also ensures that all movies meet the needs of the corrections environment. Securus utilizes a dedicated team of Content Review Specialists, in addition to automated filtering tools and resources, to perform a comprehensive review and evaluate content for appropriateness before it is available to the incarcerated population.

G. Provide tablets with a warranty for the duration of the contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As part of our proposed, Securus will replace non-functioning tablets at no additional cost to the CDOC and/or the offender. Securus proposes to provide a tablet to every eligible offender at no cost. Eligibility is determined by the CDOC and provided under the Securus and CDOC tablet deployment program.

Command and Control tablets will also be provided at no cost to all eligible CDOC staff. Further, the Securus proposal includes a comprehensive tablet logistics program where Securus will be responsible for the distribution of the tablets, the management of the tablets and the tablet inventory as well as training for offenders and staff In the rare instance where a pattern of abuse or misuse is identified by Securus and can be confirmed by the CDOC, Securus may request the assistance of CDOC to help identify financial options for replacement costs of tablets or network components caused by an offender(s).

H. Provide all tablet accessories and peripherals.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will supply all tablet accessories and peripherals as agreed to in the contract.

Accessory Name:

- Gummy Earbuds
- Over the Ear Headphone
- JP6s 7" Power Adapter
- Keyboard
- JP6s 7" Screen Protector
- JP6s 7" Tablet Case

- Gummy Earbuds with Microphone

I. Additional tablet earbuds and headphones will be approved and offered through CDOC Canteen

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with CDOC to sell earbuds to offenders. If requested, Securus can reach out to your current commissary vendor and future commissary vendors to provide initial and replacement headphones for purchase. Securus has vast experience working with hundreds of vendors to integrate services on behalf of CDOC needs.

The headphones we provide are unique and custom built to work with our phone application on the tablets. Only these custom, certified earbuds can be used with our Unity tablet, ensuring high-quality speakers and microphone. These are also the only earbuds certified to work with Investigator Pro™, the most accurate continuous voice identification software in corrections.

Earbuds provided by Securus have been customized for correctional use and meet the following specifications:

- Plug pull force: 10 kg
- Ear piece pull force: 4kg-5 kg
- Clear (no color) gummy earpieces
- Clear audio cables, with microphone
- Certified to work with Investigator Pro—these are the *only* earbuds in the industry certified as such

J. Provide tablet charging cabinet solutions to meet the safety and security needs of correctional facilities. Tablets will be charged in a common area within each unit. Individual chargers will not be provided to offenders.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Unity Tablets have high-capacity, rechargeable lithium-ion batteries. **The tablet can hold charge for over 20 hours of constant use or 350 hours of standby time. More specifically,** the tablet battery can remain charged at the following rates:

- 22hrs standby time with LCD on and 350hrs with LCD off
- 20 hours with LCD on and 140hrs with LCD off with music playback
- 13-14 hours video playback

Battery and Safety Precautions

Securus' tablet batteries have a nominal capacity of 8000mAh/29.6Wh (500 cycles). The battery includes the following safety precautions:

- **Charge termination** – The tablet is programmed to stop charging after it reaches 100% battery charge (even when left plugged in).
- **Temperature sensor** – The tablet includes an internal sensor that detects excessive heat or cold and will shut down the tablet to prevent damage caused by extreme conditions.
- **Battery App** – The tablet is equipped with a core application that monitors the cycles and usage of the battery. This assists in running diagnostics and providing relevant information when troubleshooting the offender's tablet device. Further, the offender can also look in the "Settings" application to view the status of the battery

Tablet Charging

Securus can provided both wireless and wired charging, based on the needs of the facility.

Wireless Charging

Wireless Charging is delivered through modular charging stations that are on a roll-around cart (charges up to 60 Tablets) or vertically wall-mounted (charges up to 40 Tablets per AC outlet). Both are great options—one offers mobile flexibility, and the other is a great space-saver—and there are no cords. Charging stations may be configured with an optional locking mechanism that secures Tablets during hours when Tablet use may be prohibited at your facility. **Securus wireless charging is FAST typically charging Tablets in under 5 hours. We use Pogo Pin Technology** instead of inductive charging—this technology advancement means your population and team aren't waiting. Many facilities transitioned to wireless charging as it is an efficient use of space, eliminates cables, and there's no need for access to outlets.



Benefits of wireless charging include:

- **Efficient Use of Space**: Vertical design allows multiple charging stations to be wall-mounted without taking up valuable space
- **Wireless**: Completely wireless with no need to plug in tablets
- **Modular**: Design allows for up to 60 tablets to be charged from each cart and up to 40 tablets per AC outlet when mounted on a wall
- **Flexible**: These modular wireless charging stations can be configured with an optional locking mechanism, allowing you to secure tablets during hours when tablet use is prohibited.
- **Easy Administration**: LED on tablets illuminates, indicating charging status

Wired Charging

Securus offers two wired charging options, Community Wired Charging Stations and Personal Chargers, that can be used in conjunction with Securus' wireless charging to create customized solutions that meet the unique needs of every agency we serve.

Community Wired Charging Stations use barrel cables and may be configured as 16, 40, or 80-count wall-mounted stations or as rolling cart. This provides a secure charging solution without the risk of illicit content being transferred to the tablets through other non-secure charging ports, such as USB/mini USB ports, found on competing tablets.

- 16 Count – Wall Mounted
  - AC 110V-125V
- 40 Count – Wall Mounted & Floor Standing Cart Option
  - AC 110V-125V
- 80 Count – Floor Standing Cart Option
  - AC 110V-125V







Personal Wired Charging is a forward-thinking choice that maximizes the time your population may use their Securus Unity Tablets and minimizes the work for facility staff. The available personal chargers are barrel cables and only work on Securus Unity Tablets, so there is no risk of use with contraband street devices. A WiFi connection is not required for Personal Wired Charging. This option allows your population to keep their tablets with them overnight to expand opportunities for entertainment, relaxation, and communication.

K. Provide technology to allow tablet configurations based on the CDOC policies and procedures.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

L. Offer music downloads and/or streaming music available for a monthly fee. The CDOC will decide whether to implement the music download model or the streaming music model, or both.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

From the Media Store app on the Unity Tablet, offenders have access to over 35 million songs from several genres. Offenders can search for their favorite artists, songs and albums, discover the latest music. Thirty (30) second previews are available so incarcerated individuals can listen to a sample of the audio, before they buy it.

Securus can offer both an ala carte purchase model and subscription-based music structure.

Music App

The Music application allows offenders to listen to the music that they have purchased and downloaded from the Securus Media Store. Users can download their favorite tunes to their tablet and create a customizable playlist for more enjoyable listening.

Music Subscriptions

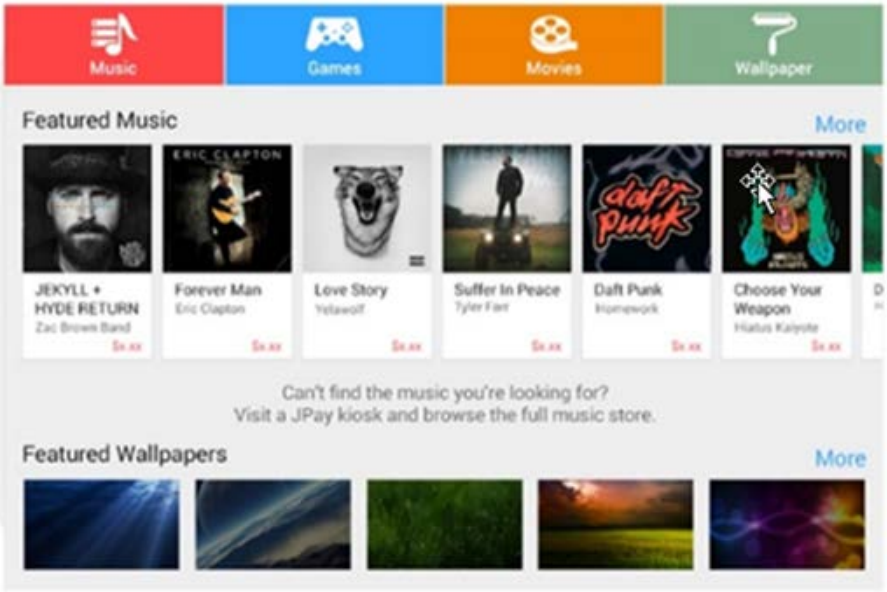
With Securus' music subscription service, offenders have access to millions of tracks through a tiered subscription model for a recurring monthly cost. Several subscription package options are available to meet a variety of consumer preferences and budgets.

We have partnered with one of the largest music distributors in the world to bring offenders music subscription access to an evolving selection of titles – new music is added catalog daily!

And unlike other competitor providers who use automated algorithms to provide 'customized' content, our music is expertly, and personally curated based on data derived directly from the facility. Our playlists and suggested artists are population-specific, created by our music professionals.

Best of all, there is no additional administrative hassle for the agency. All subscription packages are purchased and managed independently by the offender through the Personal+ tablet media store. And in efforts to expand access to music to as many incarcerated listeners as possible, we periodically run sales and promotions making subscriptions an attainable option for your incarcerated population.

A-la-carte music will continue to be available through the media store for offenders who are not interested in a subscription package option.



M. Offeror will provide technology to restrict offender to offender communication. Tablet initiated phone calls are to be governed by the approved CDOC offender phone list.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Offender accounts are subject to calling restrictions CDOC personnel will put in place in accordance with CDOC policies.

Programmable Call Restrictions

As offender phones are a shared resource, facilities often need to enforce the equitable sharing of them. While Securus will install additional phones as needed, sometimes space and logistics preclude this option. In that case, CDOC may use call restrictions to regulate offender access to ensure access by all offenders.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides calling restrictions to give CDOC control of calling activity at the offender, port, phone group, facility, or customer level. Multiple restrictions can be crafted within each restriction set.

Examples of call restrictions are:

- Maximum number of calls per day/week/month
- Maximum type of calls per day/week/month
- Maximum number of call connects, accepts and/or mins of talk time

All imposed calling restrictions are automatically managed by the NextGen SCP system to relieve facility staff of calling restriction enforcement responsibilities.

Restrictions may also be used for punitive measures or behavior modification by restricting access versus revoking complete access as done through suspension.

Offender Calling Restriction Profiles

CDOC can set up Offender Calling Restriction Profiles to limit the number and length of calls an offender can make by day, week, or month. These "velocity" Restrictions are applied to an offender's Custody Account. The limitations can be set for a specific call type such as Collect calls, Free calls, or Crime Tip calls; or for all call types depending on CDOC needs. Authorized officers at CDOC can create as many calling restrictions as necessary to meet the facility requirements, then select the profile that best fits each offender.

How it Works

When offenders enter their PIN, the system checks their daily, weekly, and monthly calling restrictions before connecting the call. If an offender has exceeded any of the limits, the call is blocked. During an accepted call, the system ensures the time limit is not exceeded for the restricted time frame.

Calling Restrictions can be setup in multiple ways:

- **By Facility –** The entire agency follows the same set of restrictions.
- **By Site –** Each site within a facility has its own set of restrictions.
- **By Phone Group –** A group of phones that use a particular calling limit that is different from another phone group in a facility.
- **By Offender –** An offender's custody account is setup with a specific calling limit.
- **By Call Type Exclusions –** Certain call types can be excluded from a calling restriction (i.e. Crime Tip, PREA or Private calls).

N. Tablets will offer video visitation technology (Refer to section xix).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

To continue our mission to evolve the incarceration experience, Securus is proud to introduce the new Unity Terminal SE. This powerful, corrections-grade terminal is built on Securus' industry-leading platform and delivers advanced technology and software solutions for our facilities and their incarcerated populations.

The Securus Unity Terminal SE supports all current and future Unity tablet features and applications and was designed with upgraded video technology to provide top-quality video services. The Unity Terminal SE is ideal in situations where:

- Facilities want to provide access to communication methods that require a camera, like Video Relay Service (VRS), Securus Video Connect (SVC), and outbound Videograms, and do not have cameras available on their tablets.
- An incarcerated individual may not be eligible for or does not want, a Personal or Personal+ Tablet.
- In the rare event of a Wi-Fi outage rendering tablets unavailable, the terminal can serve as a reliable backup with all applications accessible on the terminal.
- If a tablet were to malfunction, the terminal can serve as a backup, allowing offenders to submit support tickets to Securus and to continue communicating with their family and friends until their tablet is fixed.

Hardware features

- **Corrections-grade security** with industrial-strength hardware.
- **Upgraded video technology** with an embedded video camera, a 12” color screen display, and enhanced lighting capabilities.
- **Multiple hardware options** including a full handset, available headphone jack.
- **Space-saving, wall-mounted terminal** with an adjustable ‘sliding’ height option and tilted screen for easy typing and video recording.
- **Low Power PoE connection** with a built-in battery. The PoE provides continuous charge power, while the battery supplements that power for screen, camera, and lighting.

Software Features

- **Supports current and future Unity apps and functions** including VRS, SVC, outbound Videograms, and mirrors the same, familiar log-in process as the Unity Tablet.
- **Landscape mode** is available for all applications to provide a better app viewing experience.
- **Customizable permissions** allow facilities to limit specific applications or disable the entire terminal.

- **Manage scheduled video visitations** with the Conflict Management feature to facilitate transitioning offenders off a terminal before a scheduled video visitation is to start. Controls are configurable based on facility preference.

As the leading provider of corrections terminals, we're always working towards providing our clients and their populations with easy-to-access and easy-to-maintain technology solutions. With our solutions, onsite Securus administrators can easily replace terminals while continuing to maintain security standards. Plus, with around-the-clock securing monitoring supported by Securus staff for all facility devices, you can be confident that your Securus solutions are safe, reliable, and protected.



Unity Tablet Hardware

Securus offers the following tablet hardware specifications.

Inmate Tablet JP6S

The Securus JP6S tablet hardware incorporates the following features and specifications.

Features:

- Ruggedized Casing
- High strength, impact-resistant security glass w/ integrated screen protector
- Barrel charge port
- Pogo pin connector
- Secure WiFi
- Built-in FM Radio Receiver

Specifications:

- Internal Storage: 32 GB
- CPU: MT8163 - Quad core cortex A53
  Frequency 1.3G, 64bit CPU
- Resolution: 1280 x 800
- Dimensions: (L x W x H) 7.8” x 5” x 0.61”
- Weight: 17.2 Oz
- Battery: Lithium - 500 cycles, includes temperature sensor
- Dual WiFi Bands (2.4GHz and 5GHz)

Environmental Conditions:

- Operating Temperature Range: 50o F to 110o F (10o C to 43o C)
- Storage Temperature Range: -40o F to 150o F (-40o C to 65o C)
- Humidity: 95% RH (relative humidity), non-condensing

The following figure identifies the available ports and physical buttons.

JP6S Ports and Physical Buttons



The following table lists the complete JP6S specifications.

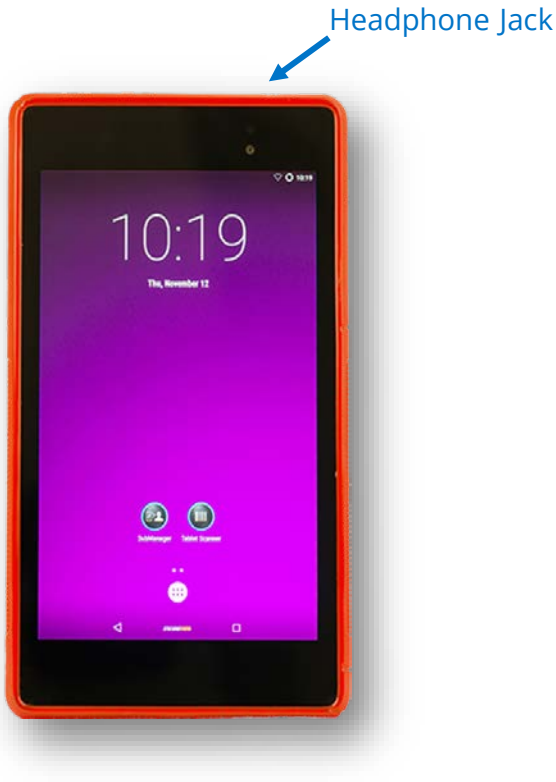
Item	JP6S
OS	Android 8.1
CPU	MT8163 - Quad core cortex A53, Frequency 1.3G, 64bit CPU
GPU (Graphics Processing Unit)	Mali-T720 MP2 GPU
DDR	2G - 512*4
Battery	8000mAh
LCD	Resolution: 800*1280
Boot On - mA during boot on	500-750 mA (LCD on)
Stand by: Stand by current on main window	300-400 mA (LCD on)
Music: Listen to music w/ ear bud plug in	380-400 mA (LCD on)
Movie: Play movie w/ ear bud plugged in	450-550 mA (LCD on)
FM: Listen to FM w/ ear bud plugged in	300-400 mA (LCD on)

Item	JP6S
Back Light	380 mA
USB (OTG)	400 mA
Stand by time	About 22hrs with LCD on About 350hrs with LCD off
Play MP3	About 20hrs with LCD on About 140hrs with LCD off
Play Video	About 13-14hrs
Storage	32GB
Buttons	Power, volume up, volume down
5G	Dual support for 2.4G and 5G
Camera	2 Mega Pixel
POGO PIN	Yes – charging and mounting

Officer Tablet Nexus 7

The Nexus 7 offers the following features:

- Red protective rubber skin casing
- Corning, scratch-resistant screen
- Micro USB port for charging—it cannot be used to transfer information
- Enabled camera for inmate tablet activation
- Secure WiFi



The Nexus 7 has the following specifications:

- 8 GB internal storage, 1 GB RAM
- Quad Core 1.2 GHz Cortex-A9
- Resolution: 800 x 1200
- Dimensions: 7.81 x 4.72 x 0.41 inches
- Weight: 11.99 ounces
- 7-inch LED-backlit touchscreen
- Lithium battery up to 14-hour charge, depending on use
- 4-7-hour charge time

Officer Tablet Specifications

Specification	Command & Control Officer Tablet
Screen Size	7 inches
Storage	8 GB
Memory	1 GB RAM
Resolution	800 x 1280

Buttons	Power, volume up, volume down
Accessories	Case, gummy ear buds
Battery	Lithium
Dimensions	7.81 x 4.72 x 0.41 inches
Weight	11.99 ounces
Secure WiFi	Yes
Speaker	Yes
Camera	Disabled

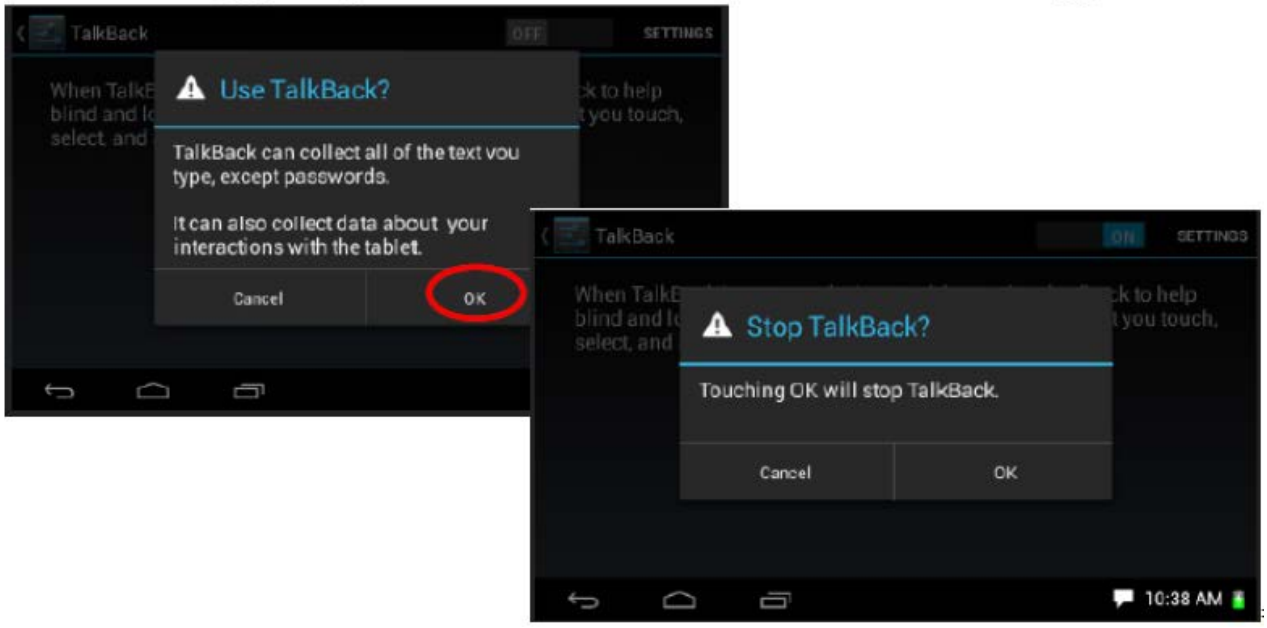
O. Provide tablets in multiple form factors and adaptive for the sensorial disabled, the wireless tablet will offer a solution that integrates with the offender phone system and other Offerors services such as mail, library, law library, commissary, grievances, documentation, education programs, vocational training, cognitive behavioral therapy, and entertainment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Offenders can use the Text-to-Talk (Talkback) feature on their Unity tablet for the secure eMessaging and Music applications. The first time the Talkback feature is enabled on the offender's tablet, a tutorial will be available to walk the user through using this function.

The Talkback functionality can be enabled or disabled at any time by clicking on the "Settings" at the top right-hand corner of the screen, selecting "Accessibility," and toggling it on/off. When toggling the Talkback feature on or off, a confirmation message will confirm the user's choice, as shown in the following image.

Toggling the Talkback Feature On/Off



15. WIRELESS TABLETS TECHNICAL ENVIRONMENT

A. The Offeror will provide its application(s) that will run on an operating system, mutually agreed upon by the Offeror and the CDOC and is capable of being upgraded at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will furnish all applications that will run on our operating system, hardware, software, interfaces, cabling, switching equipment, internet connection, labor, and licenses to set up and operate the Securus Unity Tablet services. The Unity Tablet program currently uses the publicly available Android 8.1 operating system.

Securus will also repair, replace, and update equipment and software during the contract to maintain efficient operation of all systems at no cost to the CDOC.

B. Offeror is expected to ensure that the operating system is no more than (N+2) revisions behind the publicly available kernel.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. At a minimum, the Offeror is expected to provide the following technical support services for all hardware equipment and software for services provided including, but not limited to:

i. Updates and upgrades:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus designed the Unity Tablet Program to be hassle-free with over-the-air updates. Software updates are automatic and on-going to ensure that the offender maintains access to the latest applications and content.



a. Security-related updates to their proposed solution, which may be called updates, upgrades, patches, service packs, hot fixes, and/or workarounds.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Software upgrades are pushed to the tablets whenever an update is available in order to ensure the stability, security, and functionality of the platform. Software updates are automatic and on-going in order to ensure that the offender maintains access to the latest and greatest content that Securus can provide.

b. All upgrades, bug fixes, enhancements to the software and/or hardware will receive prior approval by the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

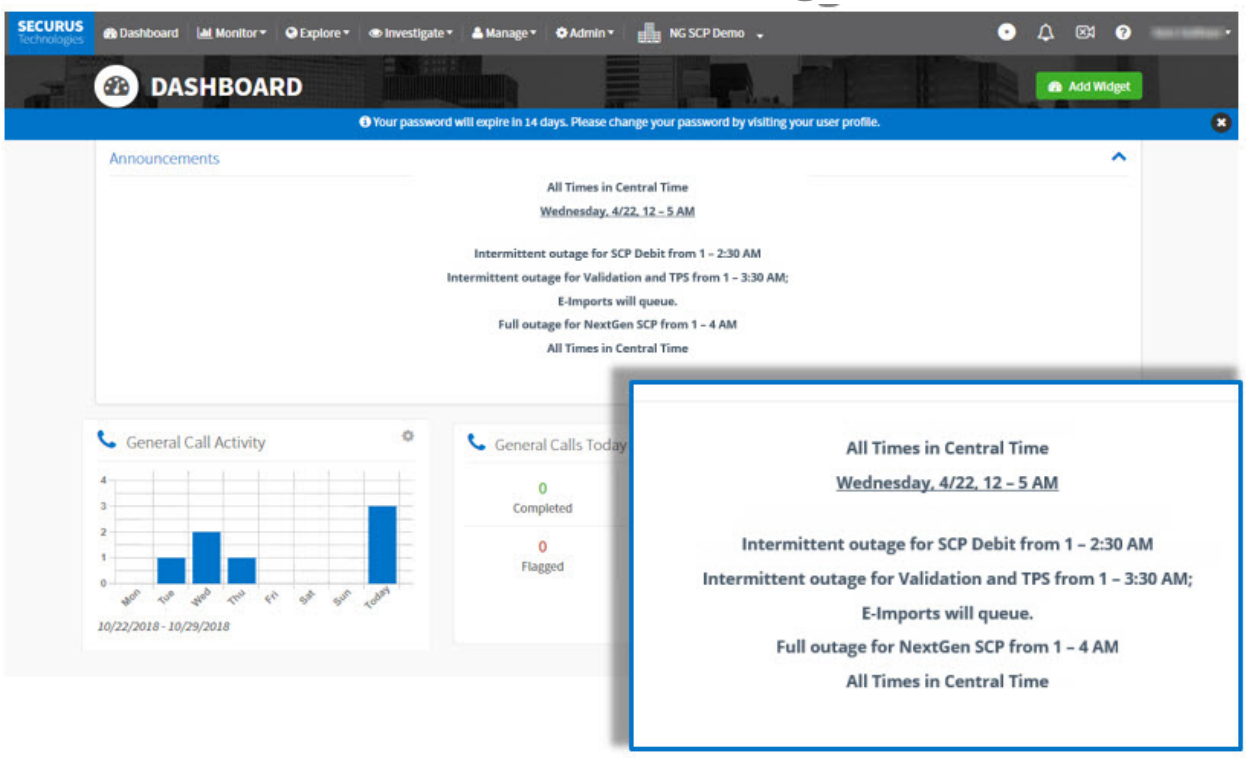
Securus provides regular updates with notifications to the CDOC prior to their applications. Securus will work with CDOC personnel to ensure CDOC software upgrade policies are followed.

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCP™ software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be

notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



c. The Offeror will provide a test environment to allow authorized CDOC staff to verify the upgrade, fix and/or enhancement is compatible with the current operating environment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Pilot sites

Securus uses customer sites as pilot sites to test-in and verify updates and upgrades in a customer environment to verify field adoption of the changes.

D. Offeror to describe how they will manage transferring any media including but not limited to streaming subscriptions and approved messages (i.e., text and photos) if new devices are introduced during the life of the contract and/or if a new Offeror is chosen upon contract termination.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

If an offender is approved for a new tablet, whether it is because a newer version of the tablet is available or because their tablet malfunctioned, the process to transfer content to the new tablet is the same. First, authorized agency staff or the Securus onsite tablet administrator must decommission the non-functioning or old tablet from the Command-and-Control Tablet. Next, from the same sub-manager application on the Command & Control tablet, they will authorize the replacement tablet. The offender will be given a new available Inventory Tablet, instructed to log into the tablet with their credentials to redeem the new tablet and reactivate their tablet subscription through the "Make Mine" process on the tablet. This tablet will now become their own Personal Tablet and their current subscription will continue. The offender will be able to access and download all their previously purchased content from the cloud.

From the Account Tab in the Media store, the offender can view and download all previously downloaded content. Any subscriptions the offender had in place would still be active. Any rentals would also be available as well. They can also download any books or podcasts he had previously downloaded through those respective applications.

Once purchased, premium content is accessible at any time from an authenticated user's Personal Tablet for no additional cost. Should a subscription end and then be restarted, the offender can access and download previous purchases. This ensures that anyone receiving a newly introduced tablet can download and access all their previously purchased.

TRANSFERRING CONTENT

Our proposed solution has offenders purchasing and renting media directly on their Unity tablets. If a new tablet is introduced during the life of the contract, all content is easily transferred. The offender will be given a new tablet, instructed to log into the tablet with their credentials to redeem the new tablet and reactivate their tablet subscription through the "Make Mine" process on the tablet. This tablet will now become their own Personal Tablet and their current subscription will continue. The offender will be able to access and download all their previously purchased content from the cloud.

From the Account Tab in the Media store, the offender can view and download all previously downloaded content. Any subscriptions the offender had in place would still be active. Any rentals would also be available as well. They can also download any

books or podcasts he had previously downloaded through those respective applications.

Transferring Content to a New Vendor

Securus' content and customer agreements prevent us from transferring licensed content to other vendor devices. In addition, while it may be "technically" possible for Securus to copy previously purchased content onto a portable media device and provide that media device to the CDOC, Securus does not have a process in place to facilitate this today, and we cannot comment on, or guarantee, the legality, feasibility, technical difficulty or potential development effort required to load any such content onto a competitor's device.

We will provide the information you are requesting if we are permitted by the record labels and/or aggregators and if they provide such metadata to us.

E. The Offeror will provide over-the-air updates to upgrade the OS (similar to how commercial Windows or smart phone provider's request to upgrade for security issues).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

F. System is expected to be deployed as a wireless network and shall not allow access to internet services outside of provider intranet.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Unity Tablet Program operates on a separate network from the CDOC secure network and will not connect or interfere with the CDOC infrastructure. Securus provides all required network connectivity on a separately installed secure network and does not require that CDOC provide any infrastructure. As a point of policy, Securus does not use client-provided network infrastructure. By providing our own network, we can monitor the network through our Network Operations Center (NOC) and provide quick resolution through our Technical Support Center (TSC) 24x7x365 without ever having to contact or coordinate with the State or client network providers. In addition, we provide and maintain all the on-site network connectivity equipment through our nationally disbursed certified technicians that carry all necessary replacement components.

G. Offeror is expected to provide a sufficient infrastructure to allow offenders to utilize all the available communication solutions at the same time.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The system and network maintain twice the capacity of normal calling volume to prevent blocking of outbound calls and busy signals. The central processing system and

its network capacity can scale to many times their current capacity within the current architecture and design.

Securus monitors the system 24x7x365. When concurrent telephone call volumes reach a predetermined threshold (not at the limit), additional capacity is added. Since the system capacity is managed to keep ahead of call growth, the maximum number of offender phones is limited only by the connectivity delivered to the facility.

Securus adds additional circuit bandwidth to each site and the central data center when necessary.

The on-site tablet servers and network equipment are scaled to provide sufficient capacity and network bandwidth to accommodate expected tablet usage for all tablets within the facility. The central data center is designed to scale beyond the current capacity based on the needs of our customers. When concurrent tablet traffic consistently cross 80% of the available capacity (either at the customer site or at the central data center, additional infrastructure is added to augment the capacity. Since the system capacity is managed to keep ahead of the usage of tablets as well as additional features and services on the tablet, the customer has the flexibility to increase the number of tablets and services enabled at a facility as needed.

H. The Offeror will provide a system that does not interfere with any wireless equipment (two-way radios, Wi-Fi equipment, etc.) already operating at a CDOC facility.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides all required network connectivity and does not require your facility to provide any network infrastructure. As a point of policy, Securus does not utilize client provided network infrastructure. By providing our own network, we can monitor the network through our Network Operations Center (NOC) and can provide quick network resolution through our Technical Support Center (TSC) 24x7x365 without ever having to contact or coordinate with our clients or client network providers. Our Unity tablet system and supporting equipment will not interfere with any wireless equipment already operating at any CDOC facility.

Site Engineering

Securus technicians and sales engineers will work with CDOC to consider all areas tablets will be used within the facility to determine where to install Wireless Access Points (WAPs). Upon award, we will coordinate site survey activities to assess the latest physical characteristics of each location to determine the optimal placement for our equipment.

All locations where the facility wants an offender tablet or Officer Tablet to work must have a WAP installed. Examples of locations of where to have WAPs installed include but are not limited to administrative areas and control rooms for Officer Tablet usage, and hallways and common areas to provide coverage for offender tablet usage. It is important to consider what locations may need WAPs in the future as well.

Day rooms, common areas and pods are ideal locations where to install WAPs because as they are generally large open areas there will be good Wi-Fi signal coverage.

In general, Securus mounts Wireless Access Points (WAPs) no less than 25 ft. together and no more than 325 ft. apart (depending on the environment) but will utilize a Wi-Fi heat map for each location to optimize coverage.

Institutional building materials to consider that could affect coverage or require a high concentration of WAPs include but are not limited to the thickness of the concrete or cinderblock walls, size of the rooms, and type of material used and thickness of doors, such as solid steel doors.

Securus' WAP's are controlled and monitored by a Ruckus controller at our offsite data centers located in Dallas, TX.

Wi-Fi Access

The firmware only allows the tablets to connect to a Securus provided unique SSID (Service Set Identifier) for Wi-Fi. The credentials for the SSID are stored in the firmware of the tablet and the users have no access to view or modify these credentials. These security mechanisms prevent the tablet from connecting to any other Wi-Fi network other than the one provided by Securus for exclusive use by the tablets.

Securus uses Wireless Access Points that are manufactured by Ruckus Wireless, Inc. and are customized to only broadcast Securus approved SSID's to support Unity tablets.

i. This includes but is not limited to two-way radio systems, telephone and data systems (other than applicable cellular devices), fire alarm systems, environmental control systems, lighting, motors, pumbs, and electrical equipment.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Unity Tablet Program operates on a separate network from the CDOC secure network and will not connect or interfere with the CDOC infrastructure.

I. Should any damage occur, the Offeror will be responsible for any repairs required.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will also repair, replace, and update equipment and software during the course of the contract to maintain efficient operation of all systems at no cost to the CDOC.

J. The Offeror will provide all equipment and software necessary to provide tablet services including, but not limited to: hardware, wiring, network equipment, etc.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will furnish all materials, hardware, software, interfaces, cabling, switching equipment, internet connection, labor, and licenses to set up and operate the Securus Unity Tablet services. Securus will also repair, replace, and update equipment and software during the contract to maintain efficient operation of all systems at no cost to the CDOC.

As a part of this turnkey installation, Securus will install the following hardware in support of the Unity tablet program:

- Fortinet 24-port network switches
- Wall or shelf mountable servers
- Wireless access points (WAPs) with Ruckus controllers

The firmware only allows the tablets to connect to a Securus provided unique SSID (Service Set Identifier) for Wi-Fi. The credentials for the SSID are stored in the firmware of the tablet and the users have no access to view or modify these credentials. These security mechanisms prevent the tablet from connecting to any other Wi-Fi network other than the one provided by Securus for exclusive use by the tablets.

Securus uses Wireless Access Points that are manufactured by Ruckus Wireless, Inc. and are customized to only broadcast Securus approved SSID's to support Unity tablets.

K. The Offeror may utilize any existing hardware belonging to the CDOC that is available, if it is deemed to be suitable and approved by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

L. The Offeror will install and manage wireless networking equipment that will allow offenders to obtain the services requested.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

M. All equipment should be tamper resistant constructed of heavy duty materials and considered appropriate for a correctional environment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With more than 300,000 tablets in the hands of those incarcerated today, Securus has the experience necessary to ensure **tablet hardware is safe, hardened,** and easy to use. **This experience has been gained over a combined 40+ years of corrections experience**, and 10+ years' experience providing personal tablet devices. Securus recently introduced our fifth-generation tablet hardware, with each generation being more capable and secure than the previous generation.

Securus' proprietary JP6S tablet was custom designed, engineered, and manufactured to ensure the safety of the user and staff while providing a consumer-grade user experience. These tablets offer the memory, battery life, and operating systems that allow for a long-term solution with the capability to support multiple applications without any upgrades.

Securus removed all factory-provided applications and re-installed our proprietary Android-based operating system and applications.



Features

The JP6S tablet includes the following features:

- 22hrs standby time with LCD on and 350hrs with LCD off
- 140hrs music playback
- 13hrs video playback
- High strength ruggedized casing
- Impact-resistant security glass w/ integrated screen protector

- Barrel charge port
- Fast Wireless pogo-pin charging
- Dual WiFi Bands (2.4GHz and 5GHz) Built-in FM Radio Receiver

Specifications

The JP6S tablet includes the following hardware specifications:

- Internal Storage: 32 GB
- CPU: MT8163 - Quad core cortex A9
- Frequency 1.3G, 64bit CPU
- Resolution: 1280 x 800
- Dimensions: (L x W x H) 7.8” x 5” x 0.61”
- Weight: 17.2 ounces
- Battery: Lithium - 500 cycles, includes temperature sensor

Uninterrupted Power Supply

The Securus standard installation comes with a UPS for the Unity tablets that supports continuous power for the following critical components:

- Onsite server
- Network storage device
- Router
- Switch

Securus uses the Eaton 3S750 UPS, 450W UPS.

Pogo Pin vs. Inductive: Which Wireless Charging Is Better?

Both pogo pin and inductive charging provide the convenience of wireless charging; however, the big difference is how long it takes to fully charge a tablet. In corrections, speed matters. Pogo pin technology charges at a faster rate than first-generation inductive charging. Securus is committed to evaluating new technology and integrating it into new product offerings.

N. The Offeror will maintain and repair all networking and wireless network hardware and software for the offender network for the services requested.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will furnish all labor, materials, equipment, and services necessary to the installation, maintenance, and management of the new offender tablet services and related products. We will fully implement and support the ongoing operation of the Unity Tablet program. Securus' service model for CDOC includes

- Prioritizing dedicated project management, installation, implementation, maintenance, logistics, and other service support to ensure CDOC's needs are met and service expectations are exceeded where possible.
- Providing dedicated workflow coordinators for CDOC, which affords greater visibility, focus, and execution on issue resolution. These dedicated workflow coordinators will better support and facilitate the larger volumes in Tech Support needs for larger agencies like CDOC and will provide tablet ticketing support for offenders.
- Coordinating and collaborating across broader cross-functional issues with CDOC
- Providing customer-specific performance reporting

O. The Offeror will be responsible for all charges related to the purchase, installation, repair, or maintenance of all hardware and software related to the offender network for the services requested. This responsibility includes, but is not limited to, all costs which may result from:
i. The provision of services to any newly constructed building(s) at an existing CDOC facility;
ii. The provision of services resulting from modifications made necessary by CDOC changes at the correctional facility;
iii. Negligent or deliberate damage or loss; and
iv. any other damage or loss related to theft, fire, explosion, water damage, electrical power incident(s), acts of God (such as earthquake or flood).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THESE REQUIREMENTS.

All the equipment that Securus is proposing is corrections-grade hardware and backed by standard manufacturers' warranties. Securus will coordinate and facilitate all warranty claims and services. Notwithstanding these warranties, Securus will repair, replace, and update all equipment and software during the contract to maintain efficient operation of all systems at no cost to the CDOC.

P. The CDOC requires the Offeror to provide reliable high-speed fiber optic cabling at each facility, at no cost to the CDOC. The fiber optic network will be used for offender phone calls and wireless tablet services.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Q. Agree to transfer the Offeror-provided network to the CDOC at the expiration of the contract. This will include all applicable cabling and wireless equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

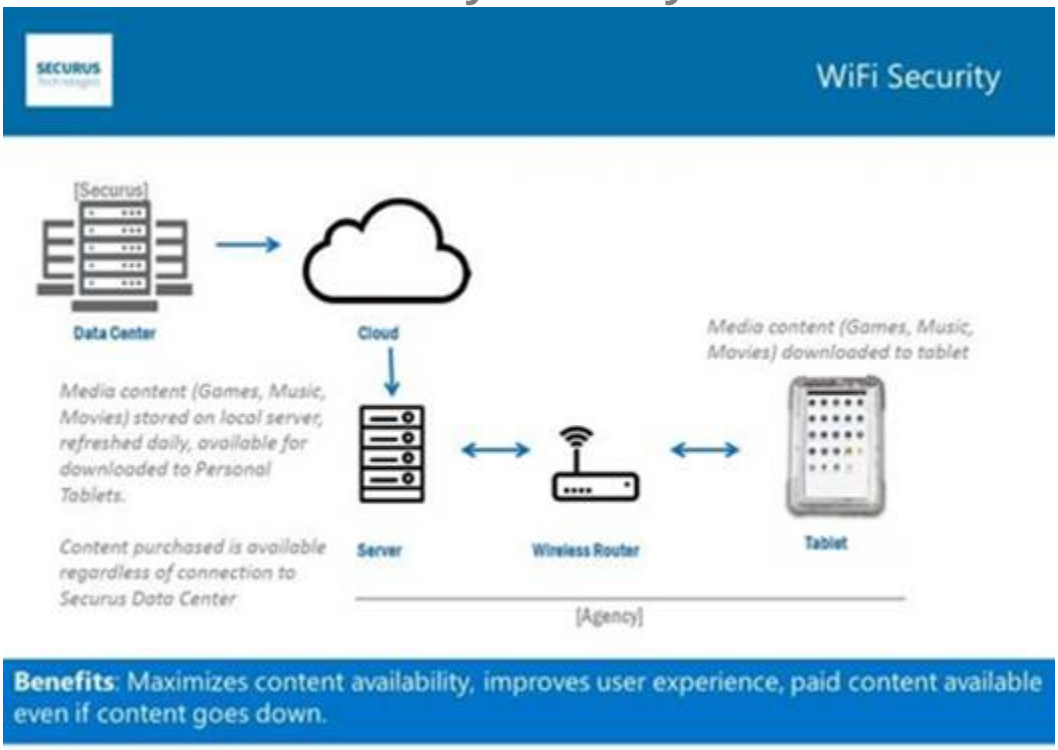
R. Offeror is expected to describe in detail all of the security built into their respective systems at the hardware, operating system, wireless infrastructure, network and application layers.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Both Unity tablet hardware and software have industry-best security practices. Internet access is restricted, ensuring users cannot surf the Internet or communicate through unauthorized channels with anyone outside of the facility.

W-iFi networks and on-premises equipment are monitored 24x7 to detect attempts to circumvent security controls.

Unity Security



Attempts are detected and responded to 24x7. Customers are notified of any unusual activity on tablets and kiosks as quickly as possible.

Securus provides multiple layers of security to ensure proper tablet usage and to prevent security breaches or tablet misuse.

Security Layer 1

Tablet Firmware

Securus Unity Tablets run a custom-developed proprietary firmware to harden their security and prevent any access to unauthorized content by the offenders. The customized firmware does not have any of the common apps that are found on consumer-grade tablets.

The following security measures have been taken to harden the firmware on these tablets:

- Browser, contacts, calendar, native phone, and messaging clients have been removed.
- The option to change configuration settings has been removed.
- Near-field Communication (NFC) and Bluetooth have been disabled, except for Wi-Fi (where applicable/approved).
- Authorized applications are pushed to the tablets through Securus' app state management process, thus preventing offenders from installing or un-installing apps.
- Tablets are prevented from accessing the public internet directly.
- Tablets are prevented from accessing third-party app stores.

WiFi Access

The firmware only allows the tablets to connect to a Securus-provided network using a unique SSID (Service Set Identifier) for Wi-Fi. Security mechanisms prevent the tablet from connecting to any other Wi-Fi network other than the one provided by Securus for exclusive use by the tablets.

Securus uses Wireless Access Points (WAPs) that are customized only to broadcast the SSID to supported Unity Tablets.

Security Layer 2

Securus Local Platform (SLP)

All the WAPs are connected to a Securus Local Platform (SLP) running Securus' custom-developed proprietary software. These SLPs have components that inspect all the network packets and provide firewall, transparent proxy, DHCP, DNS, and routing services for the tablets.

The Securus Local Platform is essential to all tablet functions. The SLP is configured to govern what the tablets can access. The tablet cannot receive any content from a network that the SLP has not been configured to provide. The SLP inspects all tablets' traffic and ensures that access is granted only to authorized content.

Although a tablet can connect to the WiFi network, it cannot obtain an IP address unless it is recognized as an authorized device by the SLP. If a tablet is not known by the SLP, it will *not* be granted access to the wireless network and will be rendered useless for applications that require network connectivity.

The SLP at the facility premises is connected to Securus' Data Center over an Internet Protocol Security Virtual Private Network (IPsec VPN) tunnel. The IPsec VPN service provides secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

Security Layer 3

Data Centers

Securus maintains a presence in three data centers in two geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.99% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier 4 (highest availability) data centers, including:

- Multiple power delivery paths
- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in, dual-door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Securus applies a high level of security to protect against cyber-attacks, and to secure its data. Applications transmitting data across public networks support SSL/TLS, Certificates, and 256-bit AES encryption. Routers, switches and firewalls are used throughout the network to protect Securus and our customers. All servers, laptops, and workstations require anti-virus and anti-spyware protection software and the latest operating system patches.

S. The Offeror will detail its ability to disable devices such as frequency modulation (FM) radio, Bluetooth radio, etc. as required by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All applications are configurable for enable/disable at the system level. Securus will work with the CDOC in advance of deployment to ensure all applications available are approved by the agency. Additionally, through our officer tablet, applications may be temporarily disabled by staff or the agency as a disciplinary tool, or for other agency designated purposes.

T. Requested devices is expected to be disabled in the basic input/output system (BIOS) and have no operating system driver installed to be classified as disabled.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Requested devices can be disabled in the basic input/output system.

U. The system at each CDOC Facility is expected to allow for authorized CDOC personnel located either at the facility or central administration to locally or remotely access each of the systems via a secure, password protected method.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All authorized personnel will have access to the system via password protected access through any appropriately internet abled system.

V. Authorized CDOC personnel is expected to have the ability to modify or view any data, privileges, accesses or restrictions pertaining to offenders based on CDOC-defined administrative rights.

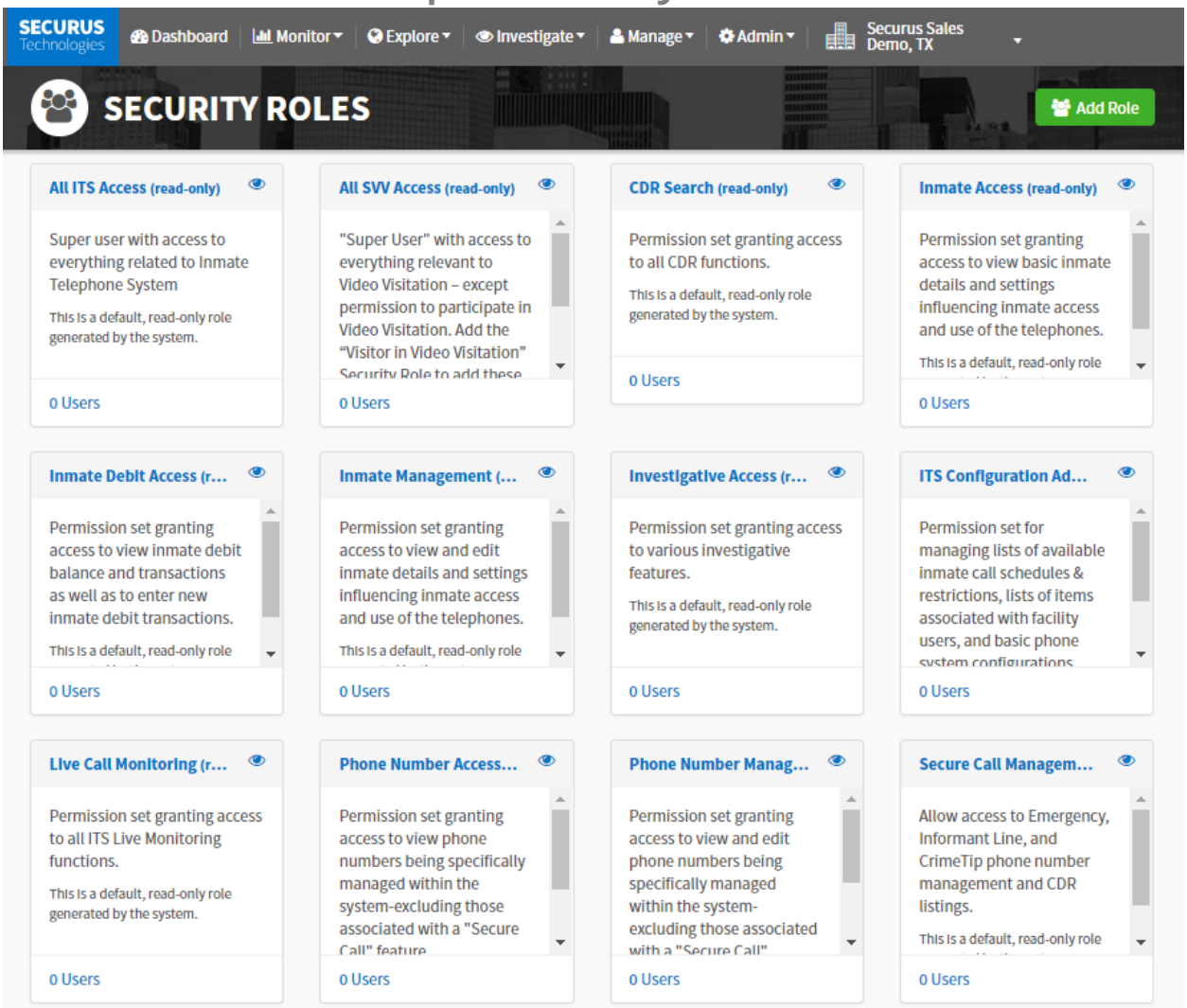
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

A variety of security levels provide multiple assigned access capabilities as assigned by the CDOC.

Security through least privilege; flexibility through customization: NextGen SCP is entirely permission-based and assigned user roles allow or prevent access to content, data, features, and privileges for each user. The platform comes with default security roles that cover most of our customer's needs for allocating access based on common job functions. CDOC may further customize security roles by duplicating and then modifying the default security roles or by creating new roles. Each user may be assigned one or several security roles, allowing unlimited options for structuring access to meet CDOC needs.

In addition, the facility administrator role can create, modify, activate, or deactivate users who have access to the NextGen SCP system.

Sample Security Roles



Default security roles identified by eyeball icon

Customized security roles identified by pencil icon

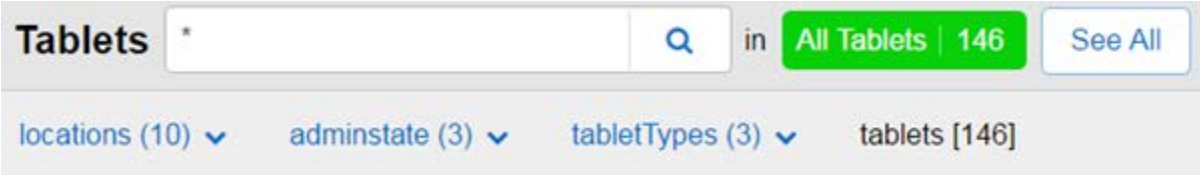
W. The system features will include, but are not limited to:

i. Centrally locate devices and remote wiping and/or blocking;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Using the tablet search feature of the Officer Tablet, facility staff can track a tablet in the event of a lost or inappropriate use. The search feature in the SubManager application provides authorized users the ability to look up information for a specific tablet, housing location, facility location, or tablet type. Tablets can be searched by offender

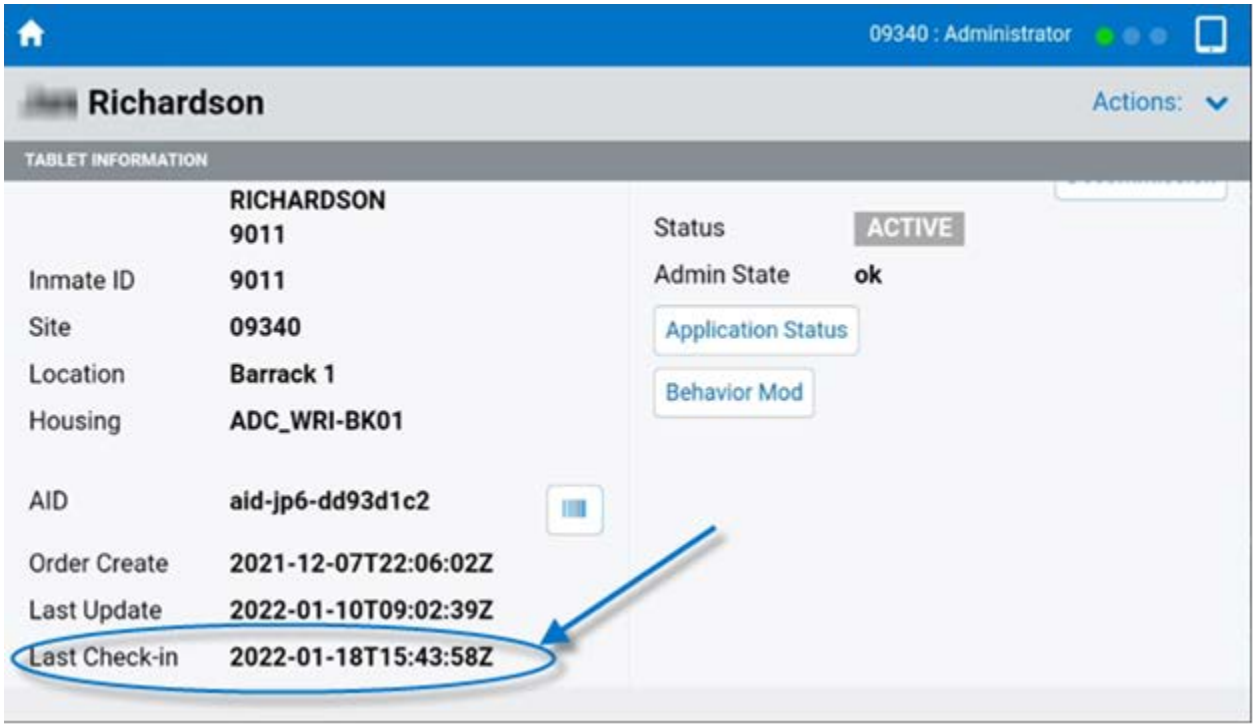
first or last name, offender ID, housing location, type of tablet (eg. offender vs. officer tablet), etc. The search window also provides convenient drop-down tabs to help officers filter their search.



From the search results, authorized staff can view an array of information linked to a particular tablet(s), such as offender screen name, offender ID, site, location, housing unit, AID, last update, type, and more.

The check-in date and time is viewable on the Officer Command & Control Tablet.

The tablet information page for SubManager has the last check-in date and time for an offender's tablet.



If any tablets are lost or you feel tablet security is compromised in any way, please alert Securus immediately so our Security team can engage and provide next steps to address the issue.

Wiping and/or blocking

After ending a tablet subscription, the Personal+ Tablet automatically reverts to a Personal Tablet, requiring no interaction by agency staff. During this process, all previously downloaded content is automatically removed from the device. Any content downloaded to a Community Tablet is wiped nightly. In addition, any tablets returned to Securus are wiped of any user identification or content.

Facility staff, using the Officer Command and Control Tablet, will have the ability to remotely wipe the tablet and/or block them from using one.

ii. Central and remote site network administration;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Command & Control Officer Tablets are customizable devices that can be distributed at your agency as needed. Agency staff can maintain complete control over all tablets at your agency. Staff can control tablet functionality by tablet, group of tablets, or all tablets at the agency in real time. Applications available on a tablet can be controlled at once or on an app-by-app basis. Officer Tablets can be configured for various roles & permissions that allow the appropriate staff the ability to control tablets under their jurisdiction. Securus knows this level of control is critical for a successful tablet program.

Officer Tablets have detailed dashboard views that allow your staff real-time search functionality and analytics. Administrative functionality on the dashboards is comprehensive and flexible. Individual staff can have a customizable level of control based on your desired specifications.

Roles and Permissions Feature

Access to certain functionality on Officer Tablets is configurable to allow for hierarchal support structures. A remote administrator's tablet can allow or deny certain privileges to other Officer Tablets accordingly.

Predefined Roles and Permissions, or the creation of customized facility Roles and Permissions, make it even easier to assign certain privileges to designated staff Officer Tablets.

Roles and Permissions can be set agency-wide or based on the area of supervision of the Officer Tablet user.

iii. Centralized management of installed / accessible packages;

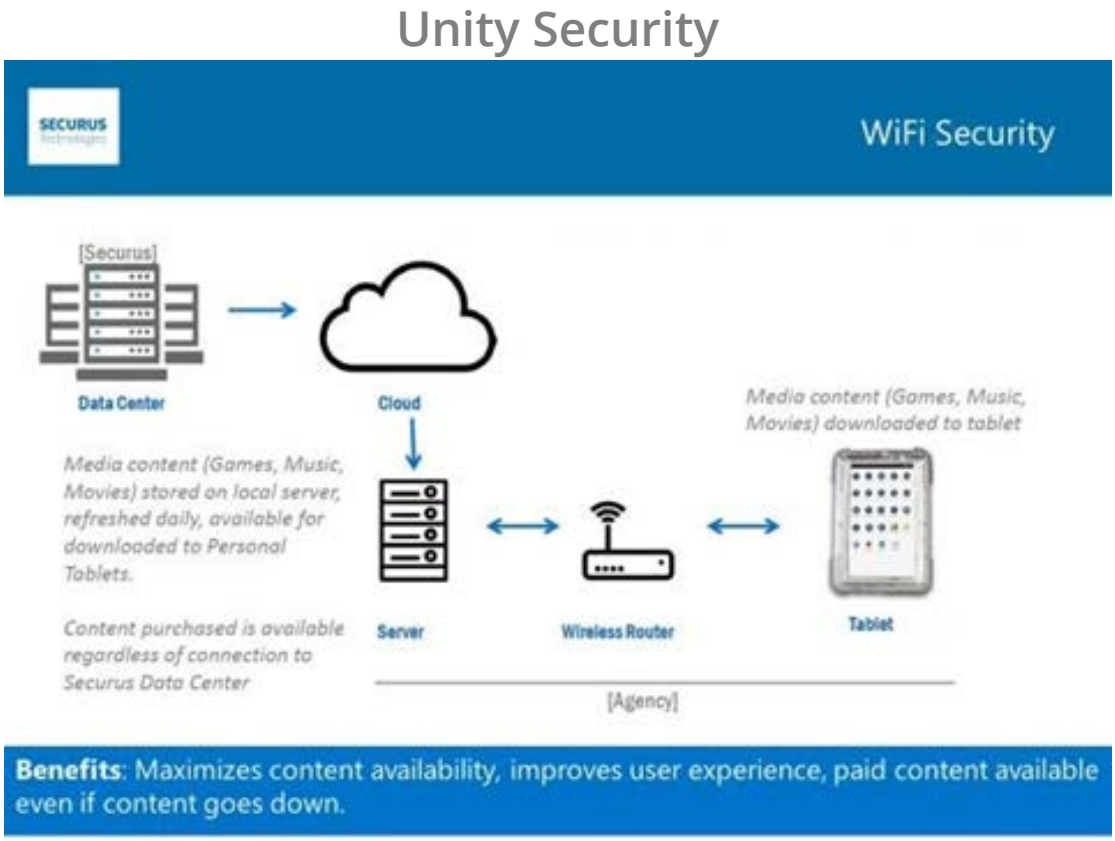
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

iv. Access point (AP) isolation or other technology to prevent unapproved communication between tablet devices and other networks;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Both Unity tablet hardware and software have industry-best security practices. Internet access is restricted, ensuring users cannot surf the Internet or communicate through unauthorized channels with anyone outside of the facility.

Wi-Fi networks and on-premises equipment are monitored 24x7 to detect attempts to circumvent security controls.



Attempts are detected and responded to 24x7. Customers are notified of any unusual activity on tablets and kiosks as quickly as possible.

v. Centralized management of authentication mechanisms; and

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

vi. System reporting.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

CDOC can receive a monthly tablet application usage report for the entire CDOC population for the previous month. These reports come from Securus and are broken down by application. This can be provided at no cost to the agency. Your Securus Account Manager can provide additional reports related to tablet usage upon request.

In addition, the Job Search application can track and measure the job search activity of your agency and provide you with access to detailed reports.

Likewise, the Forms and Grievance Application provides staff supervisors the ability to:

- See reports of the volumes and progress of forms through the workflow
- See pie charts representing age of forms currently in the workflow
- Assign staff members to process specific forms

Securus provides as much usage information as possible for administrative and investigative purposes. CDOC can receive a monthly tablet application usage report for the entire CDOC population for the previous month. These reports come from Securus, are broken down by application, and are provided at no cost to <<client>>.

In addition to the monthly usage reports and upon request, your Securus Account Manager can provide daily usage reports broken down by the following activities:

- Application
- User
- Location
- Additional detailed data

16. INMATE TELEPHONE SYSTEM (ITS)

A. The system is expected to allow for CDOC investigative personnel located either at the facility or central administration to remotely access each of the systems via a secure, password-protected method. Authorized CDOC personnel is expected to have the ability to change, modify or view any privileges or restrictions pertaining to offenders at their facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP's advanced features provide extremely powerful and flexible tools for controlling offender calling, reducing fraud, increasing investigative capabilities, and generating valuable administrative reports. The system adapts to your facilities and operations, rather than requiring you to conform to the software.

The Securus development team custom-built NextGen SCP for the corrections industry, creating a fully integrated system of simple-to-use software tools, and computer and telephony hardware for the calling service. The hardware and software components readily adapt to the changing needs of a facility's operations, and can monitor, record, and block/unblock telephone calls, and generate reports in real time.

With software updates provided three to four times per year, Securus will keep CDOC on the cutting edge of technology without any additional cost for system upgrades. Because the calling service operates on the centralized NextGen SCP, Securus can customize our solution to your specific needs, addressing the specific operating requirements of your department both today and well into the future.

The calling service will support CDOC in safeguarding the community through proactive fraud prevention and advanced investigative capabilities. It allows our customers to operate a smarter and more efficient jail through system interoperability while providing the flexibility to interface with your current operations. The investigative tools permit a higher degree of accuracy and allow investigators to locate calling information more quickly and reliably. The system is scalable and flexible, reducing labor demands by automating many tasks. Routine calling operations can be configured to require minimal administration, allowing your staff to focus on what they do best—maintaining a safer, more secure correctional environment.

The calling service provides anywhere, anytime access for authorized personnel. All the investigative and administrative resources are available to approved personnel through the NextGen SCP user interface. Users can access calling services features any time from any Windows-based computer with access to the internet, allowing your investigators to follow the leads wherever they may go.

Calling Features

The calling service gives CDOC control over system features. That means you have complete control to customize the system to your specific needs, even as those needs change. We are committed to using technology to help you safeguard the public and solve and prevent crimes.

Key features include:

- Centralized architecture
- Anytime/anywhere system access using an internet-enabled computer from any location
- Real-time software/system upgrades three to four times per year at no cost to CDOC
- Premium digital quality superior to that of analog-based systems, which is especially important for investigative purposes
- Remote monitoring 24x7x365 from Securus' Network Operations Center—we monitor system performance and can recognize and correct problems before you are aware of them.
- Advanced call recording management through a patented technology to safeguard the chain of evidence controls on each recording, backed by free, professional testimony
- User-friendly reporting and self-help capabilities

Investigative Tools

- Monitoring and recording available on all calls that are not marked as 'private'
- Patented three-way call detection and prevention
- Patented remote call forwarding detection
- Perma-Block allows called parties to block future calls from the facility
- Covert Alert with Barge-In
- CrimeTip hotline
- Scan Patrol
- Case tracking (call notes)
- Investigative reports, such as frequently called numbers, pattern dialing reports, and more
- THREADS call analytics
- Voice biometrics, including IPRO

- Reverse Lookup

Fraud Controls

- Patented three-way call detection and prevention
- Patented remote call forwarding detection
- Dual tone multi-frequency (DTMF) detection to prevent:
  - Secondary dialing
  - Switch hook dialing
  - Black boxing
  - Hacking
- Velocity restrictions

Service Features

- 24x7x365 Network Operations Center monitoring
  - You operate around the clock, and so does Securus. We can find and fix most problems before you are aware of them and we are here to help you with your questions and requirements whenever you need us.
- 24x7x365 Technical Support through Securus' in-house Technical Support Center
  - We have the largest employee base in the industry to serve you better and to make sure we continue to lead with enhanced technology.
- 24x7x365 end-user support through our in-house Securus Friends and Family Call Center (SFFCC)
  - Securus is unique among national competitors in that we operate our call center. We do not outsource our customer experience. We find our end-user satisfaction ratings improve 22% when they use our call center. Providing good service to your constituents cuts down on complaints and provides a better experience for all. We are available to serve callers 24 hours a day.
- Ongoing training as well as training for each new software release (typically provided three to four times per year)

Call Completion

- Convenient points of sale and cost-effective terms for prepaid friends and family accounts
- Numerous funding options
- In-house SFFCC

- Lobby Kiosks
- Website funding
- Western Union funding
- MoneyGram funding
- Collect, prepaid collect (AdvanceConnect), prepaid calling cards, and debit options
- offender PINs
- offender PANs
    - Like all other features of NextGen SCP, the PAN lists are flexible and may be administered in various ways: PANs can be configured manually, automatically, or by importing through integration.
- Patented Automated Operator Services (AOS)
- Customizable call prompts, branding, and overlays
- Multi-lingual call prompts
- offender name recording

Administrative Features

- Audit and activity tracking of system users
- Multi-level password controls

Call Controls

- Global blocked number lists
- Global allowed number lists
- Calling restrictions, including duration and velocity by offender, dialed telephone number, offender phone, phone group, customer, or facility
- Automatic or manual system on/off controls
- Emergency Call
- Automatic management of calling restrictions

B. The system features should include, but are not limited to:

i. Central and remote site network administration;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

ii. Centralized CDOC system database;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

iii. Automated operator;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP™ includes an Interactive Voice Response (IVR) system that provides Automated Operator Services (AOS). The AOS uses clear and concise, professionally recorded voice prompts to establish call acceptance and to assist offenders and called parties throughout the calling process.

When the called party answers the phone, the advanced answer detection triggers the call acceptance voice prompt. The called party hears, "Hello, you are receiving a collect call from [offenders's name], an offenders at the DCOC. This call is subject to monitoring and recording." NextGen SCP then gives the called party the following menu options:

- "To accept this call, press 1."
- "To refuse this call press 2."
- "To hear the rates and charges for this call, press 7."
- "To block future calls to your number, press 6."

The AOS feature reflects the options that are configured for that specific site to limit the menu and expedite prompt flow.

The following are examples of the information provided:

Available Options to Called Parties	Available Options to Offenders
• Request a rate quote • Hear the name of the facility and offender calling • Accept or reject the call • Request available balance of an AdvanceConnect account or available credit of the Direct Bill account • Hear instructions on how to add more money to their prepaid account or pay their Direct Bill Account • Connect to a live agent to setup a pre-paid account	• Listen to prerecorded announcements • Choose to place a collect or debit call; if debit, PIN entry is requested, the offender hears the available balance in their account and the cost of the call • Select a specific language at the beginning of the call (if configured) • Acknowledge that the call is going to be monitored and recorded • Hear available call time (prompt will tell the offender call time limits based

• Choose to hear the prompts on the system in English, or the language selected by the offender (if configured for this option) • Pay for the incoming call with even when they do not have a Securus Account • Hear optional messages (by request of CDOC) • Block their number prior to accepting a call	on calling schedules or calling restrictions) • Identify themselves by PIN or Voice Biometrics (if configured) • Add, remove, and/or listen to the phone numbers on their PAN list (if configured) • Hear optional messages (by request of CDOC)

***The calling service's automated operator also provides a Perma Block process, which allows a called party to block their number permanently. This feature may be used to block calls from any offender in the facility. The ability to immediately block calls helps reduce the number of called party complaints. The called party can also choose to end the call by hanging up.**

iv. Call branding;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Calling Service uses customized, professionally recorded voice prompts to guide an offender and the called party through the process of placing and accepting calls. Voice prompts are configurable to meet the needs of the CDOC branding and variable options are available. CDOC may add announcements during call setup, call acceptance, when an event occurs, or to prompt an action from either party. Securus provides multilingual support for voice prompts in 15 languages, and up to nine default language options for CDOC facilities. The called party may then select between English and the offender's selected language on each call.

v. Call blocking (including 911 and incoming calls);

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen Secure Communications Platform™ (NextGen SCP™) allows authorized facility personnel to manage blocked numbers using the platform user interface. Blocked numbers can be applied at various levels—facility, site, phone group, phone and offender. NextGen SCP offers unlimited blocking so the resulting call blocking table that is created may contain as many entries as needed. In addition, there is an associated "Description" field that allows for additional information to be attached.

Typically, the call blocking list includes the phone numbers of local judges, sheriffs, facility personnel, jury members, attorneys and witnesses. This feature prevents offenders from making calls to the specific numbers listed in the table.

Securus will upload your call blocking list during the installation process to eliminate the burden of initial setup from your facility staff. All dial-around area codes and

exchanges, such as 800, 900, and 976, are blocked by default. Access to live operator services, such as 0, 411, and 911, are also blocked by default.

vi. Three-way call blocking and detect;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Calling Service offers a robust three-way call prevention system that was designed and patented by Securus. Independent tests proved and certified the effectiveness of the Securus three-way call detection feature. Securus can provide demonstrations of our industry-leading feature and its effectiveness tests if scheduled by CDOC.

Detecting and preventing three-way or conference calls is a very important aspect of an offender calling service. Securus Calling Service three-way call prevention is more advanced than traditional systems. It makes it extremely difficult to enlist the aid of an outside accomplice to conference them, via three-way calling, to an unrestricted line to bypass system controls. Our system blocks access to the outside world.

Gain investigative intelligence and stop revenue-leakage from calls that should not be connected: CDOC may configure the system so that when a three-way call is detected either (i) the call is immediately disconnected with a message to both parties and a note in the call record, or (ii) the call will continue but a note will be added to the call record. CDOC may also configure the system to disable three-way call detection on a particular number or groups of numbers, such as attorneys.

vii. Call forwarding detect;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus leads the industry in fraud detection and prevention through real-time Remote Call Forwarding (RCF) detection. Our RCF solution can immediately terminate a call if it detects that a called party's telephone number is call forwarded to another telephone number.

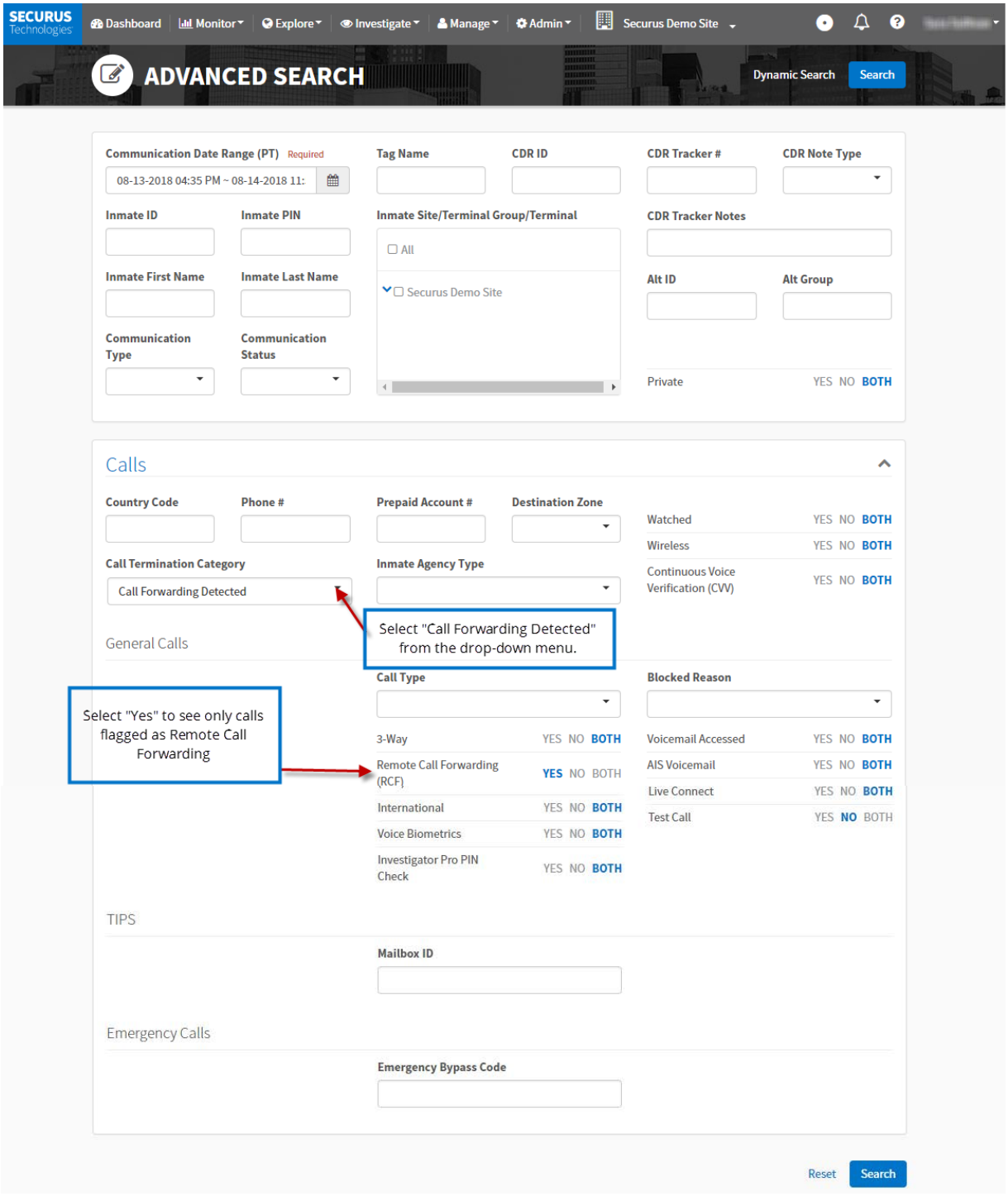
If false disconnects are a concern, the calling service can also be configured to allow the call to continue with one of the two following options:

- Announce to the offender and called party that remote forwarded calls are not allowed, and mark the call in the call record
- Mark the call in the call record, without an announcement to the offender and called party

The NextGen Secure Communications Platform™ (NextGen SCP™) user interface allows authorized users to create Call Detail Reports for those RCF calls by selecting "YES"

under the “RCF” attribute, using the specific termination code “Call Forwarding Detected,” as shown in the following image.

Call Forward Detection



viii. Call acceptance monitoring;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

For a call between an offender and a called party to take place, a valid call answer-and-acceptance must occur. The system must distinguish between legitimate call acceptance and other telephone activities such as:

- Network ring/busy signals
- Answering machines
- Operator intercepts
- Signal Interface Tones (SIT tones)
- Pagers
- Hacking
- Chain dialing

Our calling service uses call progression technology and other detection techniques to validate each call answer-and-acceptance event. The feature also enables the system to state the specific reason for the call termination when an offender's call does not complete.

Active Acceptance/Called Party Acceptance

The Securus calling service requires active "called party" acceptance using touch-tones to complete calls. When the called party answers the phone, the calling service's answer detection triggers the call acceptance voice message. This message announces the offender's call and asks the called party to accept or reject the charges of a collect call. The called party is instructed to dial a single digit on their telephone to accept the collect call charges, or hang-up to disconnect the call and refuse charges.

ix. Call duration limits and other offender calling restrictions;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) can be used to set a maximum time limit for any or all calls related to either an individual PIN or all PINs. The calling service will then automatically manage all imposed durations, reducing the workload for facility personnel.

The system will give the offender a verbal announcement one minute prior to end of their call and then enforces the facility policy with a hard stop.

Programmable Call Restrictions

As offender phones are a shared resource, facilities often need to enforce the equitable sharing of them. While Securus will install additional phones as needed, sometimes space and logistics preclude this option. In that case, CDOC may use call restrictions to regulate offender access to ensure access by all offenders.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides calling restrictions to give CDOC control of calling activity at the offender, port, phone group, facility, or customer level. Multiple restrictions can be crafted within each restriction set.

Examples of call restrictions are:

- Maximum number of calls per day/week/month
- Maximum type of calls per day/week/month
- Maximum number of call connects, accepts and/or mins of talk time

All imposed calling restrictions are automatically managed by the NextGen SCP system to relieve facility staff of calling restriction enforcement responsibilities.

Restrictions may also be used for punitive measures or behavior modification by restricting access versus revoking complete access as done through suspension.

Offender Calling Restriction Profiles

CDOC can set up Offender Calling Restriction Profiles to limit the number and length of calls an offender can make by day, week, or month. These "velocity" Restrictions are applied to an offender's Custody Account. The limitations can be set for a specific call type such as Collect calls, Free calls, or Crime Tip calls; or for all call types depending on CDOC needs. Authorized officers at CDOC can create as many calling restrictions as necessary to meet the facility requirements, then select the profile that best fits each offender.

How it Works

When offenders enter their PIN, the system checks their daily, weekly, and monthly calling restrictions before connecting the call. If an offender has exceeded any of the limits, the call is blocked. During an accepted call, the system ensures the time limit is not exceeded for the restricted time frame.

Calling Restrictions can be setup in multiple ways:

- **By Facility –** The entire agency follows the same set of restrictions.

- **By Site –** Each site within a facility has its own set of restrictions.
- **By Phone Group –** A group of phones that use a particular calling limit that is different from another phone group in a facility.
- **By Offender –** An offender's custody account is setup with a specific calling limit.
- **By Call Type Exclusions –** Certain call types can be excluded from a calling restriction (i.e. Crime Tip, PREA or Private calls).

x. Call monitoring and recording;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP™ has an integrated recording and monitoring system that is a cost-effective solution for correctional facilities of any size. Multiple levels of security ensure that only authorized personnel can access and monitor the offender recordings. Authorized personnel can listen to live or archived recordings via multi-media PC interfaces connected over local area networks (LANs).

Call Monitoring

The NextGen SCP Monitor Activity function allows for real-time monitoring of calls in progress via a multi-media PC workstation. Authorized personnel can monitor live calls by highlighting the call in progress and clicking on the handset icon ( ).

The NextGen SCP Scan Patrol feature is an extension of the Monitor Activity function, providing CDOC personnel with the ability to automatically cycle through live calls in brief intervals of time. This creates an opportunity to determine the relevance of call content for requesting further detailed analysis, Users enter a specific amount of time for the system to play each call before moving to the next active call, similar to an automobile scanning function. Scanning begins on the first active call posted and continues to the next active call, before looping back to the first active call once the scan has completed a cycle.

These processes are undetectable by the offender or the called party and will not disrupt the recording process. Concise descriptions of activity are shown for each phone in use. For example, the system shows the offender name, offender ID, dialed number, start date/time, and duration of calls. One additional feature in the NextGen Monitor Activity function is the Recent Activity tab that provides information related to recently ended calls. This gives listeners the advantage of quickly accessing a call that just ended and is no longer designated as an actively monitored call.

Additional functions available through Call Monitoring include:

- Forwarding a call to an investigator for case-related call monitoring
- Terminating a call if agency security or policies are being violated
- Adding notes, which are later viewable as part of the CDR, to an in-progress call
- Accessing recent calls to the same phone number
- Accessing recent calls from the same phone terminal
- Viewing BNA information of called party

NextGen SCP does not record any calls with entities your agency has designated as private, such as calls with legal counsel or clergy. It prevents all unauthorized attempts to listen to private calls and does not provide an option to monitor the call on these designated private calls. The communication record also clearly indicates the call as "private" in the user interface and will not contain a recording.

Call Monitoring, Silent

When monitoring occurs, the system incorporates analog suppression/amplification hardware to monitor calls without offender or called party detection. There is no noise, volume loss, or other indication of monitoring to ensure complete investigator anonymity.

Call Recording

The integrated calling services recording application works independently, so integration with a third-party is unnecessary. This allows your facility to deal with a single vendor if any issues arise. NextGen SCP also shows if the call was accessed, available call notes, or if the call is flagged. Clicking on a call will open a side-bar and any associated details for the communication event, such as the billing name and address (if available), phone location details, call type, call status, CDR ID, termination category, cost of the call, and the call prompt language selected. This side-bar provides an easy method for downloading the call recording, extending the expiration retention period date for a call recording, a note capability for he CDR, and access for viewing the recording historyall with a single mouse click.

NextGen SCP writes all recorded calls to a Network Attached Storage array (NAS) in our primary Data Center. Each NAS array is also replicated to the secondary Data Center for redundancy and failover. All recordings created on the platform reside in at least two of our Data Centers. Recordings are stored online for immediate access for two years. NextGen SCP can also be used to copy the recording and call detail information to a digital file that can be transferred to CD or DVD for additional back up, if necessary.

The calling service records all calls simultaneously and allows personnel to listen to previously recorded calls while active calls continue to be recorded. The system records the entire conversation from call acceptance to termination.

Remote Access to Recording and Monitoring

With integrated recording and monitoring applications, other agencies, such as local police departments, can also access these functions. Any user that CDOC approves can access the recording and monitoring function of offender calls from any computer or device with internet access. Securus has tested and certified call playbacks and live monitoring on:

- Operating Systems/Devices
  - iOS
  - Android OS
  - OS X
  - Windows
- Browsers
  - Chrome

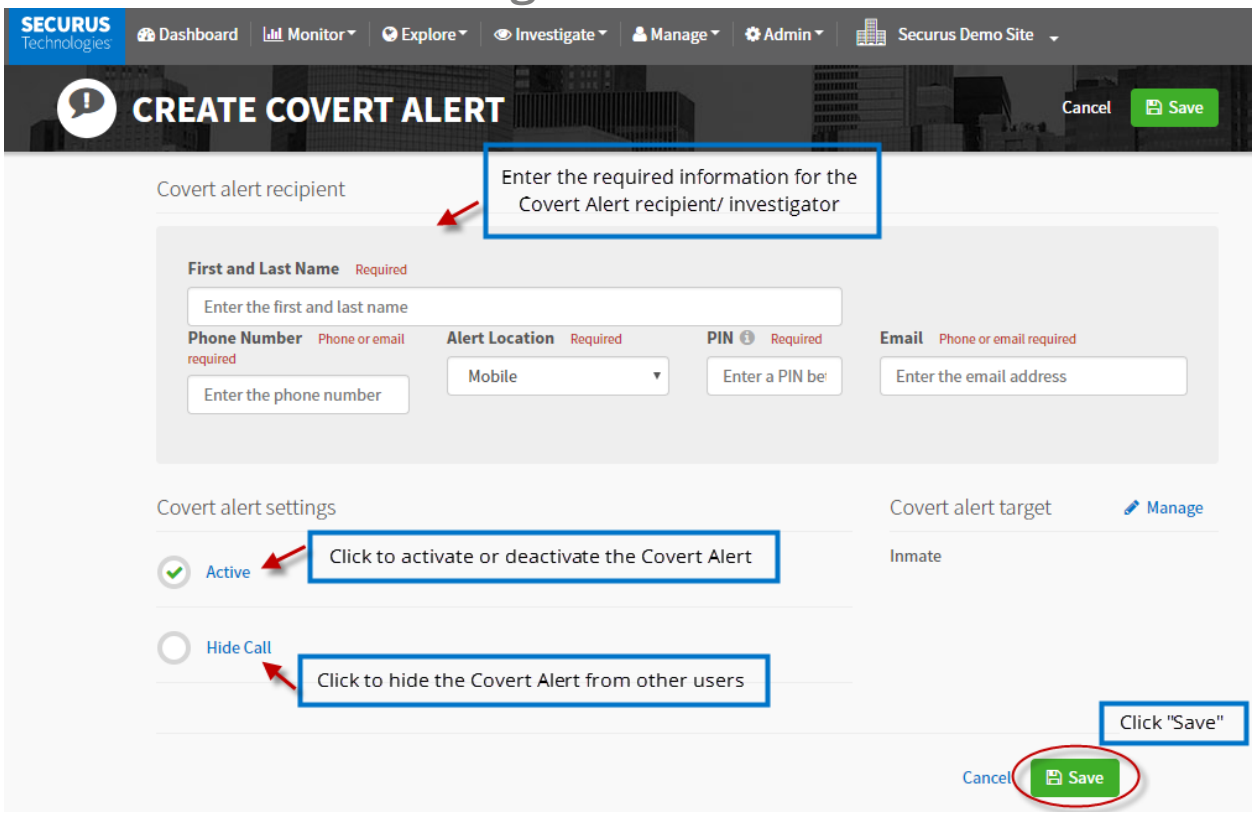
xi. Hot number tracking;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen Secure Communications Platform™ (NextGen SCP™) includes the Covert Alert feature that will automatically forward a live call to an investigator at a designated phone number in listen-only mode to offer real-time monitoring of a call. Covert Alerts can be set for a to a specific phone number, from a specific offender, or all calls from a specific terminal.

Covert Alerts are administered on the Manage Covert Alerts page. In addition, Covert Alerts for specific offender can easily be crafted and managed from the Offender Activity page.

Creating a Covert Alert



Covert Alert can bridge a call to an authorized remote number for dialed numbers, phones, or offender PINs are under surveillance by investigators. The Covert Alert feature allows authorized personnel to monitor a call, from any location, while the call is in progress.

When a call is placed by an offender, to a phone number or from a terminal that has a Covert Alert trigger, it is automatically sent to the designated investigator phone number(s) in stealth mode. A call can be sent to multiple numbers simultaneously allowing several investigators to listen to the call.

Covert Alert can send calls to any phone number within the facility or across the United States. Investigators can also monitor calls through on-site workstations using the NextGen SCP Monitor Activity page, or remote live call-forwarding feature. This allows facility investigators to monitor potential illicit activities regardless of the investigator's location.

Covert Alert can also be set to send an email to the investigator(s) with information about a Covert Alert call including date, time, offender PIN, originating telephone, and

dialed number immediately after the called party accepts the call. The following figure provides a sample alert:

Alert Notification



Additional Security Feature

For extra security, Covert Alert can be configured to require a PIN to listen to the call. If activated, a customizable message will state, “This is a Covert Alert call from John Smith, an offender at CDOC. To accept this Covert Alert call, please enter your investigator PIN now.”

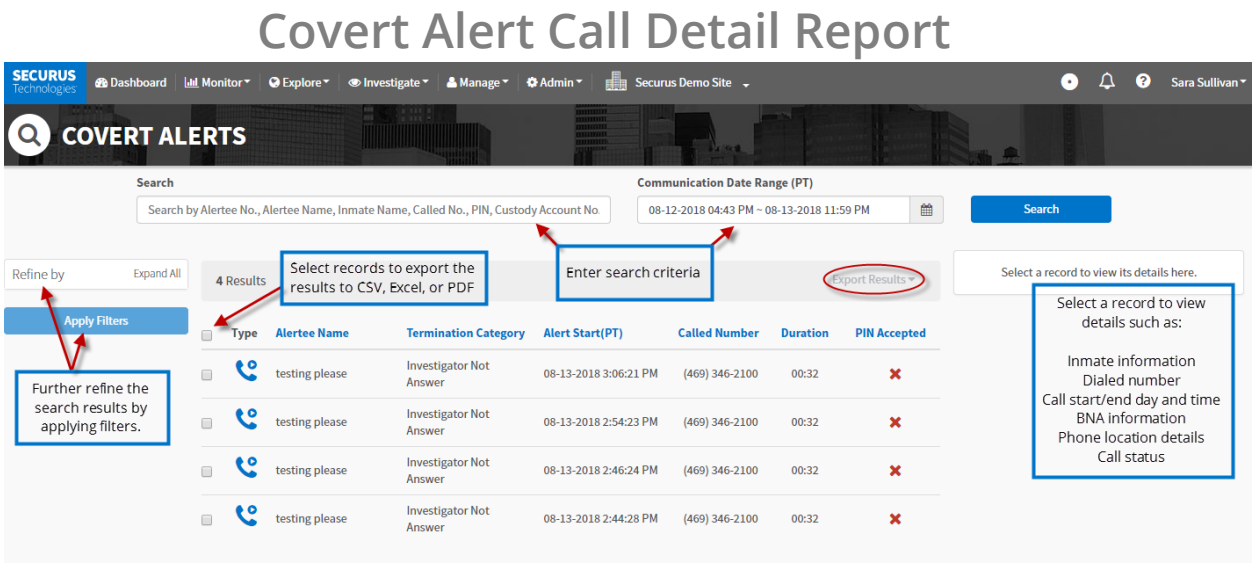
"Barge In"

While on the Covert Alert call, the investigator can immediately terminate the call by pressing a predetermined code. Covert Alert can also be configured to allow investigators to enter a code and interrupt the call and speak to both the offender and called party.

This "Barge In" feature is available through both Covert Alert and on calls forwarded from NextGen SCP Monitor Calls page. When monitoring a conversation, the call can be forwarded to an investigator cell phone, office phone, or other designation, allowing them to barge into the conversation using the predetermined barge-in code and acceptance digit.

Covert Alert Call Detail Record Report

The Covert Alert Call Detail Record Report allows authorized users to search for calls that triggered a Covert Alert. The report provides comprehensive detail regarding the call.



xii. System reporting;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Identify trends, investigate suspicious activities, and manage usage: The NextGen SCP retains communication detail records on all communication attempts and events. NextGen SCP has a report writer that provides investigative information based on the communication detail records. CDOC may search and analyze details on all

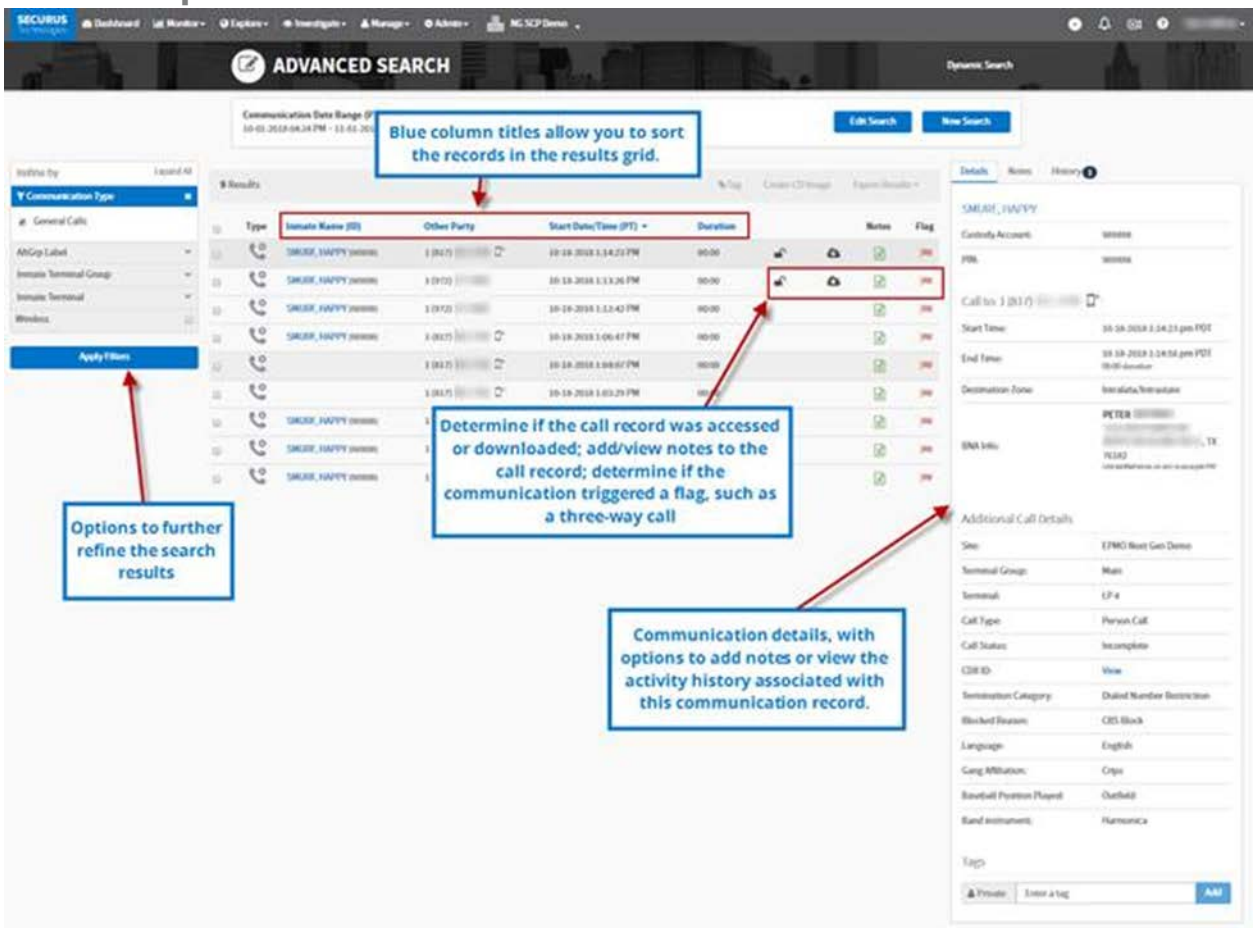
communication events through NextGen SCP and then run reports to identify communication trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

Custom and standard searches worth sharing: NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on an extensive list of criteria options. CDOC also may create customized reports by changing search criteria. After search results are generated, you can sort based on any of the communication event details. Then, with a single click, the data exports to Excel, CSV (Comma Separated Values), or Adobe PDF format and may be saved, printed, or emailed to others.

NextGen SCP™ Report Criteria Fields

- Date Range
- Identifier (ID, PIN, Name)
- Continuous Voice Identification
- Communication Type (Calls and Video)
- Communication Status (Complete or Incomplete)
- Prepaid Account Number
- Destination Number (Partial or Full Number Entry)
- Call Type
- Three-Way or Remote Call Forwarding Detected
- Watched Status
- Wireless Indicator
- Visitor and Visit Type (SVC)
- Visitor Contact Number
- Visitor Identifier (ID, Name, Email)
- Phone or Terminal Location
- Number Restriction and/or Status Assignment
- Broad Search with No Data Entry
- Suspected Fraudulent Call Activity
- Destination Zone (Local, Interlata, Interstate, Intralata, International)

Sample Communication Detail Results Screen



xiii. Ability to restrict offender's calls to 25 numbers approved by CDOC staff;

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As offender phones are a shared resource, facilities often need to enforce the equitable sharing of them. While Securus will install additional phones as needed, sometimes space and logistics preclude this option. In that case, CDOC may use call restrictions to regulate offender access to ensure access by all offender.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides calling restrictions to give CDOC control of calling activity at the offender, port, phone group, facility, or customer level. Multiple restrictions can be crafted within each restriction set.

Examples of call restrictions are:

- Maximum number of calls per day/week/month
- Maximum type of calls per day/week/month
- Maximum number of call connects, accepts and/or mins of talk time

All imposed calling restrictions are automatically managed by the NextGen SCP system to relieve facility staff of calling restriction enforcement responsibilities.

Restrictions may also be used for punitive measures or behavior modification by restricting access versus revoking complete access as done through suspension.

Offender Calling Restriction Profiles

CDOC can set up Offender Calling Restriction Profiles to limit the number and length of calls an offender can make by day, week, or month. These "velocity" Restrictions are applied to an offender's Custody Account. The limitations can be set for a specific call type such as Collect calls, Free calls, or Crime Tip calls; or for all call types depending on CDOC needs. Authorized officers at CDOC can create as many calling restrictions as necessary to meet the facility requirements, then select the profile that best fits each offender.

How it Works

When offenders enter their PIN, the system checks their daily, weekly, and monthly calling restrictions before connecting the call. If an offender has exceeded any of the limits, the call is blocked. During an accepted call, the system ensures the time limit is not exceeded for the restricted time frame.

Calling Restrictions can be setup in multiple ways:

- **By Facility –** The entire agency follows the same set of restrictions.
- **By Site –** Each site within a facility has its own set of restrictions.
- **By Phone Group –** A group of phones that use a particular calling limit that is different from another phone group in a facility.
- **By Offender –** An offender's custody account is setup with a specific calling limit.
- **By Call Type Exclusions –** Certain call types can be excluded from a calling restriction (i.e. Crime Tip, PREA or Private calls).

xiv. Ability to assign approved offender contact numbers to "speed dial" numbers.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Calling Service through the NextGen SCP™ gives CDOC unlimited options to configure speed-dial functionality. CDOC chooses and assigns speed dial numbers such as 101 or 111 to numbers frequently called, including medical alerts, commissary, and officer assistance. The speed dial numbers may range from 3 to 10 digits. CDOC may also assign a 10-digit speed dial number that automatically routes to an investigator's phone. This feature allows the investigative team to provide a phone number without revealing their direct number.

C. The Offeror will install offender telephones and all related equipment including wiring for the offender telephones, installation, and any related hardware and software/firmware specifically identified in this SOW without cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will install offender telephones and all related equipment including wiring for the offender telephones, installation, and any related hardware and software/firmware specifically identified in this SOW without cost to the CDOC.

17. INMATE TELEPHONE SYSTEM (ITS) FUNCTIONALITY (GENERAL)

A. The Offeror will provide the ITS with a technology system fully supported by an infrastructure which has the capability to provide specified services such as secure and real-time monitoring of offender telephone calls meeting the CDOC's ITS security expectations. In addition, the ITS will contain a secure database for transactional call records and provide data feeds to the CDOC's official data repository.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus system will provide the ITS with a technology system fully supported by an infrastructure which has the capability to provide specified services such as secure and real-time monitoring of offender telephone calls meeting the CDOC's ITS security expectations. Securus will work with CDOC authorized personnel to ensure that the ITS will contain a secure database for transactional call records and provide data feeds to the CDOC's official data repository.

B. Offeror is expected to have functionality to allow or establish approval processes based on hierarchy or named group before an event is allowed to occur.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. Authorized CDOC staff will be responsible for providing a daily "offender location" and "offender ID number" to the Offeror. The authorized CDOC staff will determine the type, format and transmission method of the daily "offender location". Authorized CDOC staff will define the specifications of the requested data feed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

D. The Offeror will provide complete support of all ITS software necessary to ensure provision of services at all times throughout the duration of the Contract. In addition, the Offeror will monitor changes to associated interfaced systems and accommodate changes in their ITS as needed to continue operations of the services and ITS as specified herein.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Network Operations Center (NOC) provides remote monitoring of systems and interfaces on an ongoing basis and identifies changes that impact the system. As described elsewhere, Software upgrades are issued on a regular basis to ensure the system functions to its maximum efficiency.

E. The ITS will be restricted to outgoing calls only. The ITS will not process incoming calls at any time. The ITS will allow authorized CDOC staff to program times when the ITS will be operational.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

To ensure maximum security to the system, Securus provisions the trunks in the calling service data center as outgoing only, ensuring that no incoming calls can reach the offender. Securus has performed full testing of these trunks, verifying compliance with this requirement.

F. The Offeror will comply with Code of Federal Regulations (CFR), Title 47, Volume 3, Part 64.710, identifying that the call is coming from a specific offender at a specific CDOC facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. The ITS will have the capability to be deactivated (shut down), by authorized CDOC staff or Offeror staff as authorized by CDOC. The ITS will be capable of deactivating the ITS ID feature by individual offender telephone, group of telephones and/or entire facilities, at the authorized CDOC staff's option. Regardless of the deactivation, the ITS will restrict offender calls to:

i. Prepaid collect;
ii. Normal collect;
iii. Local;
iv. Long distance;
v. Cellular; and
vi. International calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work with the CDOC to ensure that all calls are limited to calls authorized by CDOC policies and regulations – this will include Prepaid collect; Normal collect; Local, Long distance; Cellular; and International calls.

H. At no time, will the offender telephones be unrestricted due to the deactivation of the ITS ID feature. The authorized CDOC staff will have the ability to immediately deactivate any offender's telephone account, upon approval of the authorized CDOC staff for any of the following reasons:

i. 48-hours prior to any transfer;
ii. 48-hours prior to any outside medical appointment; or
iii. 48-hours prior to any outside court appointment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus On/Off Station Control provides CDOC with the ability to disable phone use at any time of day through manual intervention or preset calling schedules.

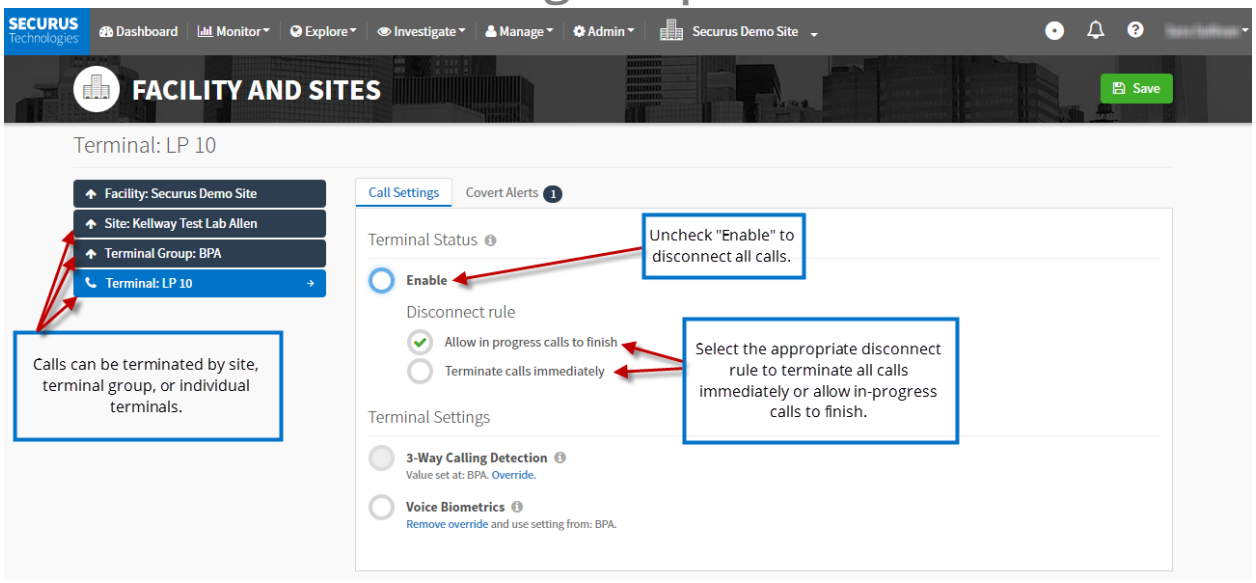
On/Off Station Control

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides complete flexibility to disable telephone use at any time of day through manual intervention or preset calling schedules.

NextGen SCP allows authorized users to disable a telephone, group of telephones, or all facility phones using any personal computer or mobile device with access to the Internet. This capability is available anytime, from anywhere, 24x7x365.

This function allows authorized users to disconnect all calls immediately or allow current calls to finish while not allowing any new calls.

Disabling Telephones



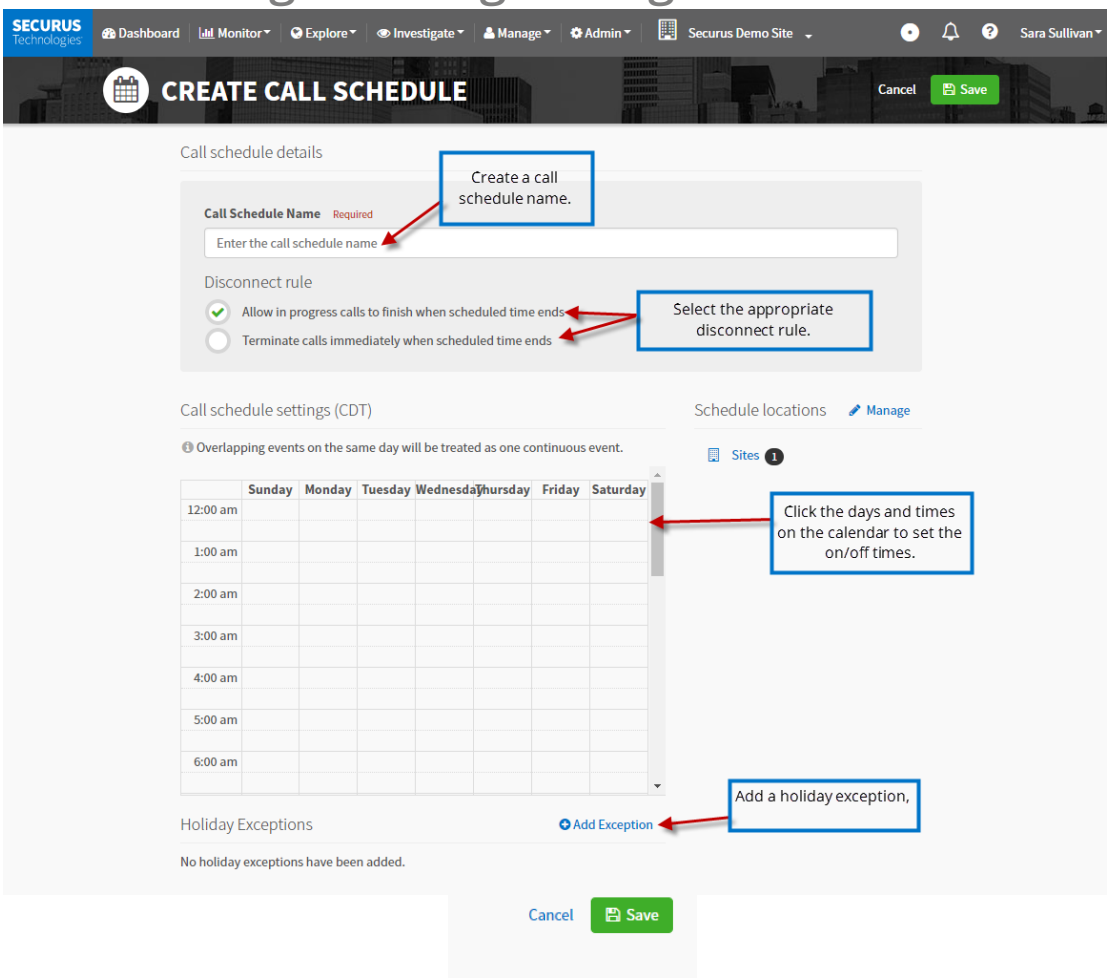
Programmable Calling Schedules

The NextGen Secure Communications Platform™ (NextGen SCP™) calling services has an automated calling schedules feature that allows the system to enforce the scheduling policies of the facility without staff intervention. Calling schedules are used to turn on and off the phones during designated times throughout the day or night.

Calling schedules are flexible and configurable allowing the facility to have multiple on and off times during the day, within a week and by day of the week and then be applied to individual telephones, groups of telephones, individual offenders and/or globally.

Also, holiday overrides can be preset to accommodate anticipated exceptions to the set schedule.

Programming Calling Schedules



Programmable calling schedules are responsive to and overridden by both the manual cut-off switches located within the facility and the Call Settings Disconnect Rule.

I. The ITS will provide for authorized CDOC staff access for the purposes of managing ITS access information in real time. Authorized CDOC staff and Offeror staff, as authorized by the CDOC, will have the ability to immediately enter, delete, change, or modify any ITS

access information including, but not limited to, calling privileges or restrictions pertaining to offenders.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All authorized CDOC personnel will have the ability to immediately enter, delete, change, or modify any ITS access information including, but not limited to, calling privileges or restrictions pertaining to offenders.

J. The ITS will provide capability for assigning an offender telephone access to an individual telephone or group of telephones so that the offender's account may only place calls from those designated telephones. These telephones will still be capable of being used by an offender whose telephone access is not specifically assigned to an individual telephone.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

K. Should there be power outage issues, the ITS and UPS will maintain all currently ongoing telephone calls for up to five (5) minutes while blocking any additional call attempts after the event. A telephone message will alert offenders that they have two (2) minutes remaining on their call. After five (5) minutes, if the UPS has not alerted the ITS that commercial power has been restored, the ITS will power down to a quiescent state that allows it to resume full operation automatically after commercial power is restored. Upon restoration of power and system recovery, the ITS will wait for five (5) minutes of stable power before allowing offenders' calls to resume.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Uninterruptible Power Supply – Facility Backup

All UPS equipment provides power conditioning and an additional layer of surge protection. The rack-mount UPS is a high-density backup-power protection solution ideal for servers, storage systems, network equipment, and other critical devices. It also offers the best UPS power protection against five of the nine most common power-quality problems. The slim design and wide range of UPS system installation possibilities make this the most versatile UPS power quality solution available.

Additionally, Securus provides offsite data storage at multiple locations to minimize risks related to localized disasters, power outages, or security breaches. Securus operates and maintains two geographically diverse and fault tolerant carrier class data centers where data is securely stored offsite. Each data center also has an uninterruptible power supply (UPS), and a generator to provide maximum network uptime.

Uninterruptible Power Supply – Data Center Backup

Power distribution units (PDUs) distribute power to individual customer racks via remote power panels. Each rack has redundant power strips (A & B) routed to diverse PDUs. Diverse uninterruptible power supply systems feed each power distribution unit.

The UPS systems in our primary data center have 2N redundancy. Dual source power runs through a static bypass switch. Battery rooms support the UPS systems with gel cell battery banks. Fifteen minutes of battery backup is available at full load (such as 90 watts per square foot). Each battery bank is continuously monitored to ensure optimal operation. Upon loss of commercial power for more than 15 seconds, paralleling switchgear automatically powers all nine generators; generators are shed to cover load as needed. Typically, the transition from UPS to generator power takes 60 seconds.

Securus Data Centers each have multiple diesel generators onsite with fuel storage tanks that hold 70,000 gallons onsite. Our generators are tested weekly and provide alerts if there is a test failure. Securus maintains multiple fuel vendor agreements to have flexibility and options for fuel purchases.

18. REGULATORY EXPECTATIONS

A. The Offeror will adhere to any and all municipal, State or Federal expectations for the Inmate Telephone System (ITS) and managed access, installation, certification, training or registration throughout the duration of the Contract. Should violation of codes, laws, statutes or ordinances occur relating to the ITS, the selected Offeror will correct the situation at no cost to the CDOC, including payment of any fines or penalties associated with the violation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will adhere to any and all municipal, State or Federal expectations for the Offender Telephone System (ITS) and managed access, installation, certification, training or registration throughout the duration of the Contract. Should violation of codes, laws, statutes or ordinances occur relating to the ITS, the selected Offeror will correct the situation at no cost to the CDOC, including payment of any fines or penalties associated with the violation.

B. The Offeror will be responsible for compliance with all regulatory expectations imposed by local, State and Federal regulatory agencies for all services provided throughout the duration of the Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will be responsible for compliance with all regulatory expectations imposed by local, State and Federal regulatory agencies for all services provided throughout the duration of the Contract.

C. The Offeror will be responsible for making all modifications necessary to allow offenders to place calls in compliance with any industry dialing requirement change(s) at no cost to the CDOC to ensure proper use of the ITS by offenders and authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will be responsible for making all modifications necessary to allow offenders to place calls in compliance with any industry dialing requirement change(s) at no cost to the CDOC to ensure proper use of the ITS by offenders and authorized CDOC staff.

D. The Offeror will keep all call processing and call rating information current and made available upon request by authorized CDOC staff. This information will include, but not be limited to:

i. Local exchanges;
ii. Area codes;
iii. Country codes; and

iv. Any other information necessary to accurately process and rate calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will keep all call processing and call rating information current and made available upon request by authorized CDOC staff. This information will include, but not be limited to:

i. Local exchanges;

ii. Area codes;

iii. Country codes; and

iv. Any other information necessary to accurately process and rate calls.

E. The Offeror will ensure the ITS provides telephone reception quality equal to the highest level of quality offered to the general public and will meet all industry standards for service quality as defined by the CDOC. The Offeror will accept the authorized CDOC staff's decision regarding determination of quality.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will ensure the ITS provides telephone reception quality equal to the highest level of quality offered to the general public and will meet all industry standards for service quality as defined by the CDOC. The Offeror will accept the authorized CDOC staff's decision regarding determination of quality.

19. NETWORK AND INFRASTRUCTURE EXPECTATIONS

A. The Offeror will provide an ITS that includes a role-based monitoring component that is capable of being accessed through an authorized CDOC staff log-in. The ITS will be capable of monitoring calls via secure, password protected internet access.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen Secure Communications Platform™ (NextGen SCP™) allows authorized users to live monitor calls in progress via a browser or any Internet-connected device. The feature provides users selectable scanning of all live calls in progress, thus allowing investigators to be able to monitor only those calls of particular interest.

The feature's integrated media player has a time-shifting capability allowing the investigator to pause, rewind, and replay calls even as the recording continues. The investigator can replay any part of the conversation even after the call has ended.

NextGen SCP also allows authorized users to forward a call to an investigator and quickly identify calling patterns for the dialed number or phone in use.

Authorized CDOC staff can access the system from any internet-enabled system with proper login password authorization.

B. In addition, the ITS will interface with all digital network services provided by local exchange carriers (LEC) as well as interexchange carriers. The Offerors response will provide the types of network services to which the ITS will interface and the purpose (use of a specific application) of such services for the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. The Offeror will use WPA-PSK encryption to secure access to networks and firewalls to bolster security measures.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus takes the security and access to our software/application very seriously and hence have implemented one of the strongest controls in the industry. Securus access controls for all systems are audited for compliancy with the following accreditations/certification:

- SSAE16; (SOC1, SAS70): Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
- SOX: The Sarbanes–Oxley Act of 2002, is a United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms.

Encryption & Security Standards

Protecting your data: Securus developed a strong corporate Information Security Governance and Cyber-Security framework using the NIST guidelines, including 800.53 current version. Applications transmitting data across public networks support TLS 1.2 with AES-256 bit encryption. Sensitive data is encrypted both at rest and in motion. Securus provides support for TLS encryption at the application network layer. All web sessions and services are conducted via HTTPS using AES 256-bit encryption. Securus uses a gold-class vendor-provided certificate service for external and internal SSL connections.

The NextGen SCP user interface encrypts and decrypts user page requests, as well as the pages that are returned by the web server. Access to Securus server information is done through HTTPS—HTTP application layering with Transport Layer Security (TLS) as a sub-layer. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks (events where attacker secretly relays, and possibly alters, the communication between two parties who believe they are directly communicating with each other).

CJIS-compliant access: Securus uses an industry-recognized leader to provide remote access to Securus systems within state networks. This remote access system provides secure, encrypted, CJIS-compliant access to Securus systems. Securus also uses a state-of-the-art Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor and protect our network boundaries. Securus infrastructure servers and all workstations require anti-virus protection and receive regularly scheduled security patches and updates

For your team, NextGen SCP can enforce strong password policies for individual with minimum password length, 30-/60-/90-day password expirations, case sensitivity requiring upper- and lower-case letters, and special characters (@, #, $, etc.).

D. The Offeror will use Cat6 Ethernet cabling to dedicated ports on an Ethernet switch that is connected to a dedicated Local Area Network (LAN). All devices should feedback to a central router and firewall located within the facility.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

E. The Offeror will routinely conduct extensive vulnerability assessments of installed networks and firmware. Offeror will ensure that the system architecture is scalable and designed to easily accommodate changes (future applications, etc.) resulting from CDOC rules and workflows.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

F. The CDOC requires the Offeror to provide reliable high-speed fiber optic cabling at each facility, at no cost to the CDOC. The fiber optic network will be used for offender phone calls and wireless tablet services including but not limited to music downloads, secured messaging, commissary ordering, offender scheduling, banking, e-books, learning and training.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. All cabling including copper and fiber is expected to comply with the State's structured cabling standards. TS-INF-005: Structured Cabling

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

H. The Offeror will provide a sufficient infrastructure to allow offenders to utilize all the available communication solutions at the same time. Offeror to offer an alternative solution to reduce stress on the CDOC network or provide a solution separate from the CDOC network infrastructure.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

20. SOFTWARE EXPECTATIONS

A. The Offeror will provide all software required to support the ITS. At the time of installation and throughout the duration of the Contract, including any renewals, all software will be the current production and considered to be state-of-the-art including software for all equipment and monitoring terminals utilized in service delivery. The CDOC will not be responsible for any licensing costs throughout the duration of the Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

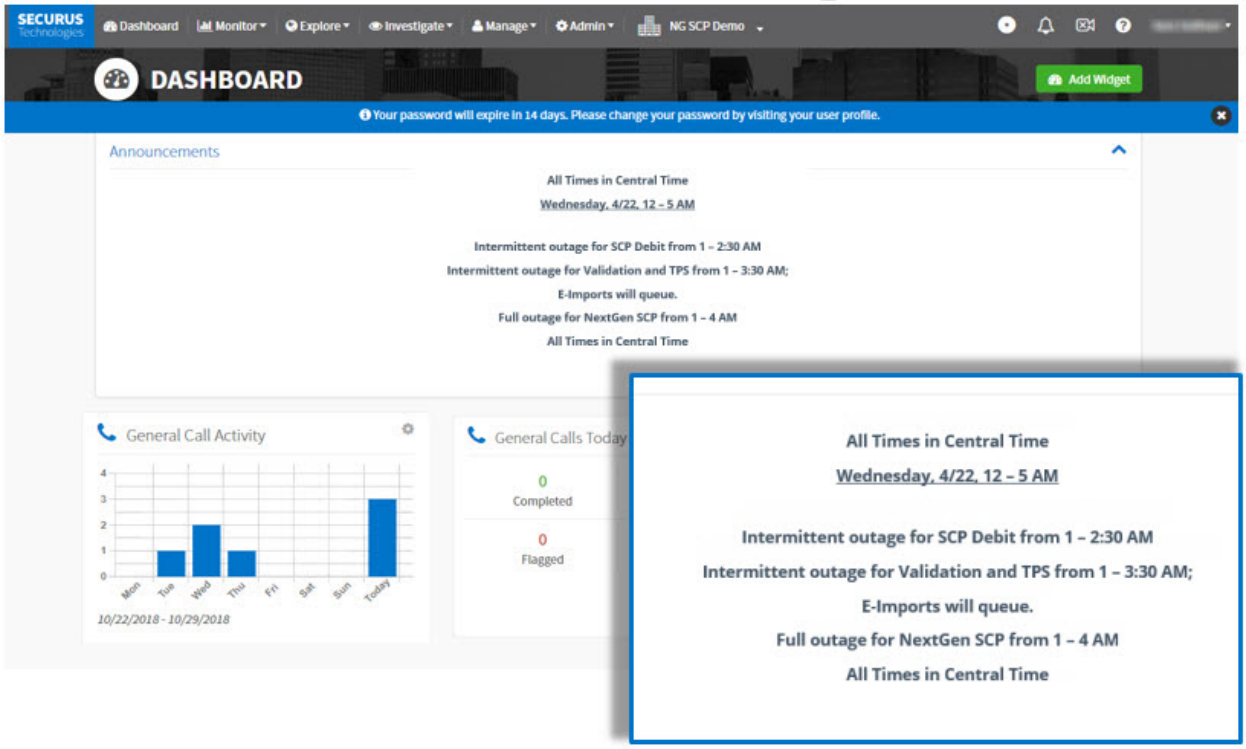
Securus will provide all software required to support the ITS. At the time of installation and throughout the duration of the Contract, including any renewals, all software will be the current production and considered to be state-of-the-art including software for all equipment and monitoring terminals utilized in service delivery. The CDOC will not be responsible for any licensing costs throughout the duration of the Contract.

Software Upgrades

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCP™ software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



B. The Offeror will provide all software required to support the ITS. At the time of installation and throughout the duration of the Contract, including any renewals, all software will be the current production and considered to be state-of-the-art including software for all equipment and monitoring terminals utilized in service delivery. The CDOC will not be responsible for any licensing costs throughout the duration of the Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. Offeror is expected to ensure that the operating system is no more than (N+2) revisions behind the publicly available kernel.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With NextGen SCP's centralized architecture, all customers will have the same version of the most current operating system.

D. The Offeror software installed on the CDOC computers/servers is expected to operate in the then-current CDOC hardware, software and security configuration. Offeror

is responsible for maintaining capability as the CDOC configuration changes, at no cost to CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Because the NextGen SCP system is Web-based, accessible through an internet browser such as Chrome, it is not necessary to install any software on the CDOC computers or servers

E. The CDOC prefers Web based tools with no software installation expectations which are compatible with current versions of Google Chrome. Please describe all Offeror software proposed to be installed on CDOC computers and/or used by authorized CDOC staff. Provide software product name, functional description, usage, and installation/configuration expectations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With the NextGen SCP's anytime/anywhere Web-based access, software installation is not necessary to access the NextGen SCP system. To access the NextGen SCP interface, users open a Chrome™ browser and enter the URL: https://ngscp.securustech.net/login and enter a valid username and password.

Securus has developed a strong corporate Information Security Governance and Cyber-Security framework using the NIST guidelines, including 800.53 current version. Applications transmitting data across public networks support TLS 1.2 with AES-256 bit encryption.

Securus uses a state-of-the-art Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor and protect our network boundaries.

Securus infrastructure servers and all workstations require anti-virus protection and receive regularly scheduled security patches and updates.

F. The Offeror will provide all required/new software enhancements/upgrades to the ITS inclusive of service delivery for the ITS and at no cost to the CDOC. Beta and Field-Tested Software will not be provided unless specifically discussed with and approved by the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide production-ready software enhancements and upgrades three to four times per year.

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Patches

System patch management: After system deployment, Securus uses the Patch Management Program to ensure that systems are updated with the latest patches.

Software Development

The Securus use of information technology (IT) best practices, industry standard quality measurement tools, and strict environmental controls ensure the highest system functionality and availability. The Securus development team uses the Waterfall Software Development Lifecycle (SDLC) to ensure high-quality deliverables. The feature/functionality enhancements process stages are:

- Analysis
- Design
- Development
- Quality Assurance
- Implementation
- Post Implementation Support

Each phase has specific deliverables and gates (controls) to ensure high quality and to minimize rework. During the lifecycle phases, software changes include an accompanying change control document that identifies, at a minimum:

- Version number
- Description of the change
- How the change was initiated
- Person or customer requesting the change
- Person responsible for the change
- Date and time of the change

Securus uses the following distinct system environments in conjunction with our SDLC:

- Development – Used by IT Development to create and unit test new enhancements
- Quality Assurance – Used by Quality Assurance Analysts to test and certify new enhancements and bug fixes

- Pre-Production – Used by Production Support to validate hot fixes for production, and for final validation and mock deployment of major functionality releases
- Production – Used by all Securus customers and accessible by only Securus Production Support and Tech Support

Each environment has access controls, and we use source code control systems to ensure the proper promotion of code and as a document repository.

Securus uses industry-standard HP Quality Center for defect tracking and follows a rigorous test cycle including:

- Verification of New Functionality – Ensures a feature is working as designed
- Load Testing – Determines the upper threshold or breaking point of the component or feature
- Performance Testing – Determines the expected user experience
- Regression Testing – Ensure all existing functionality still works as designed
- Exception Testing – Tests boundary conditions and unexpected usage scenarios

New releases typically create new functionality. Upon completion of the Quality Assurance stage, the code changes are packaged and deployed into our pre-production environment for the final end-to-end quality check, and to optimize the implementation. This effort enables Securus to minimize the maintenance window related to system changes.

Both IT and business stakeholders review and must approve all scheduled changes to production in two change control meetings to safeguard the stability of the production environment.

Upon implementation of new code into production, Securus Production Support and IT Development monitor changes closely to minimize the impact of any adverse or unexpected system behavior.

This attention to detail allows Securus to build feature functionality that leads the industry in quality and performance.

Our quality control does not end with our system design but continues all the way through system upgrades and training.

Our notification of changes is provided in the form of a splash screen upon log-in to the NextGen SCP user interface, or through an official Release Notes document. The Release Notes provides the following details:

- Version number, if applicable
- Description of the change, including whether it is a minor update or a major update
- Contact information for additional information or training
- Date and time of the change

G. All upgrades, bug fixes, enhancements to the software and/or hardware will receive prior approval by the authorized CDOC staff. If requested by the authorized CDOC staff, the Offeror will provide a test environment to allow the authorized CDOC staff to verify the upgrade, fix and/or enhancement is compatible with the current operating environment.

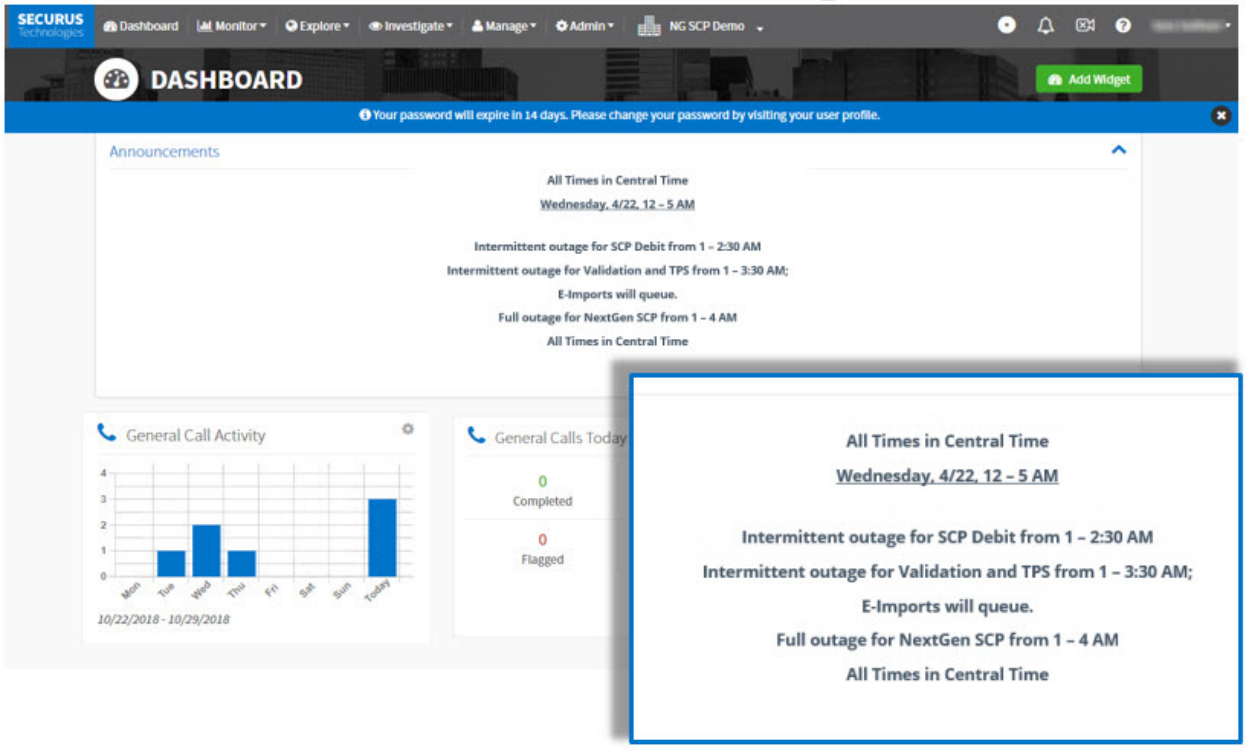
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

System updates, bug fixes, enhancements, patches and workarounds are executed as described below.

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCP™ software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



Securus will provide production-ready software enhancements and upgrades three to four times per year.

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Patches

System patch management: After system deployment, Securus uses the Patch Management Program to ensure that systems are updated with the latest patches.

Software Development

The Securus use of information technology (IT) best practices, industry standard quality measurement tools, and strict environmental controls ensure the highest system functionality and availability. The Securus development team uses the Waterfall Software Development Lifecycle (SDLC) to ensure high-quality deliverables. The feature/functionality enhancements process stages are:

- Analysis
- Design
- Development
- Quality Assurance
- Implementation
- Post Implementation Support

Each phase has specific deliverables and gates (controls) to ensure high quality and to minimize rework. During the lifecycle phases, software changes include an accompanying change control document that identifies, at a minimum:

- Version number
- Description of the change
- How the change was initiated
- Person or customer requesting the change
- Person responsible for the change
- Date and time of the change

Securus uses the following distinct system environments in conjunction with our SDLC:

- Development – Used by IT Development to create and unit test new enhancements
- Quality Assurance – Used by Quality Assurance Analysts to test and certify new enhancements and bug fixes
- Pre-Production – Used by Production Support to validate hot fixes for production, and for final validation and mock deployment of major functionality releases
- Production – Used by all Securus customers and accessible by only Securus Production Support and Tech Support

Each environment has access controls, and we use source code control systems to ensure the proper promotion of code and as a document repository.

Securus uses industry-standard HP Quality Center for defect tracking and follows a rigorous test cycle including:

- Verification of New Functionality – Ensures a feature is working as designed
- Load Testing – Determines the upper threshold or breaking point of the component or feature

- Performance Testing – Determines the expected user experience
- Regression Testing – Ensure all existing functionality still works as designed
- Exception Testing – Tests boundary conditions and unexpected usage scenarios

New releases typically create new functionality. Upon completion of the Quality Assurance stage, the code changes are packaged and deployed into our pre-production environment for the final end-to-end quality check, and to optimize the implementation. This effort enables Securus to minimize the maintenance window related to system changes.

Both IT and business stakeholders review and must approve all scheduled changes to production in two change control meetings to safeguard the stability of the production environment.

Upon implementation of new code into production, Securus Production Support and IT Development monitor changes closely to minimize the impact of any adverse or unexpected system behavior.

This attention to detail allows Securus to build feature functionality that leads the industry in quality and performance.

Our quality control does not end with our system design but continues all the way through system upgrades and training.

Securus provides software updates three-to-four times per year. With each new software update, we will provide advance notice to the CDOC. This notification is provided in the form of a splash screen upon log-in to the NextGen SCP user interface, or through an official Release Notes document. The Release Notes provides the following details:

- Version number, if applicable
- Description of the change, including whether it is a minor update or a major update
- Contact information for additional information or training
- Date and time of the change

Pilot sites

Securus uses customer sites as pilot sites to test-in and verify updates and upgrades in a customer environment to verify field adoption of the changes.

H. The ITS will provide offenders the ability to obtain account balances for telephone time and available offenders' bank account funds at no cost to the offender. If Offeror software does not have this capability, the awarded Offeror will write an interface to accommodate CDOC's needs.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Commissary account balances are provided by the commissary provider, who is tied into the agency trust/banking and they would provide the current balance of funds. As such, the display of that would be provided by the commissary provider. Securus' integration allows the offender to see information provided by the commissary.

I. The Offeror is responsible for resolving any problems identified by the authorized CDOC staff within 24 hours and at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is responsible for resolving any problems identified and reported. When a facility calls Securus, an event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a prescribed resolution timeline and escalation procedure. In all cases, Technical Support will respond to the customer within the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects 30 percent or more of system functionality. Examples of P1 service assignments include:

- Voice prompts not operating
- Features are not operating appropriately
- CD-burning abilities disabled
- Live call monitoring is not operating appropriately
- SCP access denied
- All phones out-of-service

The response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

A P1 events escalate to:

- Technical Support Department

- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If the problem resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment—our mid-level priority assignment—occurs when a system event adversely affects 5 to 29 percent of system functionality. Examples of a P2 service assignment include problems or errors with related to:

- Workstation
- Specific system ports
- Local Exchange Carrier (LEC) circuits
- Unblocks
- Blocked numbers
- Missing call detail records (CDRs)
- Call searching

The response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P2 events escalate to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment—our lowest priority assignment—occurs when a system event adversely affects 5 percent or less of system functionality. System events adversely affecting some of available facility phones. Examples of P3 service assignments include:

- Static on the phone
- A party's inability to hear
- An offender's inability to dial

- A broken phone
- Non-functioning dial pad
- Non-functioning cutoff switches
- An inability to generate reports

The response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P3 events escalate to the Technical Support Department.

Escalations

If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

The supervisory escalation chain is:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- VP Service and Technical Operations

21. DATABASE EXPECTATIONS

A. The Offeror will provide a data record of all transactions through the ITS. The data record will be maintained in a database for monitoring and analysis of offender telephone calls. The data record is used to alert authorized CDOC staff of possible trends with offender calls that could jeopardize the security of offenders, staff, or facilities.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus uses Oracle for its database file structure. Oracle Database delivers economies of scale on easily managed grids, making it easier to:

- Reduce downtime with maximum availability
- Partition and compress data to run queries faster
- Securely protect and audit data, and enable total recall of data
- Make productive use of standby resources

Oracle simplifies the process of linking data in multiple tables. This is a key feature of a relational database management system or RDBMS. Storing data in multiple tables enables Securus to define relationships between the tables, as well as the applications that feed information to those tables.

Oracle allows NextGen SCP to link the call data to multiple tables and also maintains consistency between them, ensuring that the data among related tables is correctly matched to maintain referential integrity. Oracle supports all standard relational data types, as well as native storage of XML, Text, Documents, Images, Audio, Video and Location data. Access to data is via standard interfaces such as SQL, JDBC, SQLJ, ODBC, .NET, OLE, .NET, and ODP .NET, SQL/XML and Xquery and WebDAV.

Securus can use the Oracle database to respond faster to changing business conditions, providing clients a system that is more responsive to their evolving needs.

Data Reports

Authorized CDOC staff can generate reports to spot trends through the NextGen SCP user interface. NextGen SCP™ retains communication detail records on all communication attempts and events. Authorized users can quickly run reports to spot calling trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

CDOC users can customize reports by changing search criteria such as date, time, offender identifier, dialed number (calls), visitor contact number (video visitation), destination, termination reason, and much more.

The following steps show the ease of producing valuable, customized reports:

1. Verify that the correct “Facility” and “Site” levels are selected or make changes as necessary. (This setting allows you to select the facilities, sites, phone groups, or phones you want to search.)
2. Click the **Explore** menu.
3. Select **Communication Records**. Also, CDOC users can select **Offender Activity**, **Covert Alerts**, **System Logs**, or **PAN Frequency** to generate reports within these categories.
4. Select the search criteria for a simple (dynamic) search or click the **Advanced Search** link to perform a more detailed search based on additional criteria.
6. Enter your search criteria in the appropriate fields and click **Search**.

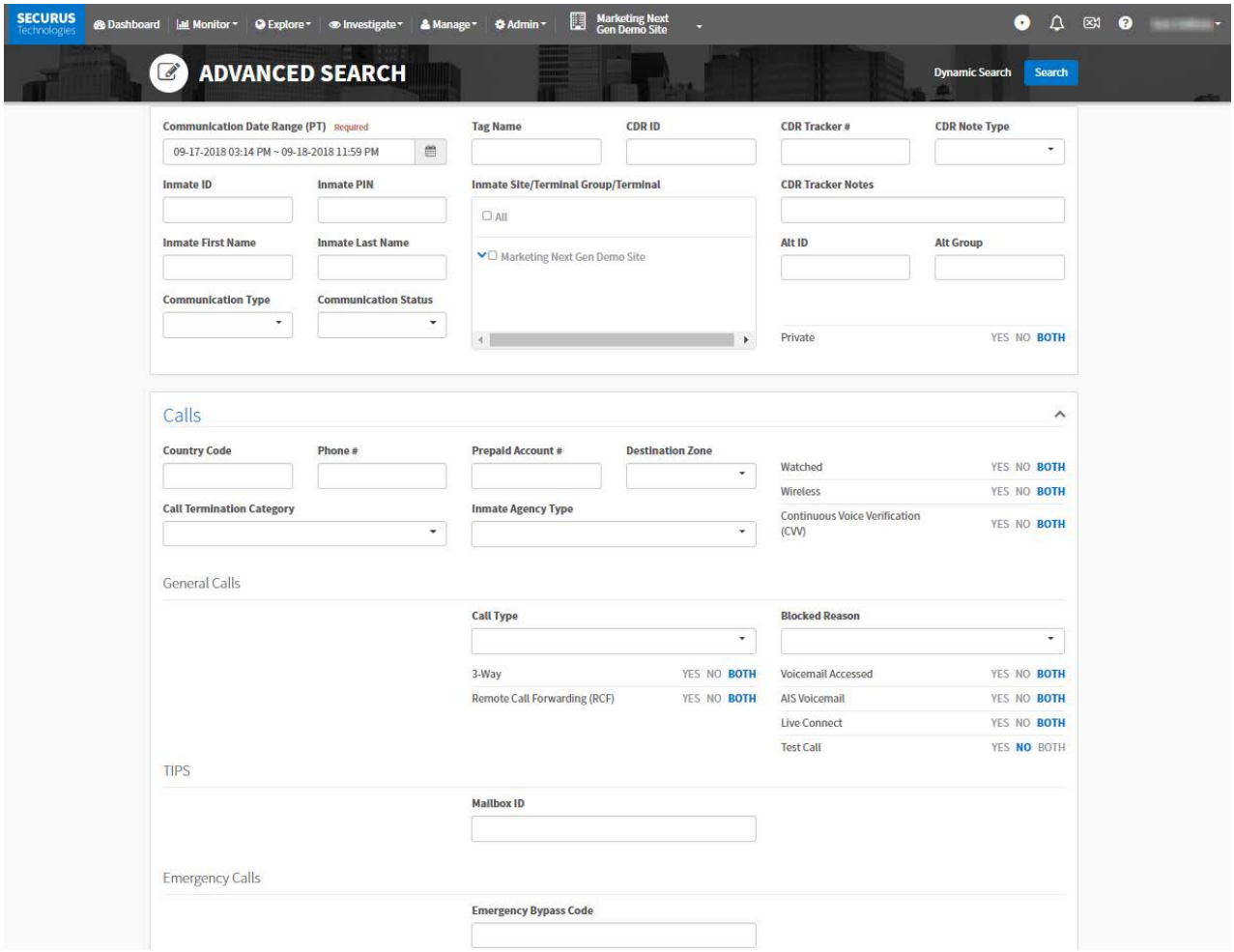
The records matching the search criteria appear. With a single click, the data can be exported to Excel, CSV (Comma Separated Values), or Adobe PDF format.

Authorized CDOC users can sort the results within the NextGen SCP user interface on the following criteria, while exporting a result to Excel allows the user to sort the results based on any of the communication event details.

- Offender Name (IS)
- Other Party
- Start Date/Time
- Duration

The resulting report can easily be saved, printed out, or emailed to others.

Advanced Search, Calls Section



Inmate Inter-Communication Evaluation and Reporting system (ICER™) Overview

ICER™—Uncovering Intra-and Inter-Facility Offender-to-Offender Telephone Communications

Offender-to-Offender communication is a long-standing problem of which the frequency and severity has been nearly impossible to determine. Correctional facilities understand this problem, but have no means to solve it. Others believe the problem doesn't even exist. The reality is: **offender-to-offender communication is real, happening all over the country, and can now be identified**.

Every day, we learn about instances of major crimes being solved because of the increasingly cooperative efforts among state and federal agencies that are beginning to share case-critical data around the United States. In the world of offender phone calls, we offer cutting-edge technology based on state-of-the-art, patent-pending, call-matching technology that identifies Offender to Offender communications even when it's between two different correctional facilities across the country.

Although illegal Offender to Offender events are identified in this scenario and details are provided to each agency regarding their leg of the call, the details of the other agency's event, such as names and telephone numbers, remain confidential unless both correctional facilities agree to share such information on an event-by-event basis. This unique information-sharing model ensures data remains secure while also providing enhanced information when needed. Securus serves more than 1,200 correctional facilities around the country where ICER events can be identified, and we have identified ITIC events within all 1,200 facilities.

Offenders are continually finding creative ways to speak to each other using the offender phone system, and ICER listens to and identifies all of these illegal communication events. Whether two offenders are calling an accomplice on the outside who is verbally relaying messages, or the accomplice has two speakerphones to coordinate gang conference calls, ICER identifies all of these scenarios and proactively notifies all authorized corrections staff of the event and provides details that can quickly and easily be traced back to a specific call. This call can then be listened to through Securus' industry-leading platform.

The Threat

Offenders have been and continue to communicate with each other over the telephone systems that have been provided for their controlled contact with the outside world.

Before ICER, Offender to Offender communications were essentially undetectable due to no practical technology or uniform networking capability to identify such communications.

Highlights of the offender-to-offender communication threat include:

- Offenders use a variety of methods to go undetected when communicating with an offender, whether that offender is in a neighboring pod, a separate facility within the same state, or in a different state. Offenders exploit conference bridges, Google Voice™, and other forms of modern telecommunications technology. In addition, they rely on called parties to bridge the calls, place three-way calls, or put two speaker phones in proximity to one another, so that offenders can talk to other offenders without being detected.

- Until recently, Offender to Offender communication events were only found when accidentally stumbled upon by correctional staff. Events are known to occur with much greater frequency than previously known.
- These illegal communications enable criminal activities to occur, including coordinating gang-related murders, human trafficking, drug trafficking, racketeering, and offender disturbances at multiple correctional facilities around the country.

How ICER Events Occur

ICER events can occur in any of the following ways:

- Three-way calling
- Manually bridged calls
- Automatic bridges
- Speaker phones
- Relaying messages in real time
- Using Google Voice

Common Element: Called Party Involvement

How ICER Works

ICER uses advanced voice analysis technology to generate a call signature—a representation of the call that does not involve any of the original audio—for each completed offender telephone call. Call signatures are then automatically encrypted and transmitted to the central data center for analysis. Because none of the original audio is used in a call signature, the ICER system is in full compliance with state laws regarding the transmission of call recordings. Under normal operations, call signatures are created, transmitted, and received at the data center for each completed call. Upon arrival, the call signature is immediately analyzed and checked against other call signatures. If an Offender to Offender communications event is detected, it is logged in the ICER system database and investigators from the participating corrections administration are automatically alerted via email to log into the ICER system for the detailed report. To protect certain elements of offender data from being displayed to participating agencies, both parties must provide online consent before details of the full report are made available. The ICER system doesn't require correctional facilities to transmit audio files and each agency is always in complete control of the level of sensitivity of any data transferred.

ICER Event Report

ICER Event Report

Inmate Inter-Communication Event
identified on
March 1, 2022 at
09:31 pm EDT

An Inmate Inter-Communications Event has been detected involving an inmate at your facility. The details of this event follow below.

	Your Facility	The Other Facility
Inmate	Jones Mike	Anderson Sam
Agency	Smith County	Jones County
Site	MRJC	Inverness
Inmate ID	1233455	338412
Called Number	123-456-7890	123-456-7890
Station Name	A31-W	B-34 E
Call ID	8833456	3342235
Call Start Time	**03/01/2022** 07:36 pm	**03/01/2022** 08:27 pm
Time into Recording (H:M:S)	00:12:01	00:02:36
Duration of Event (H:M:S)	00:39:01	00:39:01

Securus' ICER listens to every call to create a uniquely indefinable call signature. It then looks for calls occurring simultaneously or that overlap and using that call signature, identifies if there are any two calls where the same unique call signature is identified. Unlike other vendors, only Securus' ICER™ detects all offender to offender communication between separate facilities, which means you are no longer missing half of all of your offender to offender call traffic.

Spotting Trends

Securus' THREADS platform can help CDOC staff identify trends that could pose a security threat to other offenders, staff, and facilities. Through Securus' data analytics platform— THREADS™—facility data is automatically ingested the moment THREADS is enabled.

Additional external data sources can be imported and analyzed to build an investigation. All of this takes place without purchasing any additional equipment, and it can be managed remotely at any time through an assigned Web-based facility portal. This means that the CDOC can access data remotely from any location that provides Internet access.

THREADS is the most widely used investigative telecommunications platform in the industry today, with more than 1.4 million offenders served, petabytes of aggregated intelligence data, and more than 2 million phone calls processed per day. THREADS' powerful data analytics engine analyzes multiple types of facility data, such as offender communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate focused leads for investigators. THREADS is extremely robust and accurate, but is extremely intuitive, and easy to use —making it a perfect tool for busy investigative officers operating within a correctional institution.

Unlike our competitors' software, which requires users to manually upload facility data, THREADS was developed directly within the corrections market; it automatically uploads facility data and does not require any equipment to reside on-site. The unique algorithms within THREADS were designed by high-profile investigators with more than 50 years of combined experience in communications data and training of other investigative units on how to analyze that data. What used to take an entire day of multiple officers working eight-hour shifts now takes just moments.

THREADS Reports

THREADS provides the following types of reports:

- Statistical
- Linkage
- Working Group
- Correlation
- Time-Based

- Financial

Statistical Reports

Statistical analysis includes basic reports to start your investigation. This includes all occurrences of a phone number or a bounce list of numbers in the database and the most frequently called numbers by an offender or person.

- Identify everywhere a phone number occurs in the database, such as calls, SMS, phonebook, and BNA. This analysis can be run with a bounce list.
- Identify an offender as a potential owner of a device.
- Identify the phone numbers that an offender or person calls with the highest frequency.
- Identify all phone numbers associated with an offender or person including all calls, SMS, emails, and phonebook contacts. A bounce list can be generated from this report.
- Identify all communication details (calls, SMS and emails) between 2 or more targets or groups of targets. This report produces a CSV file for download.

Communication Activity Summary



Linkage Reports

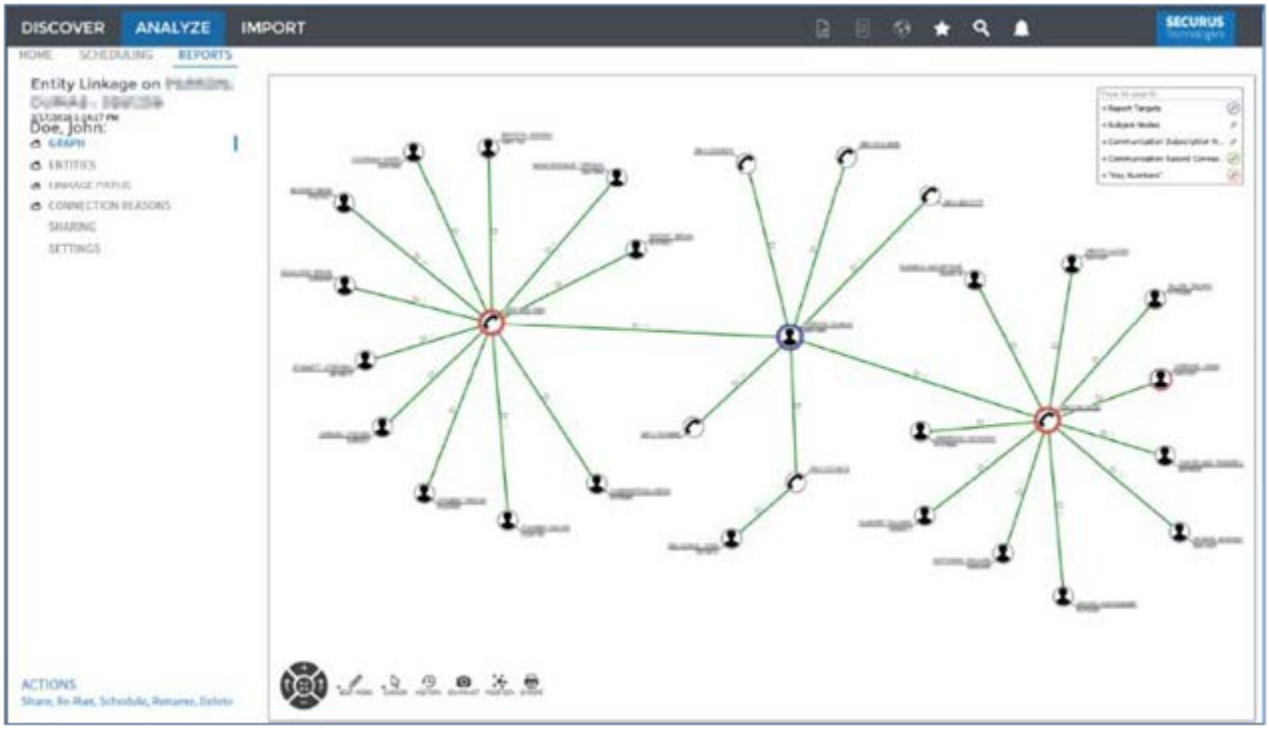
Linkage analysis shows how offenders and people are related. All the reports in this section generate graphical results that let you explore the relationships between your targets.

This visual reporting tool is a quick way to understand who offenders are talking to and how the calls are related to other known numbers or offenders.

Users can generate a linkage chart that identifies:

- A target(s) relationships based on user-selected connection types, such as calls, financials, visitation, etc.
- Connections between two selected targets or two sets of targets based on user-selected connection types, such as calls, financials, visitation, etc.
- Connections between two or more targets based on user-selected connection types, such as calls, financials, visitation, etc.
- Direct relationships between selected targets based solely on phone calls

Linkage Analysis

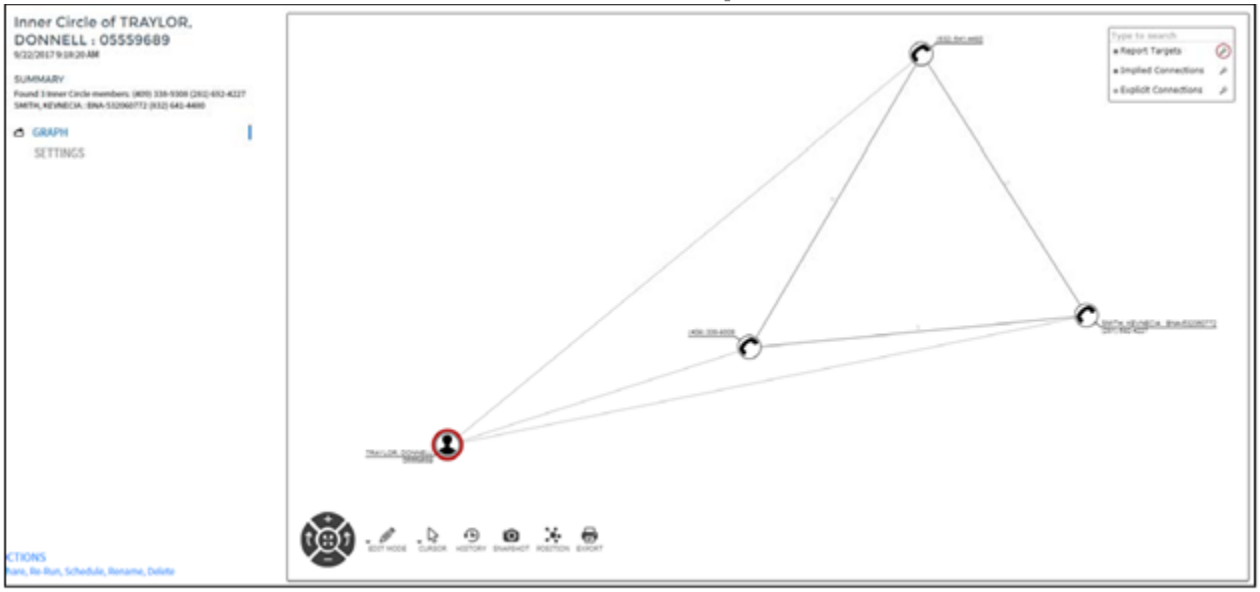


Working Group Reports

Working Group analysis uses a person's communication behavior and calling patterns to identify phone numbers and people of interest. One of the key techniques used is temporal analysis, which associates people based on time between calls. The closer the time between calls, the more likely those calls are related. By leveraging working group reports, facilities can identify gang and other organized activity. Knowing organized groups and gangs can aid staff in monitoring member activity or even taking preventive measures against illicit activities.

- Identify a target's "working group" or inner-circle based on their communication patterns. This report is a graphical linkage chart.
- Display a target's inner circle changes over a predetermined time
- Show communication sequences where a target calls two or more numbers in a pattern
- Identify communication patterns—such as two or more of the same sequence—and when they occurred
- Find a target's chain of calls. A chain is a series of calls triggered by the previous call in the chain. This report requires imported phone calls from outside the facility.
- Identify the most-likely boss in an organization based on chain analysis. This report requires imported phone calls from outside of the facility.

Inner Circle Report



Correlation Reports

Correlation analysis identifies common contacts and phone numbers between offenders, persons, and workspaces. Through correlation reporting, investigators can identify common contacts between offenders as well as fraternization between offenders and facility staff.

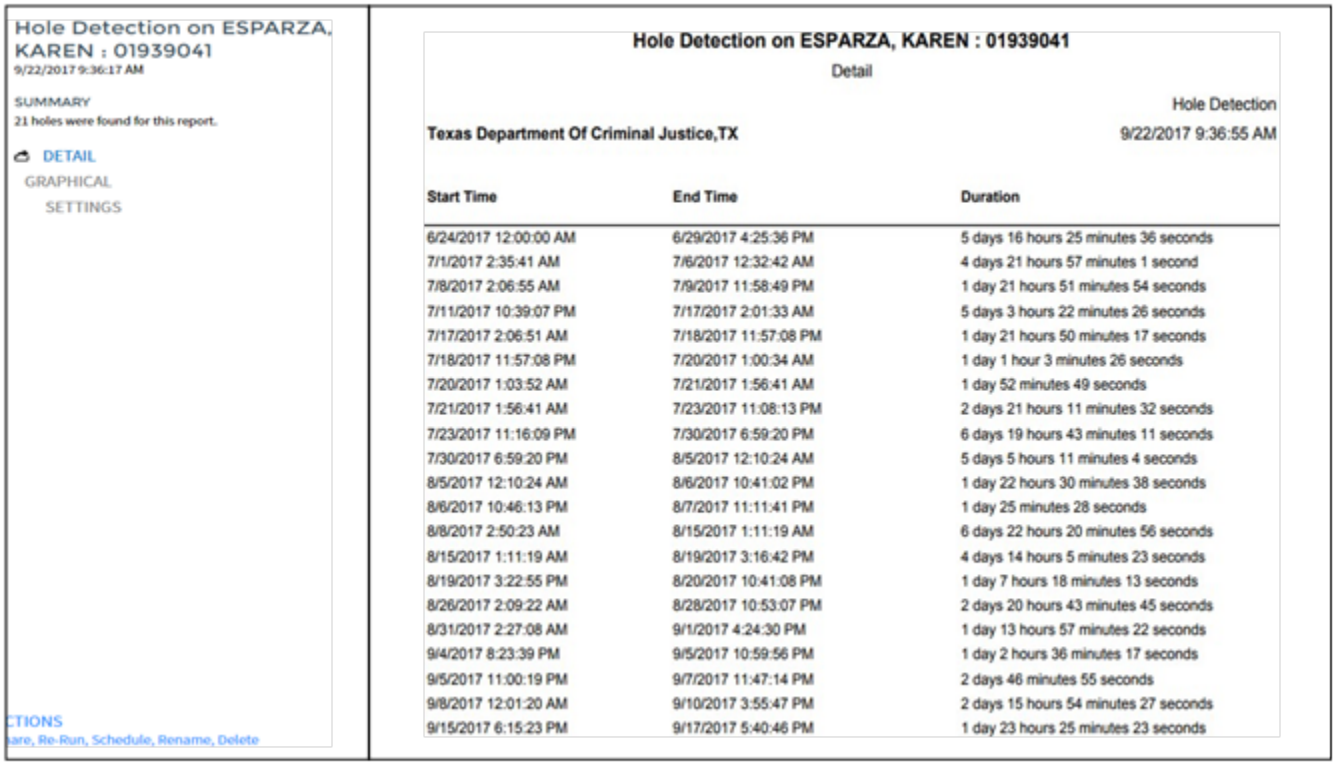
- Find any common communications between offenders, persons, or groups of targets
- Identify potential three-way calls between offenders
- Discover common phone numbers between two workspaces

Time-Based Reports

Time-based analysis provides reports based on the timing and frequency of an offender's or other person's communications. Find out when communication is frequently taking place, then identify periods of time where communication is not taking place. These gaps in communication can indicate behavioral changes as well as cell phone usage.

- Identify holes or gaps in an offender's or person's communication activity
- Display a set of phone numbers that a person called where communications stop with one phone number and starts communication with a different phone number within a close proximity of time. This might indicate a change of phone number or an organizational shift.
- Identify if two or more phones are being used at overlapping times. If there is a significant time overlap, it could indicate that the phones are being used by different people.
- Generate a graphical timeline of any activity—such as communication, association, financial transactions, etc.—that includes a date and time.

Hole Detection Report



Financial Reports

Financial analysis identifies correlations between offenders and people based on the funding of an offender's accounts.

- Identify offender financial accounts with multiple funding sources
- Identify and list financial transactions of interest for a set of targets

Efficient Automated Reports

When key information is gathered, investigators must determine where all of that data will go and then take part in the time-consuming method of analysis. However, THREADS takes it one step further by allowing facilities to set up automated reports. Reports can be scheduled to take place daily, weekly, or monthly. Through this automated reporting process, users receive notifications regarding the data they use at the timeframes they select.

Managed Data Analytics

For facilities interested in using THREADS but requiring additional investigative resources, Securus offers Guarded Exchange to provide this service. Guarded Exchange

is a Securus company run by current and former law enforcement and corrections personnel. With more than 20 years of experience, Guarded Exchange has the resources to run THREADS reporting and analytics, and provide actionable intelligence to the CDOC facility members. Guarded Exchange is here to serve the CDOC, import and filter data, and provide the investigative leads that the State is looking for.

B. The Offeror will be responsible for the generation and creation of a centralized system database. The ITS will provide the capability for every outgoing call to be recorded with a transaction record that includes, at a minimum, a recording of the telephone call on standard media in a Comma Separated Variable (CSV) format or format of authorized CDOC staff's choosing that allows for playback on standard PC, CD drives or industry standard media players.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus stores all communication recordings in centralized, disaster-resistant, carrier-class data centers.

NextGen SCP provides a unique set of features and advanced technologies to store communication recordings. NextGen SCP writes all recorded communication events to a Network Attached Storage array (NAS) in our primary data center. Each NAS array is also replicated to the secondary data center for redundancy and failover. All recordings created on the platform reside in at least two of our data centers and include transaction records.

Recordings can be downloaded from NextGen SCP in various, widely used formats and copied to a CD, DVD, or other portable media.

The NAS architecture makes all storage available to all servers on the network. The NAS solution delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network. The NAS devices can scale by adding another node of dense SATA disk to the storage array. Within the NAS, NextGen SCP uses a software-defined storage platform of very dense disk nodes. Even if three individual hard disk drives fail or one node fails during the disk or node recovery process, the system will continue to operate without data loss.

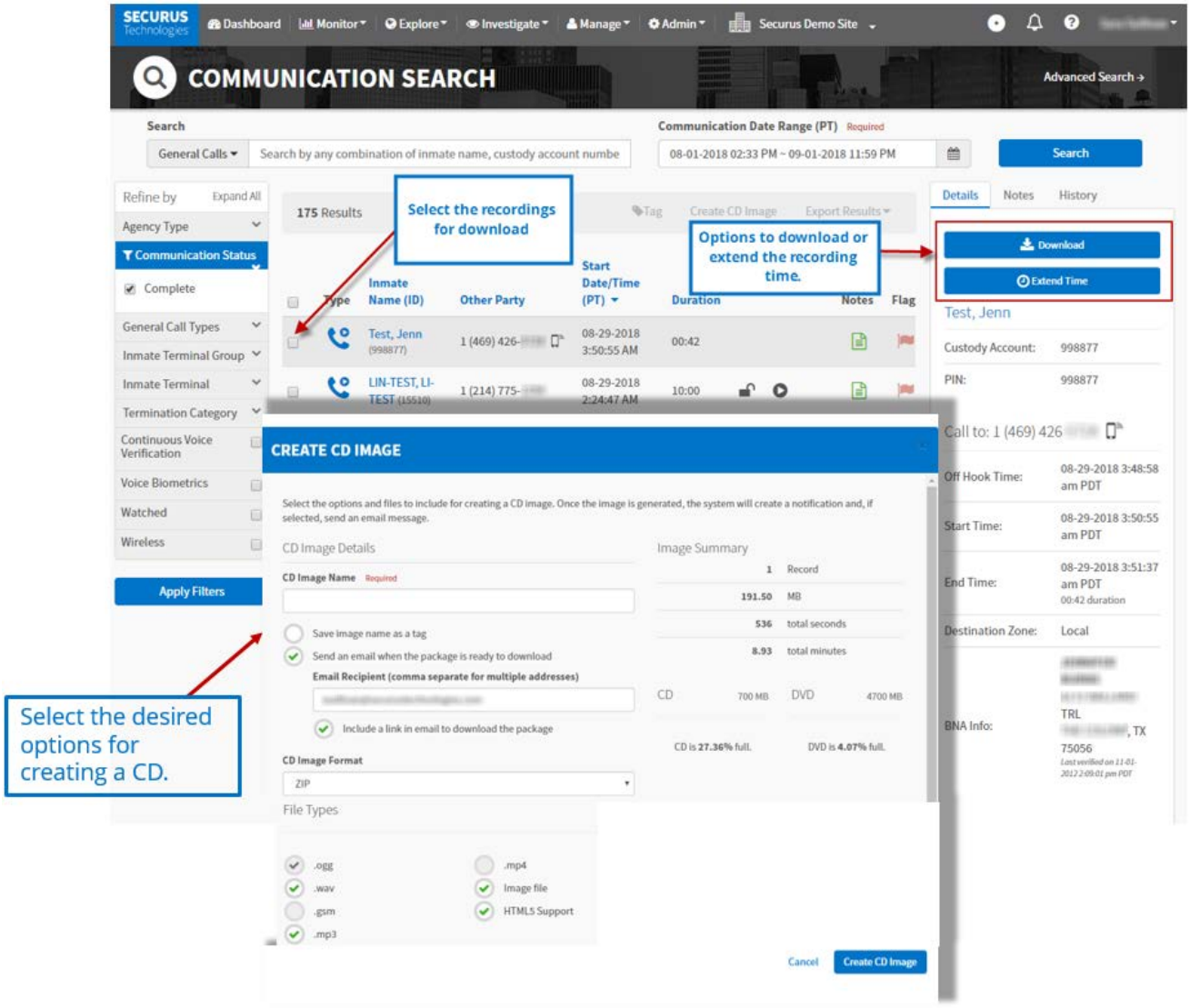
The Securus NAS has more than seven petabytes of storage space in each carrier-class data center and is continuously monitored and managed through automated processes and storage policies. When these very large storage systems approach designated thresholds, Securus expands capacity to ensure all authorized communication records and recordings are retained in secure, disaster-resistant locations.

Downloading Recordings

Tamper-proof, portable recordings for investigative and court purposes: With Securus NextGen SCP, NG SCP users may copy recorded conversations and visitation sessions to an external media device, such as CD, DVD, mp3 player, or USB drive. To maintain the accuracy of data and recordings during downloading and copying, NextGen SCP stores the files—both audio and CDR information—embedded within an industry-standard read-only format that prevents the possibility of tampering.

File type and notification options that fit your needs: When you download communication, a CD image is created, and you can add multiple recordings to an image, select the file type, view file size, and select an email notification when the CD image is ready to download.

Downloading Communication Events to External Media



C. The database will be maintained in such a manner as to allow authorized CDOC staff the capability to review and monitor offender call data regardless of which CDOC facility is housing the offender.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With CDOC approval, authorized staff can review and monitor offender call data from any of the CDOC facilities authorized for that user

D. The database will contain multiple data fields. At a minimum, the database will contain all fields required to generate reports as indicated in Reporting Expectations and all information required to establish Offender Telephone Access as indicated. Final data elements to be collected will be subject to written approval by the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP provides report access on all fields required to generate reports as indicated in Reporting Requirements, and all information required to establish offender Telephone Access, as indicated in Section 4.

E. The ITS will provide the capability for authorized CDOC staff to download reports from the database, through secured internet access, as outlined in Reporting Expectations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Reports can be generated online and exported in:

- Microsoft® Excel
- CSV (Comma Separated Values)
- Adobe® PDF format

NextGen SCP has a report writer that provides investigative information based on the communication detail records. CDOC may search and analyze details on all communication events through NextGen SCP and then run reports to identify communication trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

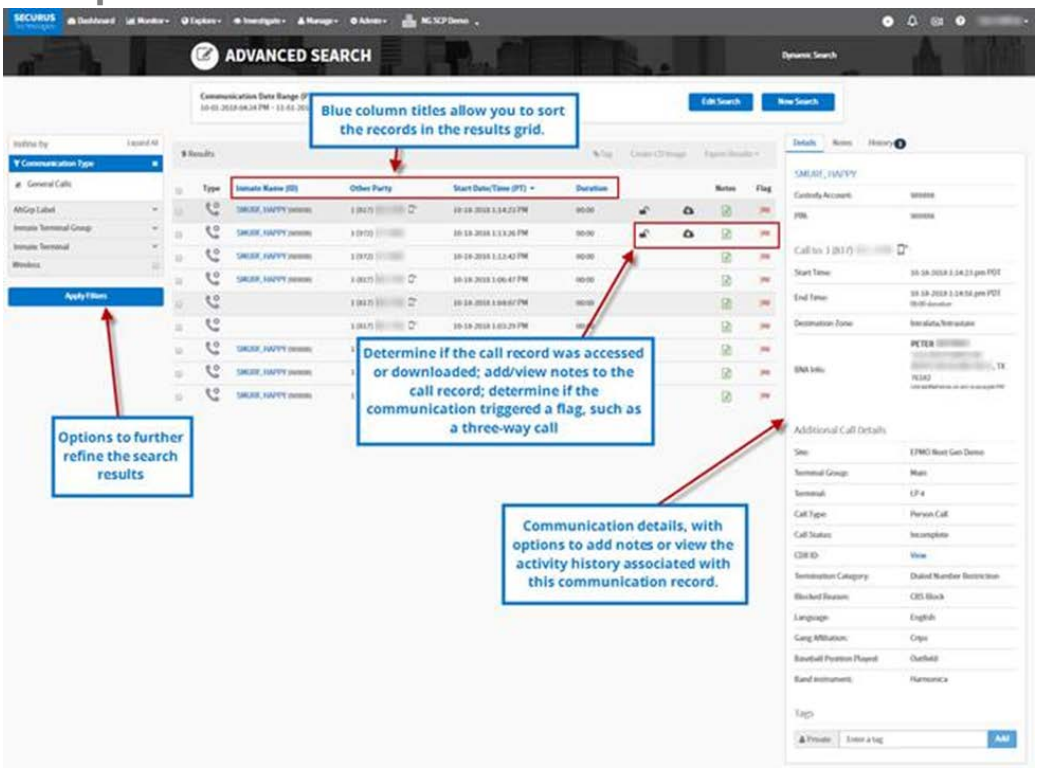
NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on an extensive list of criteria options. CDOC also may create customized reports by changing search criteria. After search results are generated, you can sort based on any of the communication event details.

NextGen SCP™ Report Criteria Fields
▪ Date Range
▪ Identifier (ID, PIN, Name)
▪ Continuous Voice Identification
▪ Communication Type (Calls and Video)
▪ Communication Status (Complete or Incomplete)
▪ Prepaid Account Number
▪ Destination Number (Partial or Full Number Entry)

NextGen SCP™ Report Criteria Fields

- Call Type
- Three-Way or Remote Call Forwarding Detected
- Watched Status
- Wireless Indicator
- Visitor and Visit Type (SVC)
- Visitor Contact Number
- Visitor Identifier (ID, Name, Email)
- Phone or Terminal Location
- Number Restriction and/or Status Assignment
- Broad Search with No Data Entry
- Suspected Fraudulent Call Activity
- Destination Zone (Local, Interlata, Interstate, Intralata, International)

Sample Communication Detail Results Screen



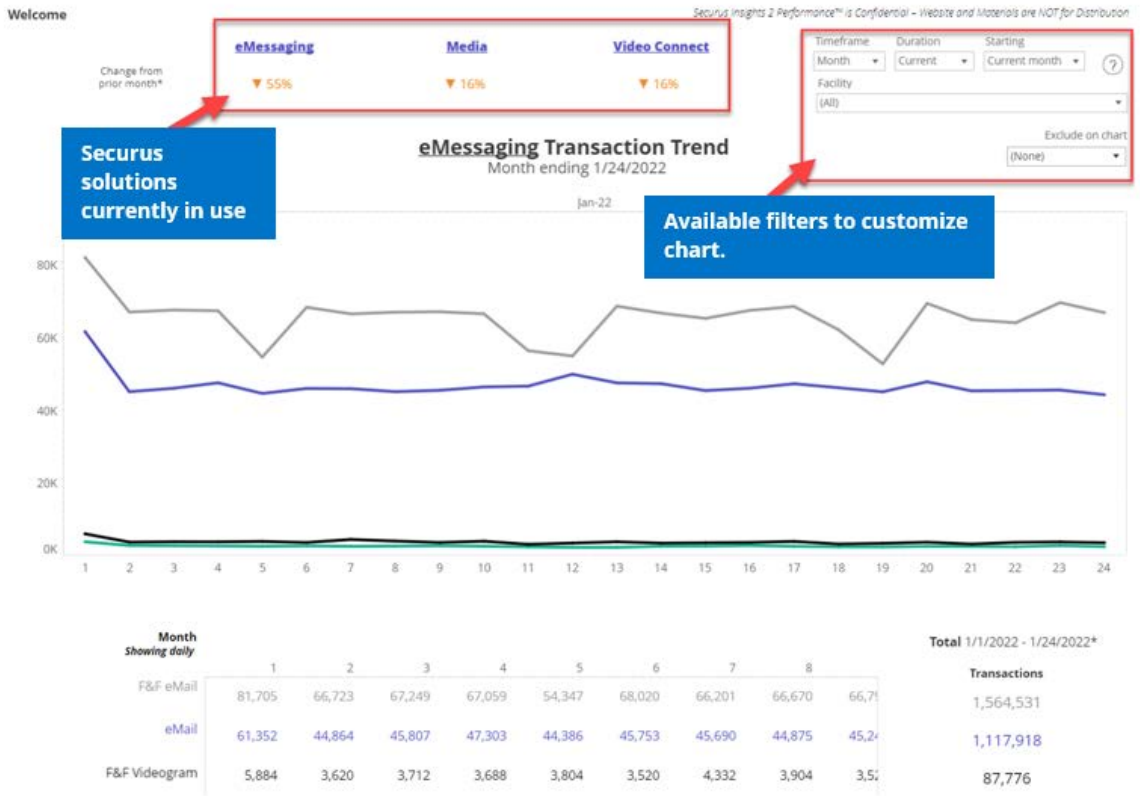
Insights 2 Performance (I2P) Portal

As part of our solution, Securus is also offering our Insight 2 Performance (I2P) portal, developed for our Department of Corrections customers, which allows the agency to see transaction data for communication services in use at the agency and monitor ticket activity for all implemented communication services. This information will allow the CDOC to monitor offender communication activity and trends and service ticket resolution times to help support administrative decisions on access to devices as well as support tracking of our responsiveness to our SLA commitments.

The I2P dashboard information will reflect the solutions your agency utilizes and will provide you product usage metrics that can be viewed for different periods (e.g., 7 days, 30 days, 3 months). Information is displayed in easy-to-understand graphical charts and tables.

Authorized users can easily customize the charts by timeframe, duration, facility, and exclusions on chart by using drop down filters.

Sample I2P Dashboard View



Service Ticket Data

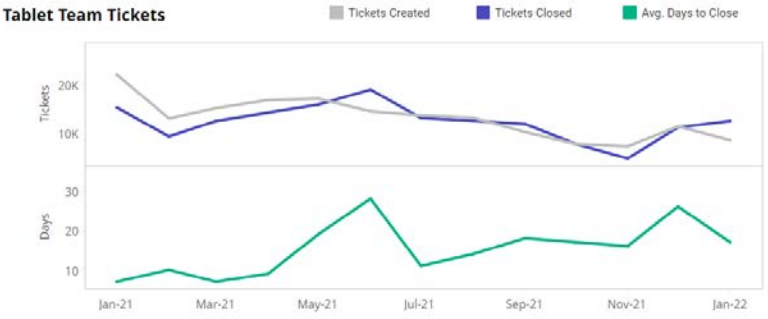
The Service dashboard will reflect both Tablet Tickets initiated by offender and Tech Support Tickets initiated by the facility. Metrics displyed will include the numberof tickets created, tickets closed, and the average number of days it took to close the ticket.

Sample Service Ticket Dashboard for a 1 Year Period

Securus Insights 2 Performance™ is Confidential - Website and Materials are NOT for Distribution

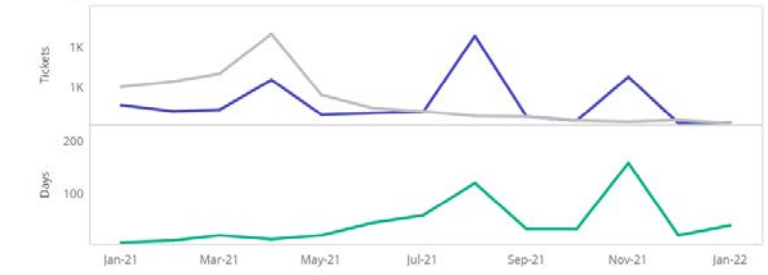
Current Tablet Counts 37,909

Tablet Team Tickets



	Tickets Created	Tickets Closed	Avg. Days to Close
Jan-21	21,905	15,238	7
Feb-21	13,023	9,327	10
Mar-21	15,093	12,476	7
Apr-21	16,748	14,190	9
May-21	17,033	15,836	19
Jun-21	14,452	18,857	28
Jul-21	13,638	13,105	11
Aug-21	13,159	12,530	14
Sep-21	10,223	11,870	18
Oct-21	7,840	7,842	17
Nov-21	7,337	4,877	16
Dec-21	11,362	11,182	26
Jan-22	8,581	12,483	17

Tech Support Team Tickets



	Tickets Created	Tickets Closed	Avg. Days to Close
Jan-21	483	256	4
Feb-21	547	179	8
Mar-21	645	198	18
Apr-21	1,138	568	11
May-21	382	138	18
Jun-21	217	158	42
Jul-21	177	171	56
Aug-21	121	1,113	117
Sep-21	115	113	30
Oct-21	64	63	30
Nov-21	49	605	155
Dec-21	69	31	18
Jan-22	30	36	37

F. In addition, the Offeror will provide access to the database through secure methods to be defined by the authorized CDOC staff. Authorized CDOC staff will be able to retrieve defined data on an on-going basis (could be real-time, daily or other).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide access to the NextGen SCP user interface through secure methods defined by the authorized CDOC staff. CDOC staff can retrieve defined data on an on-going basis

G. The Offeror will provide requested data elements in a CSV format or format to be determined by the authorized CDOC staff. Data extracts will be downloadable, as needed,

to a format of authorized CDOC staff's choosing. The data will allow the authorized CDOC staff to perform further analysis as/when needed. The authorized CDOC staff will finalize the methods, processes and functions with the Offeror.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide the requested data elements in a format to be determined by the authorized CDOC staff. Data extracts will be downloadable, as needed, to a format of authorized CDOC staff's choosing. The data will allow the authorized CDOC staff to perform further analysis as/when needed. Securus will work with the authorized CDOC staff to finalize the methods, processes and functions.

Standard Reports

NextGen SCP has a dedicated report writer that provides investigative information based on the call detail records. This sophisticated reporting tool provides a reporting interface into all calling activities.

Reports can be generated online and exported in:

- Microsoft® Excel
- CSV (Comma Separated Values)
- Adobe® PDF format

CDOC may search and analyze details on all communication events through NextGen SCP and then run reports to identify communication trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on an extensive list of criteria options. CDOC also may create customized reports by changing search criteria. After search results are generated, you can sort based on any of the communication event details.

NextGen SCP™ Report Criteria Fields:

- Date Range
- Identifier (ID, PIN, Name)
- Continuous Voice Identification
- Communication Type (Calls and Video)
- Communication Status (Complete or Incomplete)
- Prepaid Account Number

- Destination Number (Partial or Full Number Entry)
- Call Type
- Three-Way or Remote Call Forwarding Detected
- Watched Status
- Wireless Indicator
- Visitor and Visit Type (SVC)
- Visitor Contact Number
- Visitor Identifier (ID, Name, Email)
- Phone or Terminal Location
- Number Restriction and/or Status Assignment
- Broad Search with No Data Entry
- Suspected Fraudulent Call Activity
- Destination Zone (Local, Interlata, Interstate, Intralata, International)

Custom Reports

The NextGen Secure Communications Platform™ (NextGen SCP™) is very flexible and easy to use, and allows the user to create almost limitless reporting. Should customized reports be needed, Securus will provide them to CDOC at no charge except in those cases where the customized report would require a significant allocation of resources or material changes to Securus systems and procedures.

In the small number of instances where development is needed (e.g., capturing additional information from other systems), Securus will provide the development free of charge unless the request involves significant cost to Securus. In such cases CDOC will be given the option to pay for the additional services without markup by Securus.

H. The Offeror must briefly describe how Section F and G above, will be accomplished with the proposed ITS for the CDOC and what security measures are in place to ensure authorized CDOC staff have access to only those call recordings for which they are authorized.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

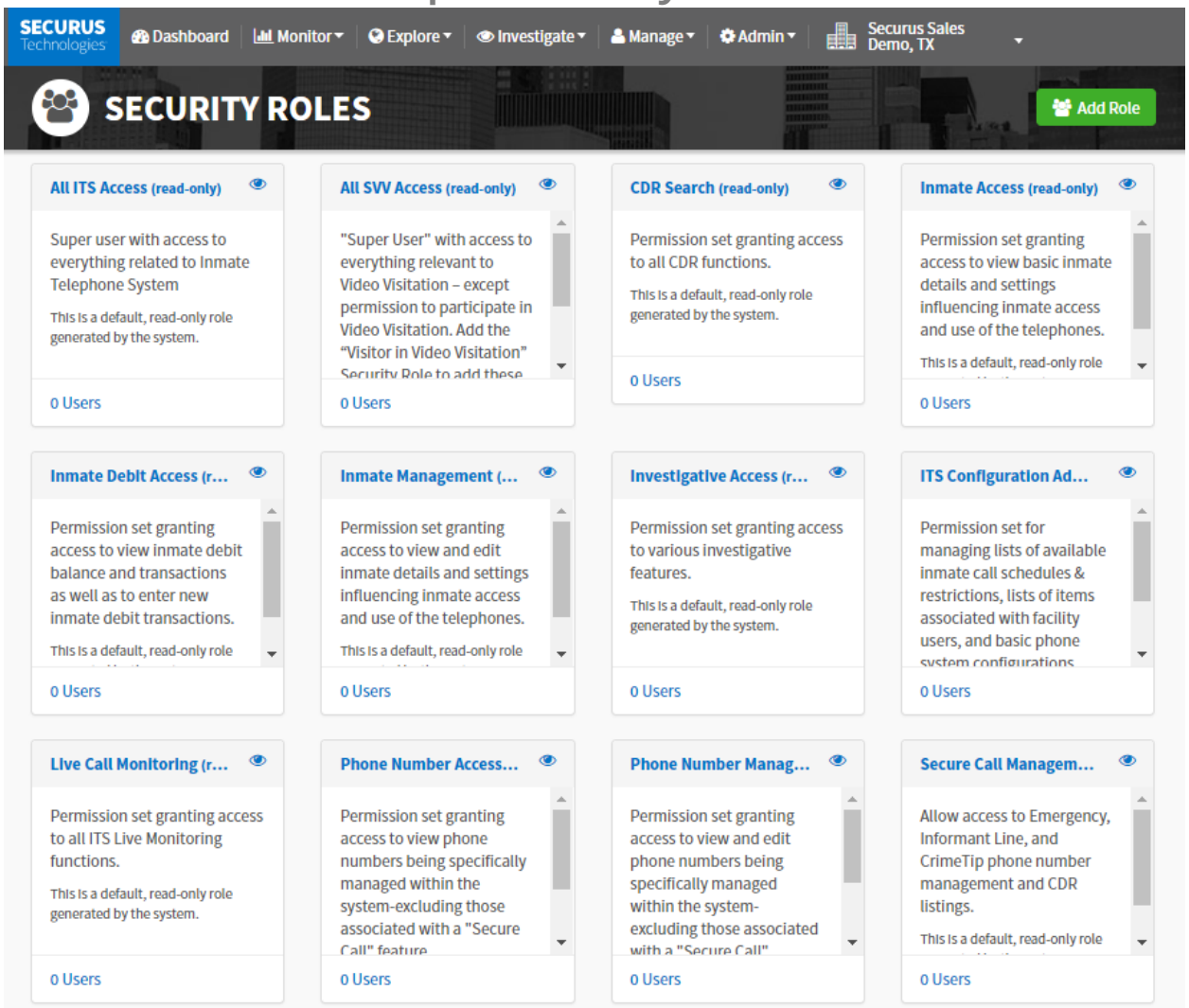
The following pages provide a brief description of the user profile settings within NextGen SCP that control which recordings and functions authorized CDOC staff can access. This document is intended to serve as a guide only and is not intended to define any particular roles within the CDOC operations.

Security Roles

NextGen SCP is entirely permission-based and assigned user roles allow or prevent access to content, data, features, and privileges for each user. The platform comes with default security roles that cover most of our customer's needs for allocating access based on common job functions. CDOC already has assigned customized security roles and may further customize security roles by duplicating and then modifying the default security roles or by creating new roles. Each user may be assigned one or several security roles, allowing unlimited options for structuring access to meet CDOC needs.

In addition, the facility administrator role can create, modify, activate, or deactivate users who have access to the NextGen SCP system.

Sample Security Roles



I. The ITS proposed by the Offeror is expected to, at a minimum, allow authorized CDOC staff to locate call recordings in the following manners:

i. Search by offender name or ITS offender ID number (approved by the CDOC);

ii. Search by certain time period (date/time);

iii. Search by certain telephone instruments;

iv. Search by called telephone number; and

v. Search by unit location.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP provides authorized CDOC staff single-point access to research the CDOC call records and recordings. Users can specify search criteria, such as offender name or ID number, time, date, calling telephone, unit location, called party telephone number, PIN, custody account number, duration, and location, and search across a site or group of sites based on their security authorization. NextGen SCP searches call detail records and can include all call attempts or just completed calls.

Search results provide detailed information about each call and will indicate whether or not the call detail record (CDR) has an attached recording. If recorded, authorized investigators can listen to the recording using the embedded call player with easy-to-use search capabilities, and features such as, pause and play.

To speed searching of a recording the player shows sound wave activity of the call to identify times of limited talk or to identify a particular event.

NextGen SCP streams call recordings to a program on an investigator's computer that can 'play" the recording through the attached speakers. While it is possible to make a recording from the speakers, this is only a copy of the original. Chain of Evidence safeguards are in place to prevent access to the actual digital copy of the recording and to eliminate any chance of manipulation, whether intentional or accidental, that could later challenge the authenticity of the call recording.

J. The ITS is expected to allow for the search criteria either individually or in combinations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP allows for the search criteria individually or in combinations.

K. The ITS Offeror proposal will provide a search capability that allows authorized CDOC staff to search call recordings for certain keywords or phrases. The Offeror will provide a description of this capability.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus; Word Alert will allow DOC staff to search call recordings for certain key words or phrases and much more. Word Alert is commercially available and can provide the following advantages for the agency and its investigators:

- A transcript of each telephone call and video session is available in minutes in its original language. *
- An English translation can be requested and displayed in seconds in line with the original language text. *
- Investigators can view a transcript alone or aligned with the audio or video player while the call or session plays. Search term matches are highlighted in the transcript. A button click jumps to the next or previous match in the transcript, moving the player automatically as well.
- Transcripts and their translations can be saved to PDF files.
- Investigators can manage a dictionary of word and phrase search terms, in any language, and create categories of search terms.
- Interactive, ad hoc searches let investigators find words and phrases in past calls and sessions.
- Automated scans constantly search new calls and sessions for target words and phrases and send alerts to investigators when matches occur.
- Alert notifications can be sent to email addresses and SMS text phone numbers.
- Snippets of matches in transcripts appear when the investigator's mouse hovers over a list of calls and sessions. Mouse clicks jump to those locations in the player and transcript.
- Integrated audio and video players can control playback speed and volume.
- Search results can be exported to downloadable reports.
- Analytics include search term category frequency graphs and totals.
- Word Alert's intelligent, behind-the-scenes analysis uncovers trending topics of conversation on calls and sessions in the facility. This can reveal illicit activity before investigators realize it exists.
- Users' call and video session playback events are logged in the NextGen SCP system, giving agencies information for auditing.

* The supported languages for transcription, and for translation to English, are Bengali, English, French, Italian, Korean, Mandarin Chinese, Polish, Portuguese, Russian, Spanish, and Vietnamese.

L. The ITS Offeror proposal will provide an alert capability that will notify authorized CDOC staff with certain keywords or phrases that are identified during the recording of the offender call.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Alerts can be configured to send email and/or SMS text message notifications. The investigator can set up the notifications when they creates the alert or at any time afterwards. They can set the frequency of the notifications, modify (add, edit, delete) the email and text message recipients, and unsubscribe from notifications for a particular alert or all email and/or text message alerts. Word Alert is commercially available.

Integrated with NextGen SCP, Word Alert is a speech-to-text transcription and keyword search tool for corrections agency investigators. It automatically transcribes all telephone calls and video sessions (if utilized) to text. Investigators can search the transcripts for words and phrases either interactively or by setting up automated, continuous scans that send them alerts when matches occur.

Word Alert helps investigators quickly zero in on the calls and sessions most likely to have investigative value. Investigators can save time by skimming a transcript or jumping to matching search terms rather than listening to the whole call or session. They can quickly get an English translation of a non-English transcript. They can uncover individuals who are talking about topics of investigative interest. Intelligent analytics reveal topics now being talked about in the facility more than in the past, uncovering problems before investigators know to look for them.

Word Alert is a Securus solution and Securus manages the solution roadmap. It is integrated with the Securus NextGen Secure Communications Platform. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.

Word Alert Capabilities

Word Alert capabilities include the following features:

- Automatic speech-to-text telephone call and SVC video session transcription
- Rapid translation to English
- Transcript aligned with the audio and video player

- Dictionary of search terms
- Interactive searches of past calls and video sessions
- Automated searches of new calls and video sessions with user alerts
- Search results with snippets and highlighted matches
- Integrated audio and video players
- Reports
- Analytics

Automatic Speech-to-Text Telephone Call and SVC Video Session Transcription

Telephone calls and SVC video sessions are automatically transcribed to text within minutes after they end. There is no need to select any for transcription. Each text transcript is in the language the offender used when starting the call or session. Transcripts are stored in accordance with the agency's call and video session retention policies.

Rapid Translation to English

The investigator can request an English translation of a non-English transcript with just a button click. The translation appears in seconds with each line under the original language line in the transcript. The English translation is stored with the original transcript for future reference.

Transcript Aligned with the Audio and Video Player

A transcript can be viewed alone or aligned with Word Alert's audio or video player. Any search term matches are highlighted in the transcript. The investigator can jump to a section of interest in either the player or transcript and the two will move in tandem to that section. In the transcript they can jump from any search match to the next or previous match, and the player will move to that location.

Export Transcript to PDF

A transcript can be exported and saved to a PDF file. Any in-line English translation in the transcript is included as well. The text is formatted exactly as it is on the screen and includes timestamps.

Dictionary of Search Terms

Word Alert has an editable dictionary of words and phrases that can be used as search terms. Investigators can add terms in any language and create categories of terms. Individual terms, or entire categories, can be used in searches.

Interactive Searches of Past Calls and Video Sessions

Word Alert makes it easy to do one-time, interactive searches of past calls and video sessions using a date range and words, phrases, and categories of terms in any language. The search can be narrowed by offender name or ID and communication type, i.e., telephone calls and/or video sessions. Results are displayed as a list of calls and sessions, each with clickable icons to show the transcript alone or with the player.

Automated Searches of New Calls and Video Sessions with User Alerts

Word Alert lets investigators set up automated scans that continuously monitor new call and video session transcripts as they come into the system. An alert is sent each time a search term match occurs in a call or session. The investigator configures an automated scan with search terms in any language and optionally with an offender's name or ID, as well as the communication type. They can also include an end date if they choose. An alert is sent to the dashboard each time a search term match occurs in a call or session. The investigator can add email addresses and SMS text message phone numbers to receive alert notifications as well.

At any time, the investigator can see the total number of alerts triggered so far by the scan. They can review the calls and sessions that triggered the alerts and can also stop the scan at any time interactively. They can modify the alerts' lists of email and text message notification recipients.

Alert Notifications to Email Addresses and SMS Text Phone Numbers

Alerts can be configured to send email and/or SMS text message notifications. The investigator can set up the notifications when they creates the alert or at any time afterwards. They can set the frequency of the notifications, modify (add, edit, delete) the email and text message recipients, and unsubscribe from notifications for a particular alert or all email and/or text message alerts.

Search Results with Snippets and Highlighted Matches

Calls and video sessions with matching search terms are each listed with their communication record information: name of the offenders, dialed telephone number, communication start date and time, and communication duration. Each record also shows a player icon and a transcript icon. Hovering over the transcript icon brings up one or more snippets from the transcript. The snippets show the search term matches in the transcript. The investigator can quickly decide whether to bypass that call or session or investigate it further. They can click on the transcript icon to open the full transcript, or the player icon to see the transcript with the player. The matching search terms are highlighted in the transcript.

Reports

The results of an interactive or automated search can be exported to a report and then downloaded. The report lists calls and video sessions that had matches, with communication record information for each one.

Analytics

Intelligent analytics reveal what people in the facility are talking about on telephone calls and video sessions without investigators having to do searches. In Analytics, the Keyword Categories screen shows how many times, and on which calendar days, words in each of the dictionary's categories occurred. The Top Keyword Trends screen shows additional words that Word Alert discovered on its own that are occurring in calls and sessions more often now than in the recent past. This trend information can uncover problems in the facility before investigators suspect they exist.

M. The security and confidentiality of data in the ITS is of critical importance. The Offeror will recover all offender telephone data for all locations, to the point of full-service operation using a data backup.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus uses a digital backup system that incorporates a mix of daily, weekly, monthly, and quarterly backups, providing facilities a complete history of their telephone data from various points in time.

Redundant protection against failures and disasters: Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at Securus Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

Unrivaled data resilience, scalability, and flexibility: The Securus storage infrastructure has more than seven petabytes of storage space in each carrier-class data center. When these very large storage systems approach designated thresholds, Securus expands capacity. We won't run out of room and there is no limit on your data

storage. The architecture of the Securus storage infrastructure makes all storage available to all servers on the network. The SAN/NAS solution delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network.

Comprehensive Security: Securus NextGen SCP is in a carrier-class data center with the most comprehensive security measures in the industry equal to appliable regulatory and compliance standards. Applications that transmit data across public networks support Transport Layer Security (TLS), certificates, and encryption. Sensitive data is encrypted both at rest and in motion. Securus provides support for SSL/TLS encryption at the application network layer. All web sessions are conducted via HTTPS using AES 256-bit encryption. Securus employs both internal and external certificate authorities to support and secure communications throughout.

N. The Offeror will perform all service and database back-ups and archiving. The Offeror will provide all archival hardware, supplies, and network recovery procedures to ensure no data is lost at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will perform all service and database back-ups and archiving, and will provide all archival hardware, supplies, and network recovery procedures to ensure no data is lost, at no cost to the CDOC.

22. OFFEROR RESPONSIBILITIES IN INITIAL INSTALLATION AND ONGOING MAINTENANCE

A. The Offeror will provide current, new state-of-the-art equipment and software at the time of installation necessary to provide the services as requested in this ITN. Offeror is expected to maintain state-of-the-art equipment for the duration of the Contract. These services include but are not limited to:

i. Telephone sets;
ii. Wiring;
iii. Connectors;
iv. Jacks;
v. Security and monitoring hardware; and
vi. Software systems;
vii. Cordless telephones.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide new, state-of-the-art equipment and software at the time of installation necessary to provide the services as requested in this ITN. Securus will maintain state-of-the-art equipment for the duration of the Contract. These services include but are not limited to:

i. Telephone sets;
ii. Wiring;
iii. Connectors;
iv. Jacks;
v. Security and monitoring hardware; and
vi. Software systems;
vii. Cordless telephones.

B. The Offeror will be responsible for all equipment in the OCS in its entirety or its individual components including, but not limited to:

i. Normal wear/use;
ii. Offender misuse;
iii. Natural disaster; or
iv. Offender unrest.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will be responsible for all equipment in the OCS in its entirety or its individual components including, but not limited to:

i. Normal wear/use;

ii. Offender misuse;

iii. Natural disaster; or

iv. Offender unrest.

Securus service maintenance agreement includes replacement and/or repair as indicated by the circumstances. Please note that Securus will repair or replace the non-functioning equipment in the ITS in its entirety or its individual components, regardless of the reason.

C. The OCS and/or component replacement will be performed at no cost to the CDOC and will occur within 2 business days upon notification to the Offeror of the OCS problem by the facility or authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will make these repairs at no cost to the CDOC and immediately upon notification.

D. Offeror provides a dedicated implementation team to deliver comprehensive training and technical support from inception to retirement.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide training and technical support from inception to retirement.

E. Offeror will provide key personnel as needed throughout the course of the work. The CDOC staff will partner with the key personnel to align the desired work outcomes, producing key results related to the critical business needs of the solution.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide key personnel as needed throughout the course of the work. Securus will work closely with authorized CDOC staff to align the desired work outcomes, producing key results related to the critical business needs of the solution.

Securus makes every effort to limit the administrative burden that can occur during a transition of service providers. We have experience installing our system at more than 2,800 customer locations. This level of experience ensures that we do not waste any of your time.

At the beginning of the project, the Securus Project Team will meet with the CDOC team on site at a CDOC location. These well-organized meetings introduce project team members and review the project plan and timetables with the CDOC team in person to ensure a successful project kick-off.

Our project managers work with the CDOC team to coordinate equipment deliveries and facility access. When Securus technicians arrive on site, they may require escorts to the phone/terminal and equipment locations. The majority of project activity will occur during normal business hours. However, Securus can accommodate late-night/overnight cut-over activities. Some customers choose this method to eliminate service interruptions.

After each facility transitions to our NextGen Secure Communications Platform™ (NextGen SCP™), our project manager and field service technician review our quality checklists with the CDOC team.

The Securus project team hosts weekly stakeholder meetings with participation from the CDOC team.

At the beginning of the implementation project, the Securus project management team will work with the CDOC team to identify key stakeholders and primary points of contact. The team defines roles and responsibilities for the duration of the project.

The Securus project management team will establish regular meeting forums and communication protocols that accommodate the requirements of the CDOC team.

Throughout the project, our project management team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

In addition to the personal communication from our project managers, Securus can set-up automated email notifications for the CDOC team. The automated email notifications the communication of updates and status changes for major milestones and other tasks.

F. For each facility installation, the Offeror will submit, to authorized CDOC staff, an implementation plan which will include an installation schedule.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide an implementation plan for each facility installation to the CDOC. A sample preliminary implementation plan is included in **Securus Attachment No. 1, Preliminary Implementation Plan**.

G. Weekly updates to the installation plan is expected to be submitted to authorized CDOC staff designated by each Participating Entity.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

H. The Offeror agrees to obtain written permission, from authorized CDOC staff, before proceeding with any work that requires cutting into or through girders, beams, concrete or tile floors, partitions or ceilings, or any work that may impair fireproofing or moisture proofing, or potentially cause any structural damage. The CDOC does not anticipate that such work will be required for the initial installation of the OCS. Initial concerns based off of site visits should be addressed in the bidder's response.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

I. The Offeror agrees to assume responsibility for all installation of equipment in accordance with the specifications contained in the manufacturer's installation instructions.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

J. Use of existing or in-place equipment including but not limited to:

i. Conduit;
ii. Raceways;
iii. Cable ways;
iv. Cable;
v. Inside wiring;
vi. Telephone set mountings;
vii. Switches;
viii. Terminal boxes; and
ix. Terminals within the facility are at the risk of the Offeror.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

K. No exposed wiring will be permitted. Ownership of any wiring or conduit placed under this Contract by the Offeror becomes the CDOC's property upon termination and/or expiration of the Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

L. The Offeror agrees that if any cabling work is required as part of any installation, all new cables will be used and marked clearly and legibly at both ends, and is expected to meet all applicable Electronics Industries Alliance/Telecommunications Association (EIA/TIA) wiring standards for commercial buildings. All new cabling required by the Offeror will be installed by the Offeror at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

If any cabling work is required as part of any installation, Securus will use all new cables and will clearly and legibly mark the cable at both ends and meeting all applicable Electronics Industries Alliance/Telecommunications Association (EIA/TIA) wiring standards for commercial buildings. Securus will install any new cabling required at no cost to the DOC.

M. The Offeror is expected to agree and have the capability to install the required quantity of telephones requested by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

N. The authorized CDOC staff reserves the right to add or delete facilities and/or facilities receiving service under the Contract upon thirty (30) days written notice. Such additions or deletions may be accomplished by letter and do not require a Contract amendment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

O. When a new CDOC facility or satellite facility is opened by the CDOC, the authorized CDOC staff will determine (in consultation with the Offeror) a schedule for installation of services and equipment at that location to ensure service as soon as practical at the new site.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

P. The Offeror will provide and install surge and lightning protection to protect their equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

In order to provide surge and lightning protection, Securus will maintain an uninterruptible power supply (UPS) backup for the equipment installed on CDOC premises. The UPS eliminates spikes, sags, surges, transients, and all other over/under voltage and frequency conditions, providing clean power to connected critical loads.

Sample UPS



The rack-mount UPS is a high-density backup-power protection solution ideal for servers, storage systems, network equipment, and other critical devices. It also offers the best UPS power protection against five of the nine most common power-quality problems. The slim design and wide range of UPS system installation possibilities make this the most versatile UPS power quality solution available.

Calls In Progress

The Integrated Access Device (IAD)s and uninterruptible power supply (UPS) maintain all in-progress telephone calls and visitation sessions for up to 30 minutes while blocking

additional call or visitation attempts after the event. After 30 minutes, the system terminates all calls/visits in progress and powers down to a quiescent state that allows it to resume full operation automatically after the restoration of commercial power.

If outages are caused by surge and/or lightning, Securus will reimburse the CDOC for lost payments.

Q. Installation of all telephones and related equipment will be accomplished during normal business hours at each facility or as directed by the facility's onsite authorized CDOC staff.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

R. The Offeror will clean up and remove all debris and packaging material resulting from work performed.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

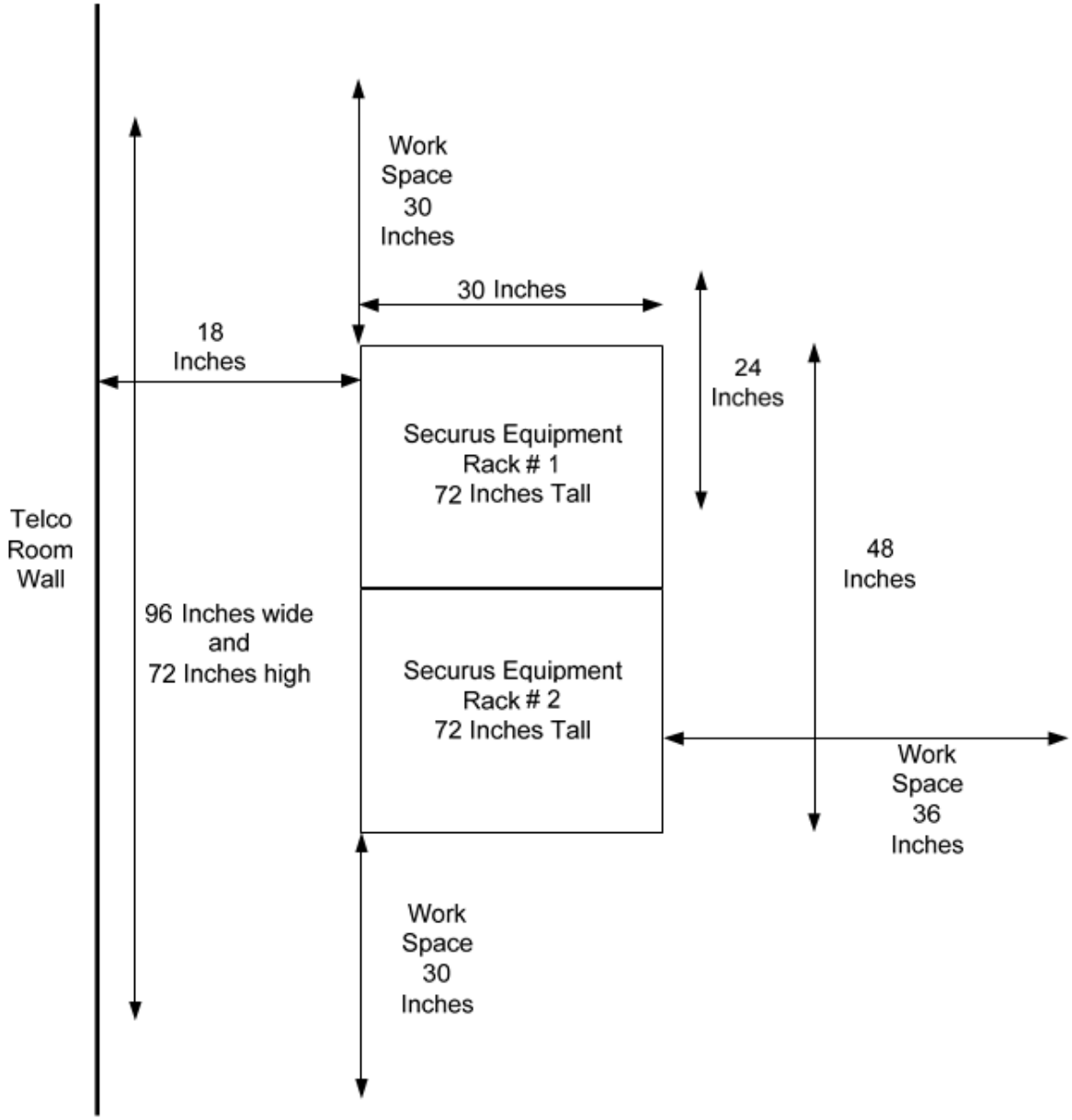
S. The Offeror will restore to original condition any damage to the CDOC's property caused by maintenance or installation personnel associated with the Offeror, including repairs to walls, ceilings, etc.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

T. Upon completion of initial installation and any additional changes as needed to the ITS, Offeror is expected to provide the authorized CDOC staff with a list of telephone numbers, serial numbers, and locations of each unit. Offeror will routinely provide updated lists containing this information to authorized CDOC staff.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

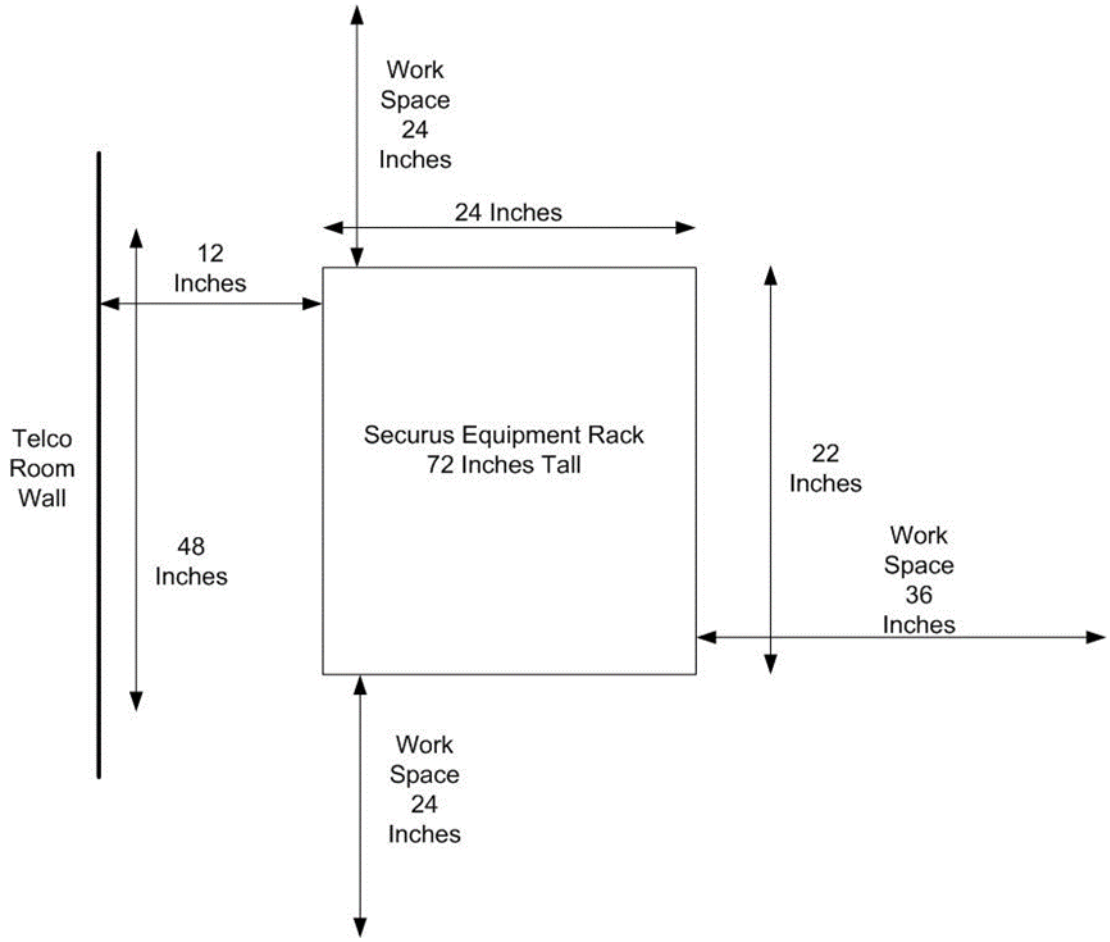
U. The Offeror is expected to indicate the physical size of any controlling equipment to be installed at the CDOC's facilities.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The following sample floor diagrams illustrate the space requirements for our NextGen SCP system, depending on each individual facility's requirements and available space.

Sample Floor and Wall Space Requirements



Sample Floor and Wall Space Requirements



V. The Offeror is expected to indicate any environmental conditions required for the proposed controlling equipment. This will include any air conditioning or heating expectations for the control room or area. The Offeror will be required to supply the necessary heating or cooling system for the control room at no cost to CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The proposed Securus solution includes equipment housed at the CDOC facility with the following requirements:

Environmental Requirements	
Operating temperature:	32°F to 104°F

Environmental Requirements	
Storage temperature:	4°F to 122°F
Relative humidity:	Up to 95% non-condensing
Air conditioning total BTUs/hour:	11,130.63 BTUs
Power:	3,262 volt-ampere

W. Cordless phones are necessary in some facilities as determined by the Appointing Authority. The Offeror will supply additional cordless telephones and/or batteries for the telephones, as needed, at no cost to the CDOC throughout the duration of this Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Upon CDOC request, Securus will provide cordless phones and/or batteries for the phones, as needed, at no cost to the CDOC for the life of the contract.

X. The Offeror will process the calls from the cordless telephones through the ITS.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The cordless phones will process calls through the NG SCP system.

23. STATION EQUIPMENT SPECIFICATIONS

A. All technical specifications and OCS expectations will meet or exceed industry standards, and will be in proper working order, clean and free from defects of features affecting appearance, serviceability, or the safety of the authorized user in normal intended use, unless otherwise required herein.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. The OCS will be capable of providing all operational features and system expectations applicable to all calls placed through the ITS, including local, long distance, and international calling.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. Telephone equipment will be powered by the telephone line and will require no additional power source. Offeror will provide a power source at the demarcation location. Offerors will be required to identify the demarcation location for each facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The telephone units are line-powered and require no external wiring, backup batteries, or electrical outlets at the telephone locations. Securus will identify the demarcation location for each facility upon award, prior to installation.

D. In the unlikely case of the loss of commercial power and the failure of the Uninterruptible Power Source (UPS), the ITS is expected to automatically restricts or "shut off" all offender telephones so that no offender calls can be made until commercial power is restored and access is once again provided by the State.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

If commercial power is lost and the UPS does not work properly or after the UPS' specified uptime, the system terminates all calls in progress per customer policy and powers down to a quiescent state that allows it to resume full operation automatically after the restoration of commercial power. Offender calls cannot be made while the system is in a quiescent state.

E. The ITS will be capable of recovering from a power outage automatically or remotely once commercial power is restored.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

After commercial power is restored, the NextGen SCP system resumes full operation automatically.

F. Offeror will explain their process to validate and restore the ITS after it is shut down. If this is longer than 60 minutes, please explain how this will become part of a service level support defect.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus Technical Support team provides 24/7/365 monitoring of all facility-based equipment, including the UPS, and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes and their vital operating statistics are sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, the Securus Field Technician will go to the appropriate location and repair or replace the equipment.

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

G. The ITS and telephone stations will contain tamper-free equipment suitable for a correctional environment. The equipment is expected to contain no removable parts.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus' offender telephones are the strongest and most reliable units available and are designed specifically for the prison environment. The following information is the manufacturer-provided telephone specifications.

The Industry Standard

The GTel model JP-3500 phones are the overwhelming choice for the Federal Bureau of Prisons, county, and city facilities nationwi proven reliability, durability, and flexibility.



Features/Options

The proposed phone models include the following features:

- Constructed of durable 14-gauge stainlesssteel
- Built in mounting plate designed for fast, easy installation

- Mounting plate includes gasket which prevents moisture from
- entering phone
- Oversized line-wire entrance hole w/ moisture preventing gasket
- Mounts directly to the wall or installs inside a hood/enclosure
- Tamper resistant locking system
- Oversized stainless-steel ADA keypad
- Adjustable volume button for full ADA compliance
- Magnetic, sealed hook switch
- Armored handset cord, with internal lanyard, is made to Bell Core standards and withstands minimum 1000-pound pulling test
- Handset cord retaining bracket is designed for fast, easy handset changes
- Stainless steel grommet provides added security for the handset cord
- Adjustable handset cord lengths, comes standard with 24" Handset length
- Optional noise-canceling microphone available
- Large customizable instruction card area
- Tested and found to comply with FCC Part 15, Subpart B and ANSI C63.4: 2014 standards. FCC Certificate of Conformity number DL-20171166613C

TTY Phones

The Ultratec Minicom IV has an easy-touch keyboard with a bright, tilted 20-character display. Minicom IV includes a printer port to connect an external printer. Turbo Code lets you enjoy "real-time" conversations with other Turbo Code TTYs, and offers the following specifications:

- Turbo Code® and Auto ID™
- Convenient GA/SK keys
- Printer port to connect to your external printer
- 20-character display
- 43-key, 4-row keyboard
- Rechargeable batteries and AC adapter included
- Baudot code (45.5/50 baud rate)



H. The Offeror will provide accommodations necessary to comply with Americans with Disabilities Act (ADA) expectations, including but not limited to: providing telephones which are accessible to persons in wheelchairs, visually impaired and

compatible with Telephone Devices for the Deaf (TDD) such as sign language video phones and, Tele- type devices and CapTel phones. The Offeror will provide the requested number of TDD units as specified by the CDOC.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.



Securus will provide accommodations necessary to comply with the Americans with Disabilities Act (ADA). The Securus program for offenders who are deaf or hearing impaired allows those offenders to place outgoing telephone calls using a text telephone (TTY) device integrated with NextGen Secure Communications Platform™ (NextGen SCP™) or through Video Relay Services.

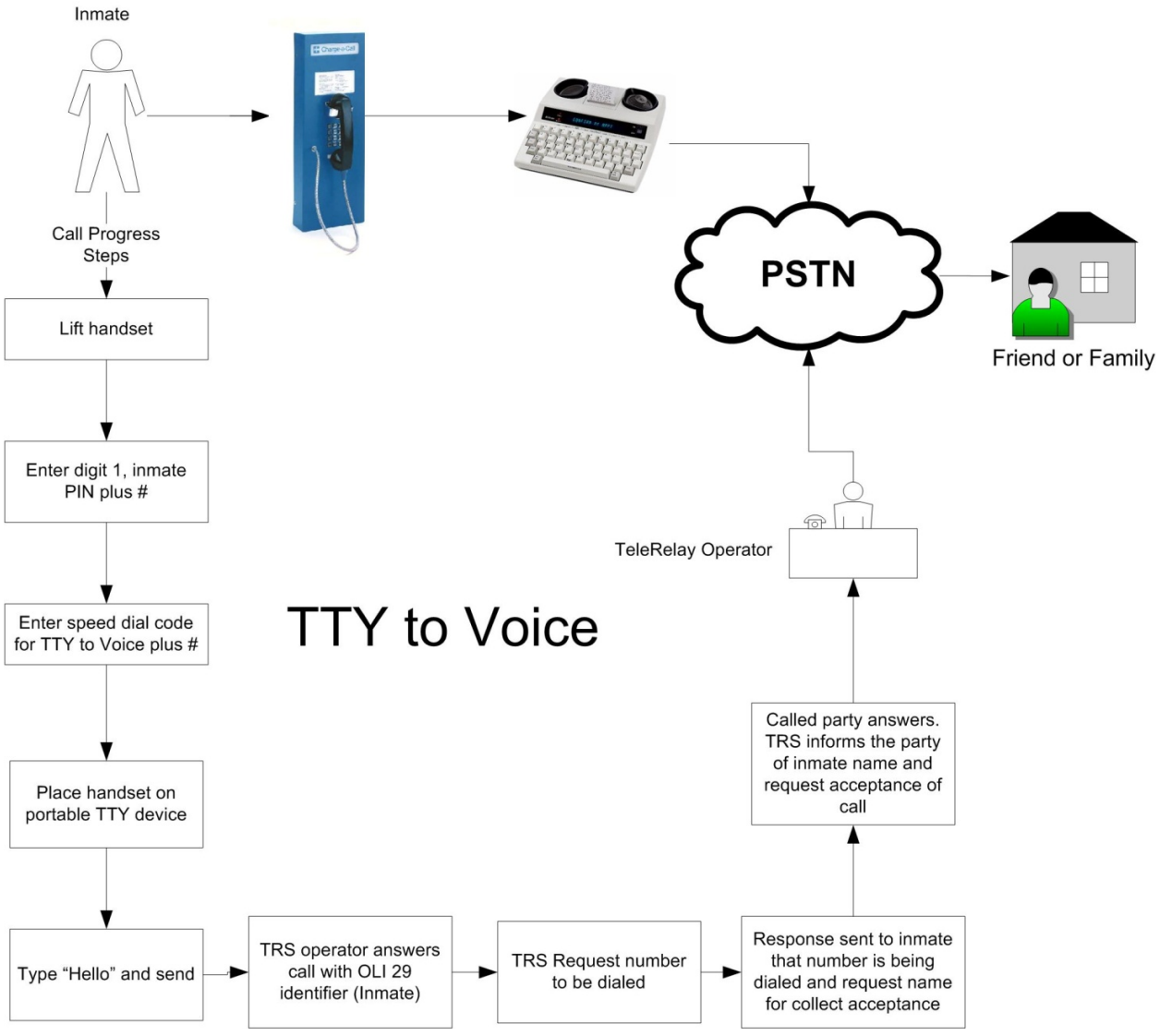
Securus is well versed with the 2010 ADA Standards for Accessible Design and Securus' installation team will work with CDOC to install our physical equipment to conform to the necessary accessibility requirements. First, Securus offers a variety of offender phone mounting options, including wall mount, floor pedestal mount, booth or enclosure, flush mount, and outdoor weatherproofed mountings. The installation team can mount the unit at varying heights to ensure there is sufficient approach, toe, and knee space, taking into consideration all possible reach ranges. The variety of mounting options along with the varying height will accommodate those with the need for accessibility for mobility impaired or wheelchairs.

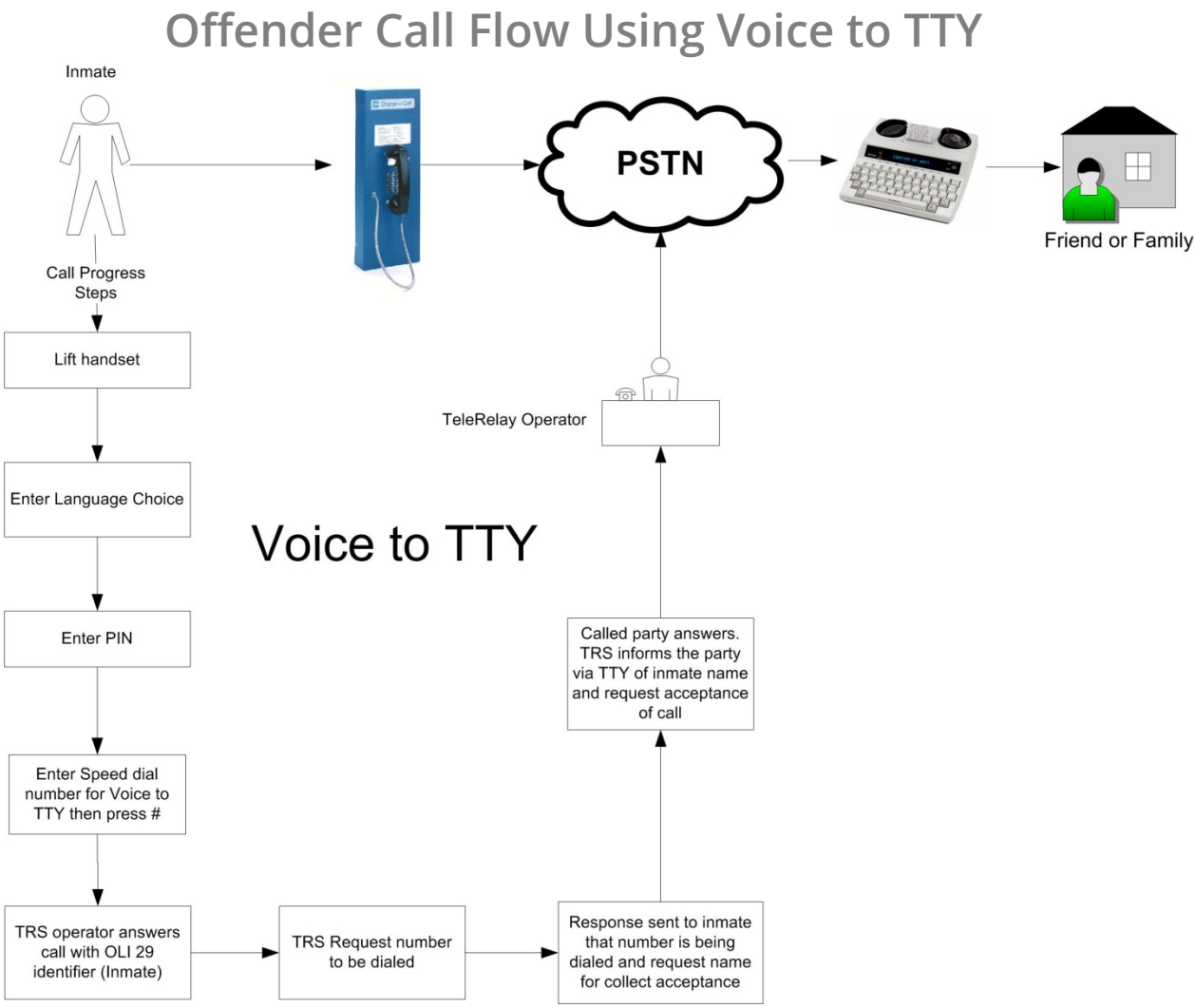
TDD and TTY Telephones

The technology provided uses dedicated ports on the NextGen SCP™ calling services and eliminates the need for a correctional officer or staff member initiating the call process. The offender placing the handset on the TTY device and entering the speed-dial number initiates the call. The offender then communicates using the TTY device through the Securus Offender Telephone System (SOTS) to the state's telecommunication relay center (TRS). The information includes the option of including the offender's PIN, along with a pre-set toll-free number that is direct-dialed to the TRS. With TRS, a special operator communicates back to the offender to confirm the connection and begins the call connection process to the called party who receives the call on a collect basis.

Integrating the TTY call through SITS allows the facility to specify various policy and security measures such as time limits, call recording, redial prevention and more. With TRS, a special operator communicates back to the offender to confirm the connection and begins the call connection process to the called party. Charges to the called party will be rated and billed by the relay service provider.

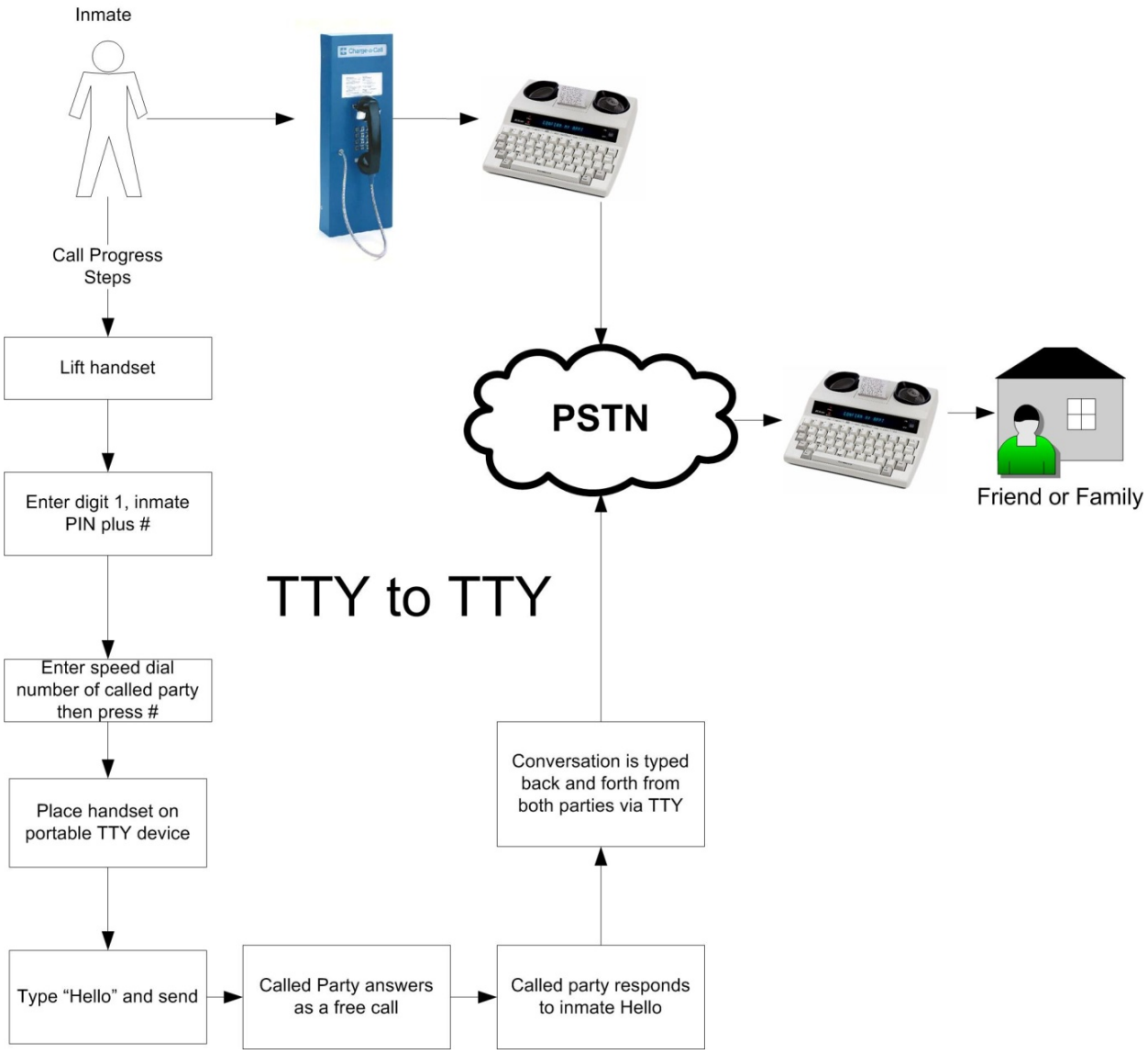
Offender Call Flow Using TTY to Voice





Offender Call Using TTY Phone Calling Another TTY (TTY to TTY).

When a hearing-impaired offender places a call utilizing a TTY phone to a friend or family member utilizing a TTY phone must include the called party on their PAN list. Facilities can apply the same calling restrictions to hearing and hearing -impaired offenders. Charges to the called party will be rated and billed by Securus and offenders can also place debit calls.



Video Relay Service

Securus provides Video Relay Services (VRS) in addition to TTY/TDD. Securus uses ZVRS/Purple for our VRS solution. The Securus offering is fully integrated into our NextGen SCP ITS and does not require users to access a totally different system to complete VRS calls. The high level of integration between Securus VRS and NextGen SCP provides hearing impaired offenders with "equal access" to communication services while providing CDOC the ability to provide, manage, and investigate offender VRS calls in a manner consistent with traditional offender calls.

Video Relay Services offer unique challenges to the correctional industry due to its reliance on American Sign Language (ASL) which requires visual communication, the automatic insertion of an ASL interpreter when needed, and adherence to FCC regulations which prohibit VRS Service providers from interfering with or recording the communication. Securus VRS addresses all of these challenges so as to provide CDOC with a VRS solution which does more than meet the requirements of ADA compliance.

Securus VRS supports both types of VRS Calls:

1. Offender VRS Phone to VRS Phone:
2. Offender VRS Phone to Standard Non-Video Phone:



Offender VRS call to F&F VRS Device



Offender VRS Call to Non VRS Phone Number



Controlling Which Offender May place VRS Calls

Authorized CDOC users can set whether an offender is eligible to use VRS from the offender custody account profile page. For CDOC, we will configure the Securus VRS application to require offender login. Then, the offender must have "VRS Allowed" setting on the offender profile set to "yes" before they are allowed to login to the application.

The Securus VRS ConnectUs application will require offenders to enter both their designated offender ID as well as their issued calling PIN before being allowed to place VRS calls. To accommodate the needs of the hearing impaired, Securus VRS can be configured in designated booking &/or intake areas to not require the use of offender

PINs to place VRS calls through Securus VRS. By these controls, CDOC is provided both security over VRS calling as well as flexibility to allow VRS calls in situations where detainees have not yet been issued a PIN.

Call Controls

Our VRS is fully integrated within the NextGen SCP network, allowing for standard NextGen SCP policies, such as PAN list control, call recording, time limits, remote printing of the call contents, redial prevention, and more. Securus VRS highly leverages the standard offender call management control structures used by NextGen SCP for traditional offender calls, including the following:

- Calling Schedules
- Max Call Duration controls
- Calling Restrictions
- Calling Velocity
- Specific called party phone number controls both globally and on offender PAN lists
- Control over which calls to record

VRS Call Monitoring and Recording

The nature of our relationship with Purple, along with the proprietary integration of technologies, allows NextGen SCP to record VRS calls while still remaining compliant with FCC regulations. If a VRS call is in progress, the GDC user will be able to click and see the video call in progress. Further, because of the full integration of VRS with NextGen SCP, call recordings are searchable within the platform and will appear in the Call Detail Record.

Securus VRS call recordings include the visual component of the offender call for both the offender and the other end of the video portion of the VRS call. The other end of the VRS call might be the offender's called party (if they are a registered subscriber to the public VRS service) or the VRS interpreter (if the called party is not a registered subscriber to the public VRS service). Since the public VRS service automatically bridges in a VRS interpreter when necessary, Securus VRS fully accommodates the various scenarios the public VRS service may encounter. These scenarios include the potential that a VRS Service provider supports Voice Carry Over (VCO). When VCO is supported, the Securus VRS call recording will include the audio component of the VRS call.

Recorded VRS calls are available for download in MP4 format and can be put on a CD for investigative purposes.

I. All telephones is expected to be of the "amplified" or of volume-controlled sort.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

J. The ITS will process calls:

i. At a minimum, in English and Spanish.

By default, the Securus calling service offers language prompts in both English and Spanish. Securus can provide additional languages on request. The NextGen Secure Communications Platform™ (NextGen SCP™) can be configured to provide prompts in as many as nine languages.

After the language prompts are configured in the calling service system, offenders select their language choice at the beginning of the call process by dialing a single digit. During call acceptance, the called party receives the acceptance instructions in English first, followed by an option to continue in the language selected by the offender. This fraud deterrent feature eliminates offender attempts to confuse called parties with a language they do not understand.

ii. Offeror will identify all possible languages to be provided to the CDOC.

iii. The offender is expected to be able to select the preferred language utilizing a simple two (2) digit code.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen SCP system currently supports the following languages. However, Securus will provide additional languages upon request by the CDOC:

English	Haitian Creole	Somali
Spanish	Vietnamese	Mandarin
Polish	French	Korean
Russian	Navajo	Italian
Portuguese	Hmong	Bengali

K. The Offeror will indicate whether the called party can also select the preferred language for call prompts.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Offenders select their language choice at the beginning of the call process by dialing a single digit.

L. Written dialing instructions for all languages will be provided to CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide durable printed dialing instructions in English, Spanish, and any other languages in use on each offender telephone, using materials and techniques appropriate for the correctional environment that explain the process in a clear, easy to read manner, as shown in the following image.

Sample Dialing Instructions in English and Spanish



SECURUS Technologies
connecting what matters

INCARCERATED INDIVIDUAL STARTS THE CALL PROCESS

Incarcerated Individual: Pick up the phone. Select an appropriate prompt

Visitor: Pick up the phone only when light blinks behind the label on the phone.

If busy: Both sides hang up and go through the process again

EL INDIVIDUO ENCARCELADO EMPIEZA EL PROCESO DE LAS COMUNICACIONES

Individuo encarcelado: Levante el teléfono. Seleccione la opción apropriada

Visitante: Levante el teléfono después que la luz en el telephone este encendida

Si la línea suena ocupada: Ambas personas cuelguen el teléfono y repitan el proceso de nuevo

1-800-844-6591 **www.securustech.net**

Securus Correctional Billing Services, a division of SECURUS Technologies IP_VIS_SM_1120



SECURUS Technologies®

DIALING INSTRUCTIONS
Calls are subject to monitoring & recording

- Select your language preference
- Select your payment option
- Follow the prompts to complete your call.

PHONE ACCOUNTS
Your Family & Friends can set up accounts by calling or visiting:

INSTRUCCIONES PARA HACER LLAMADAS
Las llamadas estarán sujetas a inspección y grabación

- Elija el idioma deseado
- Elija la opción de pago
- Siga las instrucciones para realizar su llamada

CUENTAS TELEFÓNICAS
Sus parientes y amigos pueden establecer cuentas llamando o isitando:

1-800-844-6591 **www.securustech.net**

Securus Correctional Billing Services, a division of SECURUS Technologies

IP_GEN_SM_1120

M. During the call set up process, the ITS will provide a pre-recorded announcement identifying that the call is coming from a specific offender at the facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

When a called party answers, NextGen SCP announces a collect/prepaid call from an offender and states the name of the correctional facility. The specific offender's recorded name is played to the called party as part of this call acceptance message to provide identification of the calling offender.

For example, a typical announcement would say, "You have a collect/prepaid call from an offender, "John Doe," at the [DOC Facility Name]. This telephone call may be monitored or recorded."

Each facility can customize the facility name used in call announcements.

N. The ITS is expected offer the called party an option to receive a rate quote during the call set-up process.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Once the Securus calling service notifies a called party they have a collect call from CDOC, the called party hears a quote rating of the cost of the call.

O. Call acceptance by the called party will be accomplished for all calls through caller confirmation (positive acceptance). The ITS will be able to recognize and distinguish, but not be limited to, the following:

i. Standard or irregular busy signals;
ii. Standard or irregular ringing signals;
iii. Answering machines;
iv. Cellular telephones;
v. Operator intercepts;
vi. Quick disconnects;
vii. Chain dialing; and
viii. No voice from the called party.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP complies with the requirements of sections items I - viii, as described in detail below.

P. The Offeror will provide information on how the proposed ITS will meet this requirement.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP requires active "called party" acceptance using touch-tones to complete calls. When the called party answers the phone, the NextGenSCP answer detection triggers the call acceptance voice message, which instructs the called party to accept or reject the charges call.

NextGen SCP uses call progression technology and other detection techniques to validate each call answer-and-acceptance event. The feature also enables the system to state the specific reason for the call termination when an offender's call does not complete.

For a call between an offender and a called party to take place, a valid call answer-and-acceptance must occur. It is imperative that the system be able to be able to accurately distinguish between legitimate call acceptance and other telephone activities such as:

- Standard or irregular busy signals
- Standard or irregular ringing signals
- Answering machines
- Cellular telephones
- Operator intercepts
- Quick disconnects
- Signal Interface Tones (SIT tones)
- Pagers
- Hacking
- No voice from called party
- Chain dialing

Q. The ITS will provide a recording back to the offender detailing why a call was not completed. Please provide a list of the available recorded reasons.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus' calling service has Call Termination Warnings to notify the offender why a call was not completed.

Examples of prompts for incomplete calls include:

- "Your call was answered but positive acceptance was not received from the called party possibly indicating an answering machine. Goodbye."
- "The number you called is busy. Please try again later. Goodbye."
- "The number you dialed was not answered. Goodbye."
- "Your PIN is inactive. Please hang up and try your call again at a later time. "
- "No calls are allowed at this time. Goodbye."
- "Your call was not accepted. Goodbye.
- "You have entered an invalid response, please hang up and try your call again. Goodbye."
- "The number you dialed is not on your approved calling list. Goodbye."
- "This call is being terminated by the facility. Goodbye."
- "You do not have sufficient funds to continue this call. Please hang up and try your call again at a later time."
- "Please hang up and try your call again at a later time."
- "The number you dialed is blocked from receiving collect calls at this time. Goodbye."
- "The number you dialed is blocked from receiving calls at this time."
- "Your account has been suspended. Goodbye."
- "That number is restricted. Goodbye."
- "You have entered an invalid telephone number."

NextGen SCP's Call Termination Warnings also notify the offender and the called party of call termination at one to two minutes prior to ending a connected call.

R. Completing all CDOC authorized calls is a requirement. State the process for completing those calls that would normally be blocked because of Competitive Local Exchange Carrier (CLEC) issues.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides options to connect calls that would normally be blocked because of CLEC issues:

The majority of called parties receiving calls have pre-established accounts with Securus. For called parties who do not have a Securus account and who would normally be blocked because of a CLEC issue, the AdvanceConnect Single Call (ACSC) service allows for single calls to connect that previously would not have been

completed. Instructions are provided on how to set up a Securus AdvanceConnect account.

ACSC allows family and friends to connect to their offender without having an existing Securus AdvanceConnect prepaid account or in the event that their AdvanceConnect account does not have enough funds to complete a call.

Upon receiving an unbillable call from an offender, the family or friend will be presented with the opportunity to enter a credit or debit card to pay for the just one call. They will be billed for the time of the call at the facility specific per-minute rate plus government taxes and applicable fees for that facility.

S. Provide operational specifics and a description of the proposed ITS validation process.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As a real-time, computer telephony-based switching system, the Securus calling service never connects an offender to a conventional dial tone. All dialed numbers, whether prepaid or collect, are thoroughly analyzed prior to processing the call. This includes determining the validity of area code and exchange by checking the number against any restrictions. These include customer requested blocks, confirmation of payer's available funds or credit worthiness, and phone number attributes by accessing national database information. The system will only dial a number after passing all of these tests.

To ensure proper billing of offender calls Securus establishes a relationship with our customers and does not need to bill through other carriers or a third party. Securus offers a wide verity of payment options; Friends and Family prepaid, Direct Billed (collect), offender prepaid debit and prepaid calling cards that do not rely on other carriers for billing or collections.

- AdvanceConnect - a friends and family-owned prepaid calling account that allows friends and family members to receive collect calls from offenders and have the call charges deducted automatically from the prepaid balance on the AdvanceConnect calling account.
- Direct Bill – a friends and family-owned calling account that allows friends and family members to receive collect calls from offenders and have the call charges billed directly from Securus to the Direct Bill account holder each month. Friend and family members are required to pass a credit check in order to be approved for a Direct Bill account.
- Offender prepaid card - an offender purchases prepaid calling card at the commissary and uses their PIN to access the card's funds

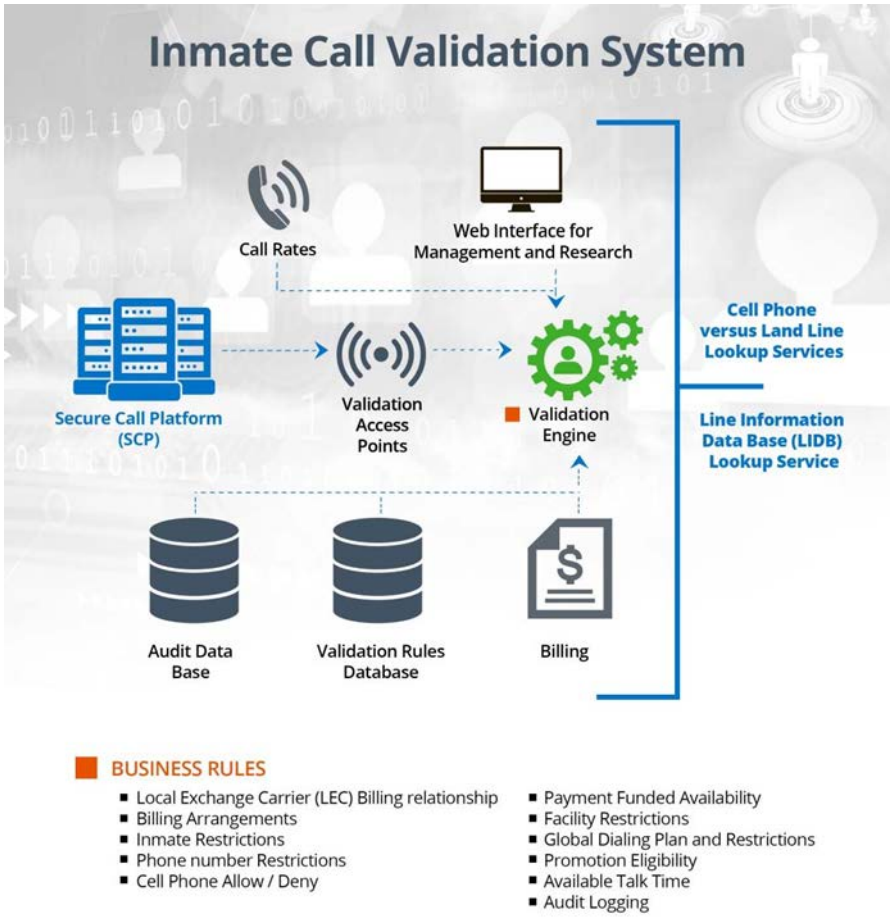
- Prepaid account for offender - Friends and family members can fund an offender prepaid account through any of the Securus funding options
- Offender trust fund account - offender funds directly debited from the offender's trust fund account (optional, requires trust fund integration)

Securus uses our own billing system and does not contract with outside billing contractors, which might expose call records to tampering or corruption. Because SCP is a centralized platform, there is no need to download call records as there would be with a traditional premises-based system. Call records are entered directly into the billing system for rating and billing on a near real-time basis. High-level data security measures prevent tampering of call records in all hardware and software systems used by Securus to rate and store call records.

Validation Process

We screen all calls to eliminate fraudulent activity, and to ensure only authorized individuals receive calls. The real-time validation process, as shown in the following graphic, outlines the elimination of unauthorized activity.

Call Validation Process



The following checks are performed during the validation process:

- When personal allowed number (PAN) lists are used by a facility, the first check ensures the number dialed is included on the offender's PAN list.
- All calls are verified to determine if the payer has requested a block.
- All calls are compared to system and administration blocks to ensure numbers that are not allowed will not be called.
- All collect calls are validated through a national line information database (LIDB) to determine if any calling restrictions exist for the number.

T. Include whether the Offerors validation is done in real time or by batch.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus' validation process is real-time.

24. DATA STORAGE

A. The Offeror performs all ITS database back-ups and archiving including all call records, ITS programming database and call recordings. All archival hardware, supplies, network and recovery procedures, which ensure no data will be lost, will be provided by the Offeror at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus uses a digital backup system that incorporates a mix of daily, weekly, monthly, and quarterly backups, providing facilities a complete history of their CDRs from various points in time.

Securus stores all facility data in centralized, fault tolerant data repositories for easy, secure retrieval from any location, by any authorized user. If there is a localized facility outage, approved facility personnel can access site data from any location, at any time. The platform resides in two, geographically diverse, fault tolerant, carrier-class data centers to ensure data integrity, all at no cost to the CDOC.

B. The Offeror will briefly describe how they will perform back-up or ITS redundancy of call data.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus uses a digital backup system that incorporates a mix of daily, weekly, monthly, and quarterly backups, providing facilities a complete history of their CDRs from various points in time.

Securus stores all facility data in centralized, fault tolerant data repositories for easy, secure retrieval from any location, by any authorized user. If there is a localized facility outage, approved facility personnel can access site data from any location, at any time. The platform resides in two, geographically diverse, fault tolerant, carrier-class data centers to ensure data integrity.

Redundancy

Redundancy is a key component of the Next Generation Secure Call Platform (NG SCP). While operating on a single platform, Securus' NG SCP runs on duplicate environments in separate data centers in Atlanta, Georgia, and Dallas, Texas. Each component has N+1 redundancy, meaning that a failure of any one component does not result in downtime because there is a backup available to resume its function. In addition to the inherent redundancy of SCP, Securus has also designed redundancy into all support systems, either through N+ 1 configuration, database clusters, virtual machines, load

balancing, or other failover methods. All network transport has redundant network equipment and routing to allow traffic to reroute in the event of a failure.

The NG SCP platforms in Dallas and Atlanta were designed and built to the same specifications. This standardization allows re-homing of systems from their primary data center to an alternate data center in the event of a failure.

All circuits coming into Securus data centers use multiple diverse carriers, including the interconnections between data centers. In the event of a failure, traffic will reroute across a redundant circuit or path. In addition, Securus uses multiple carriers for offender calls from the NGSCP platform. Calls to family and friends will immediately reroute upon failure of any carrier.

Securus uses multiple methods of storage to minimize the risk of data loss. All critical systems and data are backed up at regularly scheduled intervals and stored offsite for retrieval, if needed. In addition to offsite storage, Securus replicates voice clips, call recordings, and validation data between the data centers.

Securus uses industry-leading vendors for all platform and network hardware, including Dell, Cisco, Oracle, EMC, Big IP, and Intel. In addition to the redundancy designed into the platform and network, Securus also maintains a spare parts inventory onsite at each of our data centers to expedite repair of a failed component. Securus also maintains premium-level support contracts with each vendor that define stringent service level agreements in case of a failure.

Securus maintains an inventory of spare parts for our facility-based components at our headquarters in Dallas, Texas, and has distribution agreements with multiple vendors to provide expedited national delivery service. The corporate headquarters maintains a standardized emergency recovery package of frequently used spare parts and equipment that will be available for shipment to support restoration efforts at our customer sites. Our technical field representatives located throughout the country also carry an inventory of the most commonly needed spare parts. With spare parts on board our service vehicles, most facility-based equipment malfunctions can be resolved with a single site visit.

C. The Offeror will provide full ITS programming back-up on a daily basis including, but not limited to:

i. All call restrictions;
ii. ITS offender ID numbers;
iii. Recorded offender names;
iv. ITS prompts; and
v. Other ITS operating database information.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus uses a digital backup system (as described above) that incorporates a mix of daily, weekly, monthly, and quarterly backups, including settings such as call restrictions, offender ID numbers, recorded offender names, ITS prompts, and other ITS operating database information.

Securus will comply with items I – v.

D. The Offeror will provide full ITS programming back-up in real time including, but not limited to:
i. All call restrictions;
ii. ID; Both CDOC, ITS and/or PIN
iii. Recorded offender names;
iv. ITS prompts; and
v. Other ITS operating database information.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Changes made to the ITS settings, such as call restrictions, offender ID numbers, recorded offender names, ITS prompts, and other database information are backed up in real-time as the changes are made. Securus backs up all call restrictions; iD—both CDOC, ITS and/or PIN; Recorded offender names; ITS prompts; and other ITS operating database information.

E. For example, when an Administrator updates an offender's ID, the ITS automatically backs-up such changes immediately to the Offerors off-site location.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Updates to an offender's ID are automatically backed up immediately to the Securus off-site location.

F. The Offeror will provide full ITS offender call record back-up from each CDOC location on a daily basis.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus incorporates a mix of daily, weekly, monthly, and quarterly backups, so facilities will have a complete history of their CDRs and recordings from various points in time.

Call recordings are available for playback immediately. As an additional layer of protection, Securus replicates call recordings between its Dallas and Atlanta data centers, at a minimum, on a daily basis.

G. The Offeror will provide full ITS offender call record back-up in real time. For example, when an offender has completed all information regarding the call, the Offeror will back-up immediately to the Offerors off-site location.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus backs up call records in real time by using a combination of Oracle™ database and Elasticsearch® for storing the communication detail records (CDRs).

Oracle database delivers economies of scale on easily managed grids, making it easier to:

- Reduce downtime with maximum availability
- Partition and compress data to run queries faster
- Protect and audit data, and enable total recall of data
- Use standby resources exclusively

Oracle simplifies the process of linking data in multiple tables. This is a key feature of a relational database management system. Storing data in multiple tables allows Securus to define relationships between the tables, as well as the applications that feed information to those tables.

Elasticsearch is a distributed, RESTful search and analytics engine that provides Google™-like search capabilities for the platform. Elasticsearch stores a subset of CDRs from Oracle, allowing our customers to perform full-text queries with faster access.

Securus uses the Oracle and Elasticsearch datastores to respond faster to changing business conditions, providing clients a system that is more responsive to their evolving needs.

H. The Offeror will briefly describe how the local ITS databases at all CDOC facilities will be kept current with the ITS back-ups at the Offerors off-site location in case of required re-programming or ITS recovery at the CDOC facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus stores all facility data in centralized, fault-tolerant data repositories for easy, secure retrieval from any location, by any authorized user. Securus uses a digital backup system that incorporates a mix of daily, weekly, monthly, and quarterly backups so that facilities will have a complete history of their CDRs from various points in time.

If there is a localized facility outage, approved facility personnel can access site data from any location, at any time. The platform resides in two, geographically diverse, fault-tolerant, carrier-class data centers to ensure data integrity.

Call recordings are available for playback immediately. Should Securus permanently lose call data, Securus is responsible to the CDOC for reimbursement. However, as an additional layer of protection, Securus replicates call recordings and records between its Dallas and Atlanta data centers.

I. The Offeror must agree that the CDOC retains ownership of all archived information, call detail, offender records, call recordings, etc. The Offeror must agree that the CDOC has the right to obtain all archived information, call detail, offender records, call recordings, etc. associated with the ITS regardless of the location of such information within the Offerors organization or site.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus agrees that ownership of archived information such as call detail, offender records, call recordings, etc. in the performance of this contract will become and will remain property of the CDOC.

J. The ITS will store all call detail records, including all attempted and completed calls. This data will be stored at the Offeror sites throughout the duration of the Contract. Upon successful ITS implementation, the Offeror will either import the previous year's telephone data or pay the previous Offeror to provide two (2) years of call record storage and retrieval at no cost to CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP™ retains communication detail records on all communication attempts and events. Securus does not limit the communication data storage time. Since every site's requirements are different, Securus works with each facility customer to define their optimal data storage timeframe. All recordings are stored online within both carrier-class data centers.

Securus will either import the previous year's telephone data through our THREADS platform or negotiate and pay the previous vendor to provide two years of call record storage and retrieval at no cost to CDOC.

K. The Offeror will provide authorized CDOC staff with a "Certificate of Destruction".

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide authorized CDOC staff with a "Certificate of Destruction".

L. The ITS will record all data with a historical transaction record. All data will be stored/archived for retrieval/backup in a database when requested by authorized CDOC staff in accordance with the following:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

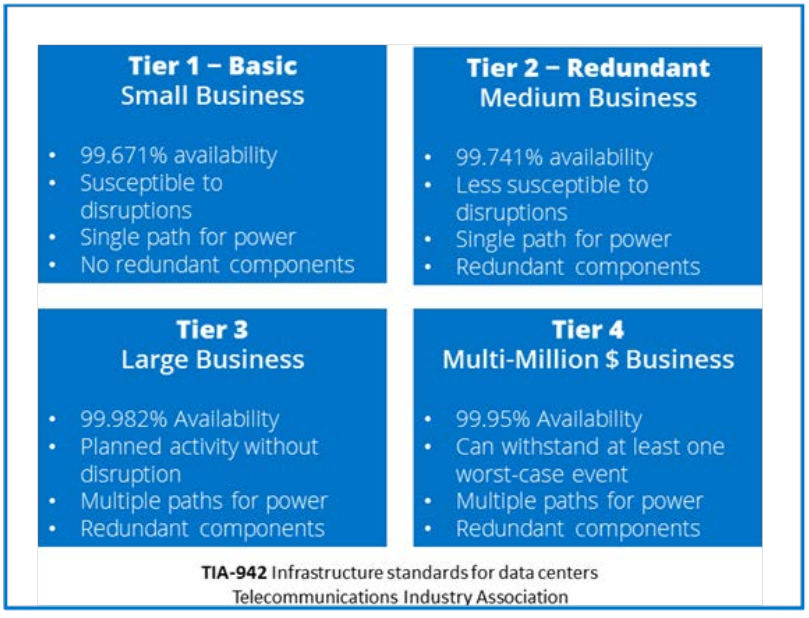
NextGen SCP records all data with a historical transaction record—the communication detail record. All data is stored/archived for retrieval and backup in a database when requested by authorized DOC users.

i. All historical data will be centrally stored and accessible for reporting purposes.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All historical data is centrally stored and accessible for reporting purposes, from our data centers. Securus maintains a presence in two data centers in geographically diverse locations. Our data centers are designed to withstand worst case events and maintain 99.95% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier IV (highest availability) data centers including:

- Ability to withstand a 96-hour power event
- 2-hour fire protection
- Multi-layer physical security
- Multiple power delivery paths.



Additionally, Securus data centers have redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity. Securus data centers are manned 24x7x365 for immediate physical assistance inside the data center.

Multiple checks ensure data center physical security including guarded, photo-verified check-in, dual door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Reporting

Authorized DOC users can access the historical call detail records through the NextGen SCP user interface, using any web-enabled device. NextGen SCP has a report writer that provides investigative information based on the communication detail records. CDOC may search and analyze details on all communication events through NextGen SCP and then run reports to identify communication trends, assess monitoring efforts, investigate suspicious activities, and manage phone/terminal usage.

Custom and standard searches worth sharing: NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on an extensive list of criteria options. CDOC also may create customized reports by changing search criteria. After search results are generated, you can sort based on any of the communication event details. Then, with a single click, the data exports to Excel, CSV (Comma Separated Values), or Adobe PDF format and may be saved, printed, or emailed to others.

NextGen SCP™ Report Criteria Fields
▪ Date Range ▪ Identifier (ID, PIN, Name) ▪ Continuous Voice Identification ▪ Communication Type (Calls and Video) ▪ Communication Status (Complete or Incomplete) ▪ Prepaid Account Number ▪ Destination Number (Partial or Full Number Entry) ▪ Call Type ▪ Three-Way or Remote Call Forwarding Detected ▪ Watched Status

NextGen SCP™ Report Criteria Fields

- Wireless Indicator
- Visitor and Visit Type (SVC)
- Visitor Contact Number
- Visitor Identifier (ID, Name, Email)
- Phone or Terminal Location
- Number Restriction and/or Status Assignment
- Broad Search with No Data Entry
- Suspected Fraudulent Call Activity
- Destination Zone (Local, Interlata, Interstate, Intralata, International)

ii. This information is expected to be available for reporting in a CSV format or format of authorized CDOC staff's choosing.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Standard reports can be generated and then exported into Excel, PDF, or CSV files. Should the DOC need another type of format, Securus will work with the State to provide the necessary formats.

iii. The Offeror will store telephone data throughout the duration of the Contract and/or successful transfer of the data to the authorized CDOC staff. Call records detail and call recordings will be available "on-line" for a minimum of twenty-four (24) months from the date of the call and call records detail will be available "off- line" for an additional forty-eight (48) months, or a total of seventy-two (72) months from the date of the call. "Off-line" records will be in a format readily accessible to the authorized CDOC staff upon request.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will store telephone data for the duration of the contract and/or successful transfer of the data to the authorized DOC staff. Call detail records and call recordings will be available online for a minimum of 12 months from the date of the call and call records detail will be available off-line for an additional 48 months, or a total of 60 months from the date of the call. Off-line records will be in a format readily accessible to the authorized DOC staff upon request.

iv. All data will remain the property of the CDOC and the Offeror will not use the data for any purpose other than as required in the Contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus with comply with the requirement that all data will remain the property of the CDOC and the Offeror will not use the data for any purpose other than as required in the Contract.

M. The Offeror will have a written Disaster Recovery Plan and Continuity of Operations Plan and associated internal system equipment that will be capable of providing for support in case of failures in power, ITS data networking, and Offerors equipment at its host site through the user-level equipment provided by the Offeror, and for all natural or man-made disasters including flood or fire at the host facility. These plans and all updates will be reviewed and accepted by the authorized CDOC staff and kept for reference purposes.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus written Disaster Recovery Plan and Continuity of Operations Plan is designed for rapid response with unmatched service and support in any circumstance. Our goal is to prevent or minimize down-time and remove your administrative burdens. **Securus takes care of communications and technology while you take care of your population and facilities.**

- Robust network architecture designed to mitigate issues before they occur
- Field service team readily positioned close to your facilities and on-call 24/7
- A plan for escalating issues, adding resources, and recovering quickly

If a natural disaster or other significant adverse event occurs, CDOC has the full support of the Securus Network Operations Center, the Securus Technical Support Team including engineering resources, and the Securus Field Service Team, including over 290 Field Service Technicians supported by a centralized field dispatch team. **Our Field Service Technicians are fully trained in our disaster recovery plan and processes**, and they are strategically positioned to support your ongoing maintenance and fast response in emergencies.

Response operations begin as soon as personnel safety is assured, and all emergency recovery operations are prioritized by critical facilities and equipment locations. For situations that are expansive in nature, we prioritize maximum-security sites and facilities with high offender phone usage.

Securus' Three-Tiered Approach to Disaster Response and Recovery

1. **Facility-Specific Emergency Response Checklists**

   For every facility, Securus develops an emergency response checklist to protect equipment and personnel in the event of an emergency. These procedures may be as simple as using sandbags to stabilize equipment and placing tape on windows exposed to high winds. Your checklists will focus on mitigation and recovery with contingencies for extreme conditions such as earthquakes, flash floods, power outages, etc. Each checklist will be coordinated with CDOC for consistency with your policy and procedures.

2. **Systemwide Disaster Response Plan**

   Securus works with you to declare emergencies for situations that are catastrophic and may impact a localized area or wide-spread region. Recovery plans are triaged based on the extent of impact and recovery operations may last a few hours, days, or weeks. Securus prioritizes recovery of premise-based equipment by facility type and equipment location. The Securus Local Recovery Team will continue recovery operations until operations are restored. Retrospective reports are completed for all declared emergencies to advance our emergency recovery planning efforts for the future.

3. **A Foundation of Network and Equipment Preventative Measures**

   CDOC avoids many communications-related disasters because we are prepared: Securus provides a network and infrastructure tested to withstand adverse conditions, minimize outages, and protect your data. We research what works and then we implement continuous improvements. Securus adds layers of redundancy at the local and national level to our core network and operations centers. We stock your facility and our Field Service Team with spare parts. We back up your data at two geographically diverse Securus data centers and layer redundancy throughout each component of our network. Information is routed through geographically diverse and route-diverse network paths, all while we monitor operations and communications 24x7x365.

Additional details on the Securus Disaster Recovery Plan and our preventative measures are outlined on the following pages. It's difficult to contemplate every contingency, but with 30+ years of experience providing communications and technology services to the corrections industry, **Securus has the experience to take care of CDOC even when the unexpected occurs.**

CDOC Emergency Condition Declaration

If you encounter a catastrophic adverse event or disaster at your facility, immediately call the Securus Emergency Numbers that you are provided. Your call will be answered 24x7x365. Then with your Securus Account Manager you will request that Securus General Manager declare an emergency condition. Operations management then establishes an immediate conference bridge with the appropriate participants to gather information substantiating that an emergency status is warranted and determines the Disaster Level.

Securus classifies disasters on a Disaster Level Scale of 1-3:

- Level 1 Disasters are catastrophic events that are extremely wide-spread and affect many facilities and many customers.
- Level 2 Disasters are high-impact and affects a more wide-spread area than Level 3.
- Level 3 Disasters are moderate impact disasters typically affecting a localized area or specific facility with consideration that elevation of level may be needed.

A single event trouble ticket is used to track all recovery efforts. The Securus Technical Support Team will open a new trouble ticket in our ticket tracking system, indicating the declared condition level and the date and time of the declaration. All open tickets pertaining to the ongoing emergency recovery effort will be linked so that all recovery efforts are tracked as a single incident to facilitate complete resolution. This is critical for efficient and complete resolution in situations of extended recovery.

If needed, Securus will deploy and pull resources from our nationwide network and engage our vendors to supply additional resources, equipment, or manpower.

SECURUS EMERGENCY RESPONSE DISASTER LEVELS

Disaster Level 1

Securus provides a full-headquarters response and may deploy a Headquarters Response Team to the region to coordinate and assist local recovery efforts. Securus Local Recovery Team activated, and your Account Manager will work with you to initiate a Command Center, including Securus Leadership. Necessary skill levels and geographic proximity are matched to your site's needs; additional personnel are dispatched as needed.

SECURUS EMERGENCY RESPONSE DISASTER LEVELS

Disaster Level 2

Securus Headquarters Response Team assists Securus Local Recovery Team as needed; onsite technician requirements assessed, and additional personnel dispatched as and when needed.

Disaster Level 3

Securus Local Recovery Team coordinates all recovery operations. Headquarters assistance beyond standard Network Operations and Technical Support Teams likely not required.

Risk Mitigation and Proactive Monitoring



The Securus Network Operations Center (NOC) continuously monitors all data centers, infrastructure components, platform systems, and network/communication systems using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus NOC also monitors real-time video surveillance and environmental alerts for the Securus data centers. In the event there is an issue at the Securus Network Operations Center, **Securus maintains a fully redundant backup Network Operations Center at a separate physical location.**

The Securus Technical Support Team monitors all facility-based equipment and connectivity 24x7x365 including firewalls, integrated access devices (IADs), visitation phone monitoring (VPM) units, routers, switches, on-site systems, wireless access points, user interfacing kiosks and terminals, and uninterrupted power supply (UPS) systems.

The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. In addition to real-time monitoring and alerting, Securus Technical Support also leverages our network performance monitoring system to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. This ongoing, proactive, in-depth analysis of your systems' performance enables our Technical Support Team to prevent and mitigate facility issues.

Data storage redundancy is a key component of Securus' Risk Mitigation and Disaster Recovery Plan. Securus maintains two data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.995% availability.



Securus' data centers meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier III, with some Tier IV (highest level) attributes, for data centers including:

- ability to withstand a 96-hour power event
- multi-layer physical security
- multiple power delivery paths

Each data center has redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity.

Securus' data centers are staffed 24x7x365 for immediate physical assistance inside the data center.

Data is no longer susceptible to loss due to an individual drive failure or issues at your location: The Securus communication platform uses technology that is much more advanced than traditional local onsite storage. Securus uses a mix of Storage Area Network (SAN)—a high-speed sub-network of shared storage devices—and Network-Attached Storage (NAS). This architecture avails all storage devices to all servers on Local Area Networks (LANs) or Wide Area Networks (WANs). Data is stored in Redundant Arrays of Independent Disk (RAID) formats, spreading the data across multiple drives, which provides additional protection. Accordingly, this architecture provide facilities with the ultimate protection against single drive or server failures, as well as increased security. **Securus maintains hardware replacement inventory on your site, in our Field Service Team vehicles, and at centralized locations.** In addition, we have distribution agreements with our vendors so that in the event of disaster recovery efforts, we can get replacement equipment to your facilities quickly.

Localized Event Affecting Only Securus Facilities

In the event of a disaster impacting Securus, the local Securus Network and systems, or NextGen SCP, Securus immediately assembles a team of engineers to investigate and restore services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and a list of third-party vendors to engage if needed. Our priority is fast resolution and minimal downtime. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Upon confirmation of a service-impacting event, the Network Operations Center will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

The Securus Executive Team and the Securus Account Management Team receive SIRs and communicate with you directly. In addition, the Securus Technical Support Team may communicate a service-impacting event via a splash screen on the NextGen SCP user interface introductory page. Securus updates you regularly throughout resolution. Securus investigates every service-impacting event, completes a root-cause analysis, and provides the analysis to you upon request.

N. The Offeror will store data throughout the duration of the Contract and/or successful transfer of the data to the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

25. SECURITY FEATURES

A. The ITS will allow multiple operators simultaneous access while maintaining adequate security to prevent unauthorized use and access.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The SCP allows an unlimited number of authorized users to access the user interface simultaneously, while providing security to prevent unauthorized use and access. All users must have a valid username and password to access the system.

B. The ITS will contain security features, which prevent unauthorized individuals from accessing any information held by the Offeror. Secure access to the ITS and the database will be maintained at all times.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus takes the security and access to our software/application very seriously and hence have implemented one of the strongest controls in the industry. Securus access controls for all systems are audited for compliancy with the following accreditations/certification:

- SSAE16; (SOC1, SAS70): Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization
- SOX: The Sarbanes–Oxley Act of 2002, is a United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms.

Encryption & Security Standards

Protecting your data: Securus developed a strong corporate Information Security Governance and Cyber-Security framework using the NIST guidelines, including 800.53 current version. Applications transmitting data across public networks support TLS 1.2 with AES-256 bit encryption. Sensitive data is encrypted both at rest and in motion. Securus provides support for TLS encryption at the application network layer. All web sessions and services are conducted via HTTPS using AES 256-bit encryption. Securus uses a gold-class vendor-provided certificate service for external and internal SSL connections.

The NextGen SCP user interface encrypts and decrypts user page requests, as well as the pages that are returned by the web server. Access to Securus server information is done through HTTPS—HTTP application layering with Transport Layer Security (TLS) as a sub-layer. The use of HTTPS protects against eavesdropping and man-in-the-middle

attacks (events where attacker secretly relays, and possibly alters, the communication between two parties who believe they are directly communicating with each other).

CJIS-compliant access: Securus uses an industry-recognized leader to provide remote access to Securus systems within state networks. This remote access system provides secure, encrypted, CJIS-compliant access to Securus systems. Securus also uses a state-of-the-art Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor and protect our network boundaries. Securus infrastructure servers and all workstations require anti-virus protection and receive regularly scheduled security patches and updates

For your team, NextGen SCP can enforce strong password policies for individual with minimum password length, 30-/60-/90-day password expirations, case sensitivity requiring upper- and lower-case letters, and special characters (@, #, $, etc.).

C. The ITS provided by the Offeror will not be capable of being detected by the called party for calling number identification (caller ID).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen SCP is undetectable to the called party for calling number identification.

D. The ITS will prohibit direct-dialed calls of any type.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All calls are processed through the NextGen SCP and the automated operator services. Direct- dialed calls are prohibited.

E. The ITS will prohibit access to "411" information service.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP will be installed and maintained so that access to the 411-information service will be prohibited and blocked. NextGen SCP offers unlimited blocking so the resulting call blocking table that is created may contain as many entries as needed. In addition, there is an associated “Description” field that allows for additional information to be attached.

Securus will upload and maintain a DOC call blocking list during and after the installation process to eliminate the burden of initial setup and maintain ongoing updates from your facility staff.

All dial-around area codes and exchanges, such as 800, 900, and 976, are blocked by default. Access to live operator services, such as 0, 411, and 911, are also blocked by default.

F. The ITS will prohibit access to CDOC designated numbers.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will include DOC-designated numbers in the global call blocking list upon installation and as an ongoing service.

G. The ITS must be able to be shut down quickly and selectively. Authorized CDOC staff must be able to shut down the ITS by virtual cut-off switches at several locations including, but not limited to:

i. At demarcation location - total facility telephones;

ii. By central control center - select telephones; and

iii. By select housing units - control center.

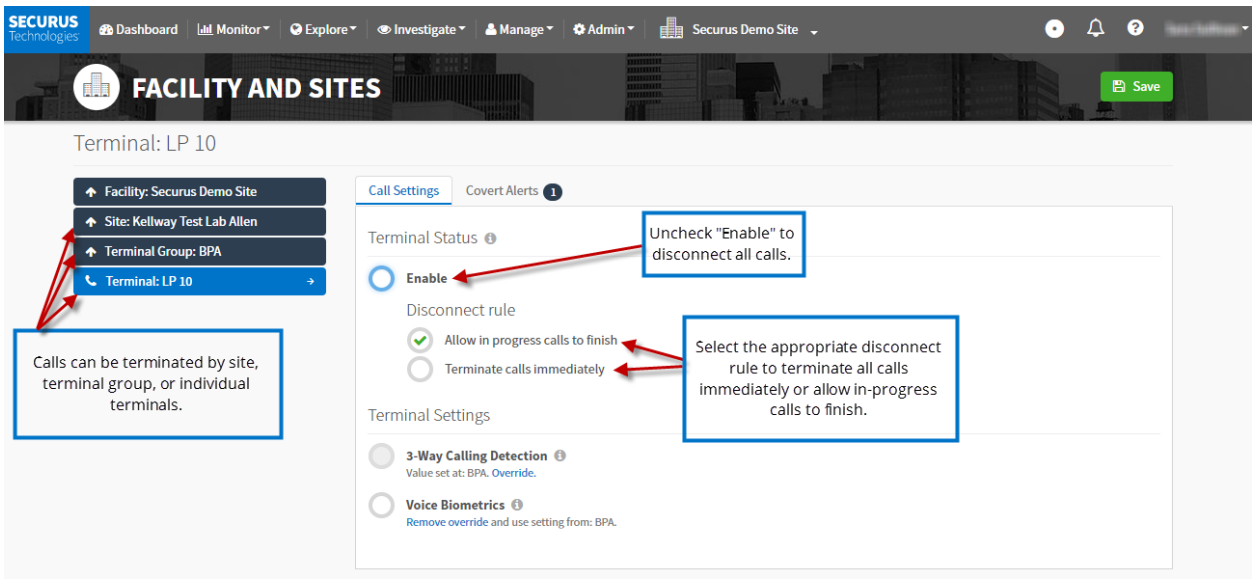
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will include cut-off switches at each demarc location, central control centers and select housing units to allow for manual cut-off of the NextGen SCP system

Authorized DOC staff can also disable a telephone, group of telephones, or all facility phones using any personal computer with access to the NextGen SCP via internet access.

This software function allows authorized users to either kill the calls immediately or allow current calls to finish while not allowing any new calls.

Disabling Telephones



H. The ITS will be able to take an individual telephone out of service without affecting other telephones.

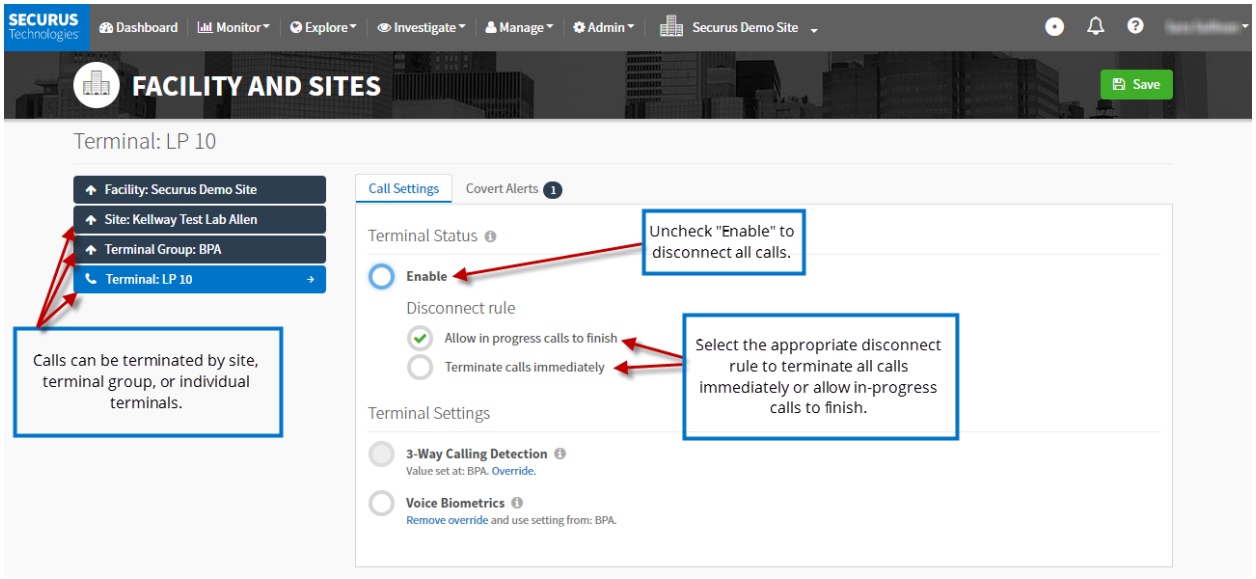
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The same on/off station controls that allow DOC staff to shut down the ITS also allow authorized users to take an individual phone out of service without affecting other telephones.

NextGen SCP allows authorized users to disable a telephone, group of telephones, or all facility phones using any personal computer or mobile device with access to the Internet. This capability is available anytime, from anywhere, **24x7x365**.

This function allows authorized users to disconnect all calls immediately, or allow current calls to finish while not allowing any new calls.

Disabling Telephones



I. The ITS will not process incoming calls at any time. The Offeror will agree that no offender telephone will be capable of receiving an incoming call and the Offeror will work with the local exchange carriers (LECs) to ensure such control.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP will not process incoming calls at any time. To ensure maximum security to the system, Securus provisions the trunks in the Secure Call Platform (SCP) data center as outgoing only, ensuring that no incoming calls can reach the offender.

Securus has performed full testing of these trunks, verifying compliance with this requirement.

J. The Offeror will describe how it detects "false disconnects".

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides some of the most advanced fraud detection and false disconnect capabilities in the corrections industry. NextGen SCP™ continuously analyzes call data and system parameters to detect anomalies, hardware failures, fraud indications, or unusual usage patterns.

NextGen SCP will provide, at a minimum, the following false disconnect aids:

- Detection of three-way calls (patented)
- Detection of call forwarding

Voice Quality

False disconnects are minimized and more easily detected by using a mixture of G.711 and G.729a signaling protocol, we dedicate enough bandwidth for each conversation over our dedicated network to keep packet delays under 100 milliseconds. This can achieve a Mean Opinion Score (MOS) of 4.3—better than digitized telephone quality.

K. The ITS will have the capability of answer detection.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP uses accurate answer supervision/detection. The Securus calling service requires active "called party" acceptance using touch-tones to complete calls. When the called party answers the phone, the calling service's answer detection triggers the call acceptance voice message. This message announces the offender's call and asks the called party to accept or reject the charges of a collect call. The called party is instructed to dial a single digit on their telephone to accept the collect call charges, or hang-up to disconnect the call and refuse charges.

L. The Offeror will describe its answer detection methodology.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our calling service uses call progression technology and other detection techniques to validate each call answer-and-acceptance event (See response to 3.9.12 above). The feature also enables the system to state the specific reason for the call termination when an offender's call does not complete.

For a call between an offender and a called party to take place, a valid call answer-and-acceptance must occur. The system must distinguish between legitimate call acceptance and other telephone activities such as:

- Network ring/busy signals
- Answering machines
- Operator intercepts
- Signal Interface Tones (SIT tones)
- Pagers
- Hacking
- Chain dialing

M. The offender's call will be muted until the called party has positively accepted the call. The ITS will not allow the offender to hear the called party prior to the actual positive acceptance of the call.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Mute Acceptance and Call Progression feature in Securus' calling service can be configured to allow the offender to either mute or hear call progression.

NextGen SCP™ is initially configured to always mute the offender's line until the system detects positive acceptance by the called party. The offender can never speak to nor hear the called party until the called party positively accepts the call. This applies to both collect and prepaid calls.

N. The ITS will be capable of limiting the length of a call, providing the dial tone at certain times of the day and allowing a maximum number of minutes per offender, per month.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP's Programmable Call Duration, Calling Schedules, and Calling Restrictions features provide DOC staff with the necessary capabilities to limit the length of a call, provide the dial tone at certain times of the day, and allow a maximum number of minutes per offender, per month.

Programmable Call Duration

NextGen SCP™ can be used to set a maximum time limit for any or all calls related to either an individual PIN or all PINs. The calling service will then automatically manage all imposed durations, reducing the workload for facility personnel.

The system will give the offender a verbal announcement one minute prior to end of their call and then enforces the facility policy with a hard stop.

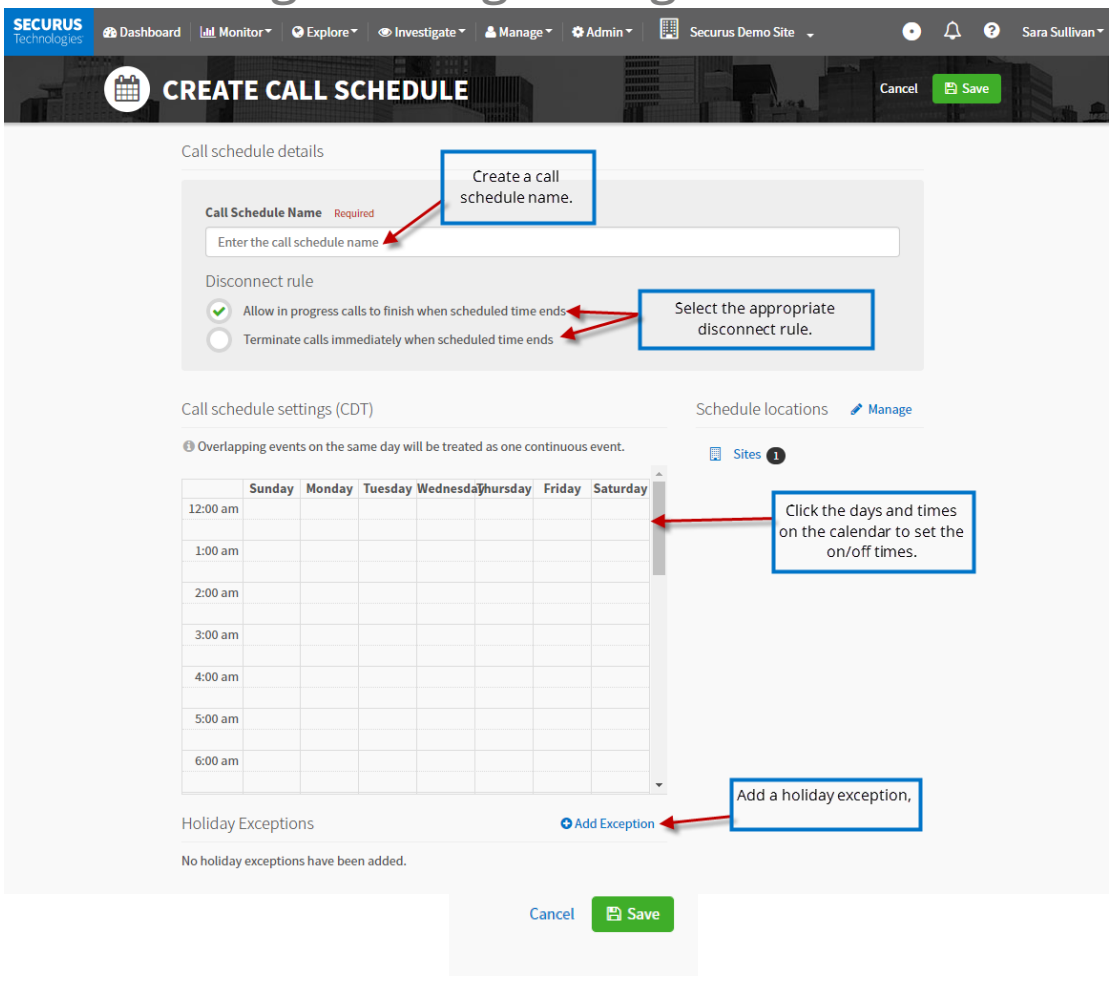
Programmable Calling Schedules

NextGen SCP™ calling services has an automated calling schedules feature that allows the system to enforce the scheduling policies of the facility without staff intervention. Calling schedules are used to turn on and off the phones during designated times throughout the day or night.

Calling schedules are flexible and configurable allowing the facility to have multiple on and off times during the day, within a week and by day of the week and then be applied to individual telephones, groups of telephones, individual offenders and/or globally.

Also, holiday overrides can be preset to accommodate anticipated exceptions to the set schedule.

Programming Calling Schedules



Programmable calling schedules are responsive to and overridden by both the manual cut-off switches located within the facility and the Call Settings Disconnect Rule.

Programmable Call Restrictions

NextGen SCP™ provides calling restrictions to give CDOC control of calling activity at the offender, port, phone group, facility, or customer level. Multiple restrictions can be crafted within each restriction set.

Examples of call restrictions are:

- Maximum number of calls per day/week/month
- Maximum type of calls per day/week/month

- Maximum number of call connects, accepts and/or mins of talk time

All imposed calling restrictions are automatically managed by the NextGen SCP system to relieve facility staff of calling restriction enforcement responsibilities.

Restrictions may also be used for punitive measures or behavior modification by restricting access versus revoking complete access as done through suspension.

O. In all circumstances, the ITS will limit the offender to a single call request. The ITS will always require the offender to disconnect and initiate another call.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP limits the offender to a single call though the dual-tone-multi-frequency (DTMF) detection fraud prevention tools. The system, by default, does not allow the offender to press additional digits, which makes it impossible for offenders to receive a secondary dial tone or call anyone by dialing additional digits after call connection or call disconnect.

The system uses our patented DTMF collection techniques to collect and only act upon digits that the system is expecting. For example, when SCP asks for language selection it expects a one-digit answer; when asking for a PIN it expects the maximum PIN length.

The system does not expect digits after call connection and will not accept any extra pressed digits to initiate another call unless the first call is disconnected.

P. The Offeror will provide information on any additional or optional features, investigative or management systems or tools provided that may be of interest to the CDOC (i.e. word recognition/keyword search, reverse look-up, visitation telephone recording, pattern analysis, digital forensics, etc.). Please ensure a complete description of the features of the application is included.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is uniquely equipped to provide a full spectrum of civil and criminal justice technology solutions, including new technology, investigative tools, and management systems. From public safety incident response to post-incarceration community supervision— and all points in between—only Securus can provide more options to customize any given technology for the corrections environment means a more efficient, cost-effective system that creates value and opportunity for The State of Colorado.

Features Designed for Corrections

Only Securus is a true technology company. We invest heavily in technology and lead the market in innovation. We have more patents than the rest of our industry combined.

Over the past five years, we have re-invested over $1 billion in technological advancements. We do this because we believe technology has — and will continue to — revolutionize the corrections experience creating safer facilities, reducing recidivism and increasing operational efficiencies.

Securus has the widest variety of corrections solutions that reduce operational workload, increase safety & security, and provide staff and offenders unprecedented communication access. Our commitment to technology means that we'll continue to innovate and provide you with cutting-edge solutions, now and throughout the term of our agreement.

The Securus proposal includes the following additional and optional features, investigative systems, management systems and tools that may be of interest to the DOC. Certain services and technologies do have associated costs and are included in the cost proposal:

Investigative Solutions:

- **Investigator Pro (IPRO) Continuous Voice Identification**— Integrated with NextGen SCP, IPRO includes robust reporting of all offenders on a phone call using continuous voice identification and voice biometric technology
- **ICER - Offender to offender Communications Detection**— Identifies offender-to-offender communications wherever and whenever they happen. Automatic detection and reporting of conversations between offenders within a facility or between facilities when offenders are calling same or different numbers.
- **Word Alert –**Speech-to-text transcription and keyword search tool for corrections agency investigators. It automatically transcribes all communications to text.
- **THREADS - Data Analytics and Pattern Analysis**— Analytical software integrated into NextGen SCP with automatic upload and analysis of calling records, trust account funding data, along with easy import of retrieved contraband cell phone data - plus much more

Advanced Investigation & Intelligence Professional Services

- **Dedicated On-Site Investigative Staff**
- **Hourly Professional Services**— Customized onsite or remote investigative assistance using experienced call monitors, certified forensic analysts and proprietary software and hardware solutions to identify actionable intelligence based on client investigative priorities.
- **Human Trafficking Investigative Service**
- **Centralized Forensic Lab & Customer Specific Forensic Lab Services** — Allows for customer specific forensic lab of dedicated/certified forensic technicians, including all standard hardware and software. Can also provide data extraction for shipment of confiscated contraband cell phones and computers to a centralized forensic lab

Contraband Cellular Interdiction Service

- **Contraband Cell Phone Detection**— Deployment of ferromagnetic detection devices to identify contraband cell phones and metal
- **Mobile Contraband Cell Phone Assessment**— Assessments provide actionable intelligence by identifying and reporting on contraband cell phones determined to be within a correctional facility
- **Wireless Containment Services (WCS)**— WCS (aka Managed Access) type contraband cell phone solution which provides dashboard and rich investigative intelligence from use of contraband cell phones in facilities; also blocks calls from leaving facility.

Corrections Solutions:

- **Automated Information Services**— Automated Interactive Voice Response (IVR) system for auto answer of routine questions, with optional voicemail and trust and/or account funding.
- **Dedicated On-Site Administrators –** Securus can provide personnel assigned to facilities to managing communications systems and tablets.
- **Visitation Phone Monitoring**— Visitation Phone Monitoring (VPM) deployment includes enhancing security and investigative capabilities for onsite visitation. The enhancement introduces the deployment of SCP call monitoring and recording of non-contact visitations where visitors are only allowed to use a telephone handset to communicate with an offender using another handset

while looking at each other through a glass or Plexiglas partition. Installation includes new wiring to connect the visitation stations to the SCP platform.

- **Phone Calling with Tablet**— Deployment of tablets and associated wireless network will allow for a phone calling application to be placed on the tablet, giving offenders the ability to make SCP phone calls, with retention of the same security features as calls placed from traditional phones hanging on the walls.
- **Video Remote Interpretation**— VRI is an on-demand service that provides communication between deaf or hard-of-hearing persons and hearing persons that are in the same location, utilizing an interpreter by way of a stationary or mobile video enabled kiosk or computer device.
- **Inbound Voice Messaging**—Allows offenders to receive secure inbound voicemails from friends or family members.

Post Incarceration Services

- **Securus SMS Re-Entry Tool** – Our SMS reentry tool is the first in may steps to provide easier access to needed services and rehabilitation.

INVESTIGATIVE SOLUTIONS:

Investigator Pro

Investigator Pro™ (IPRO) is the most powerful voice biometrics solution in the corrections industry. It is currently installed at several hundred state, county, and local agencies across the United States.

IPRO includes a wide range of tools that identify voices by name, deter offender PIN abuse, and provide leads for investigators to identify and prevent illegal activity carried out over the offender telephone system. It is fully integrated with the Securus communications platform and is hosted in Securus' data centers. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.

Investigator Pro Advantages

Investigator Pro provides these advantages for the agency and its investigators:

- A choice of offender enrollment methods - supervised or covert - with the ability to mix the two or change from one to the other at any time.
- Real-time initial pre-call PIN check voice biometrics to reduce PIN theft.

- Continuous voice biometrics throughout the call to identify offenders by name no matter how many offenders are on the call or whose PIN was used.
- Ability to identify called parties by name when they are known to the system, to help find calls to released offenders.
- Voice search for offenders and called parties on both sides of calls using voice samples taken from either side.
- Offender-to-offender communication reporting through the seamless integration of ICER™, the Offender Intercommunication Evaluation and Reporting System, into IPRO.
- A call player rich in features such as the ability to skip pauses, control playback speed, mute one side, and learn more about the voices on the call.
- Ability to add custom gang information and high-interest group labels to offenders and phone numbers, and to search on that information.

Offender Enrollment Method Choices

The agency can choose supervised or covert enrollment to create a voice-ID/PIN pair for each offender. It can switch from one method to the other at any time. It can also choose to enroll existing offenders covertly and new ones through a supervised process.

Supervised enrollment creates a staff-verified voice sample for each offender ID/PIN. Investigators then have a known audio file of each offender to play. In covert enrollment IPRO learns a voice and associates it with an offender ID/PIN. There is no staff involved and offenders are not asked to record their voices. Offenders are unaware of when and how covert enrollment occurs.

Pre-call PIN Check Voice Biometrics

IPRO's real-time pre-call PIN check feature, which the agency can elect to enable or not, reduces PIN sharing and theft. When an offender begins a call IPRO verifies in real time that the offender's voice matches the sample associated with the ID/PIN used to make the call. If it does, the call goes through. If not, the call is blocked.

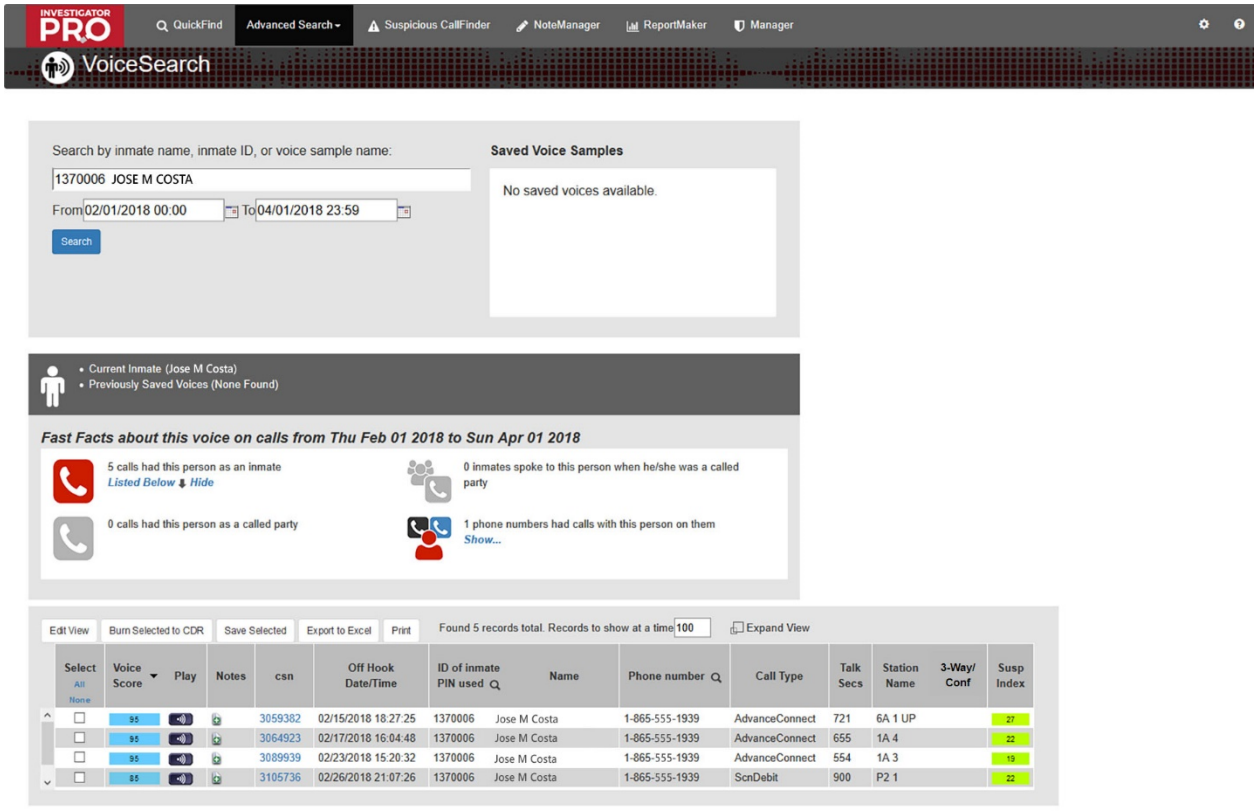
Continuous Voice Identification

Investigator Pro does continuous voice identification throughout a call. It identifies all the speakers on the offender side of the entire call by name, no matter how many there are, which one started the call, or whose PIN was used. It covers 100% of every call without tipping off the offender(s) or called party. IPRO constantly "learns" and improves its voice identification accuracy. IPRO identifies called party voices by name when the names are known to the system, as in the case of released offenders.

Voice Search

The investigator can search for calls that have a particular voice on the offender or called party side of the call. He can do a voice search by offender name, offender ID, or a voice sample that he saved from either side of a call in the call player. Search results include facts about that voice on those calls. With just a click the investigator can get a listing of the calls, offenders, or phone numbers involved

IPRO Voice Search



Voice search results include facts about the voice and links to the relevant calls, offenders, and called phone numbers.

Identification of Likely PIN Abusers/Imposters by Name

Investigator Pro flags calls that are likely cases of PIN sharing/theft. It names the likely imposters and gives the investigator tools to pursue those offender names, calls, and voices further.

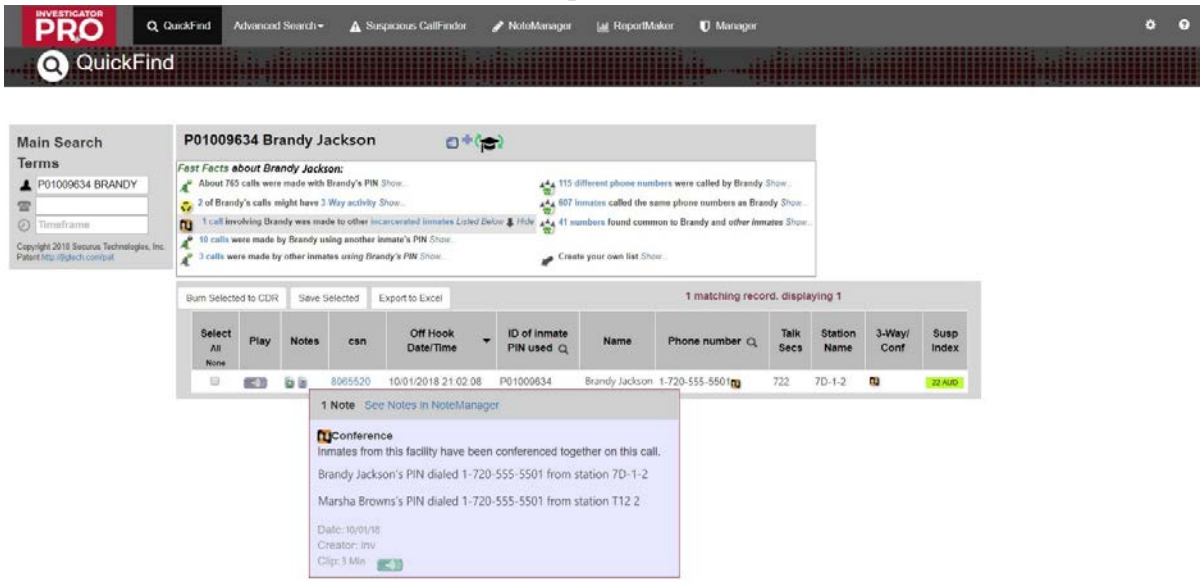
Offender-to-Offender Communication Reporting

IPRO detects offender-to-offender calls no matter how or where they happen, because ICER, the Offender Intercommunication Evaluation and Reporting System, is integrated

into Investigator Pro. ICER finds these calls whether the offenders are within a facility or in different facilities across the country, and whether the two offenders called the same or different outside numbers to make the connection.

IPRO puts ICER information at the investigator's fingertips on the home screen, in the results of call and offender searches, and in the call player.

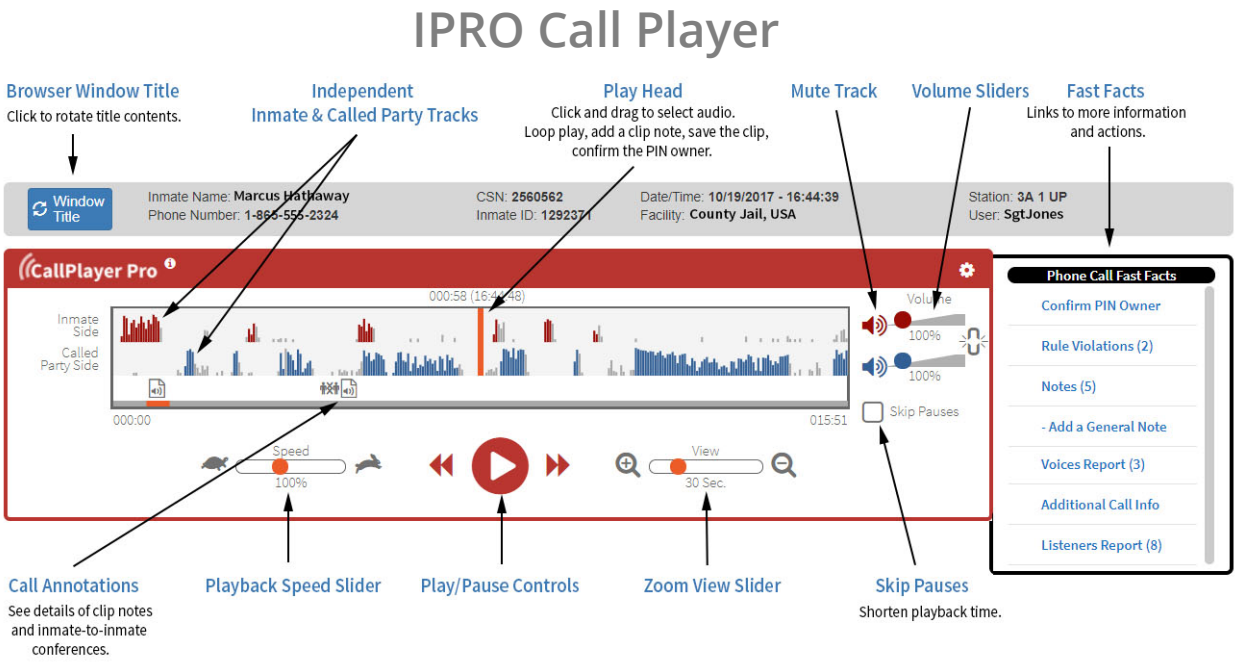
IPRO Quick Find



An offender search from the home screen gives valuable information, including details about offender-to-offender calls.

Call Player

Investigator Pro has a full-featured call player that makes listening to offender calls quick and easy. Some of the things investigators can do in the call player are: skip pauses, mute either side of the call, slow down/speed up playback, create audio clips, create and distribute call and clip notes with case numbers and category assignments, learn about the voices on the call, save voice samples for later voice searches, and learn about any rule violations on the call.



Investigator Pro's call player makes listening easy and efficient. The Fast Facts box beside it has links to more information and actions for the investigator.

3-Way Call Detection

When IPRO suspects 3-Way activity on a call it flags it in the call player and in lists of calls.

Database Search

Investigator Pro has a large database of information about calls, offenders, voices, and telephone numbers. Investigators can search the database by criteria such as offender name, offender ID, date range, saved voice sample, custom High Interest Group label, offender-to-offender (ICER) calls, 3-Way calls, originating station, and case number.

Custom High-Interest Group Labelling

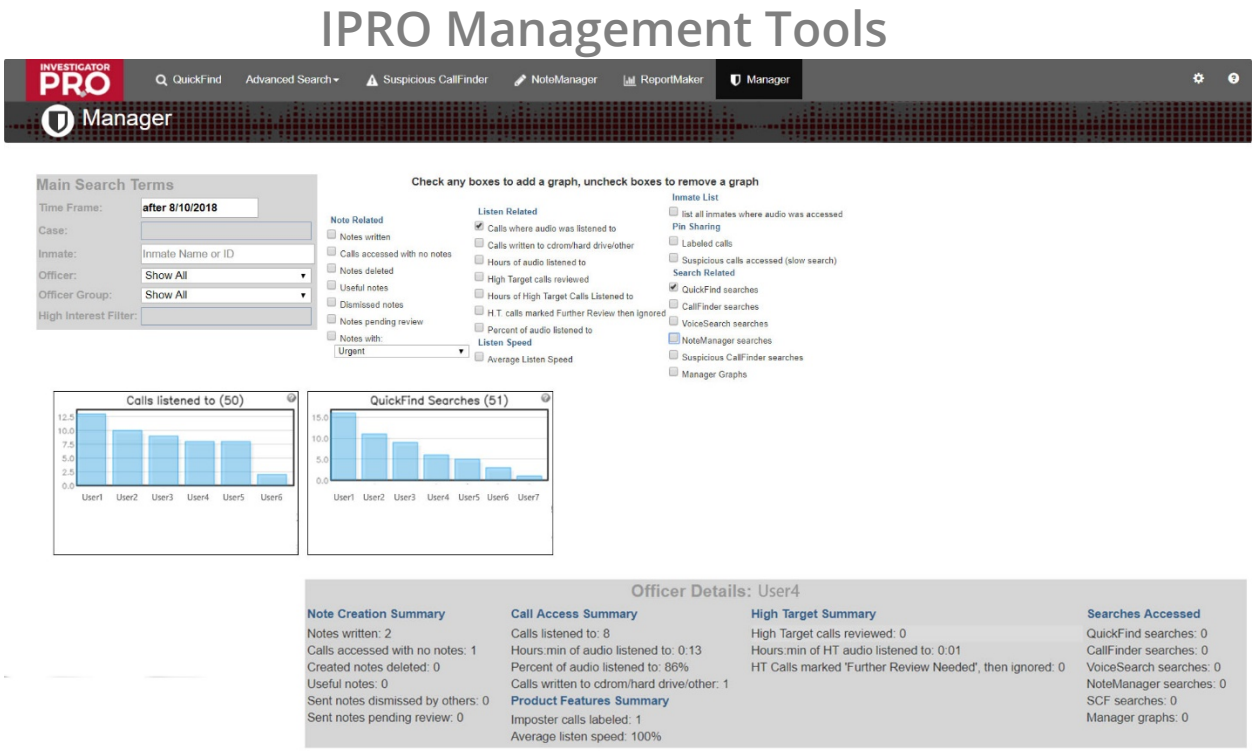
Investigator Pro lets investigators add their own information to the database and find it in searches later. They can tag offenders and phone numbers with their agency's own custom High Interest Group labels. They can also add notes and case numbers to calls, identify and label imposters' voices in cases of PIN abuse, and confirm the voices of PIN owners on calls.

Custom Gang Data Feeds

IPRO can be customized to automatically import the agency's own gang data, removing the need for investigators to manually add High Interest Group labels to offenders and called numbers.

Management Tools

Investigator Pro has management tools such as role-based access permissions, the ability to see officers' use of individual IPRO features, and the ability to create, organize, search for, and forward notes on calls/call clips.



Agency management can readily see any officer's use of the different features in Investigator Pro.

Reports

Investigator Pro can generate many useful reports with data such as pre-call PIN check results, likely PIN abusers, the most common called party numbers, and IPRO's voice learning results.

ICER – Offender to Offender Communication Detection

Offenders are continually finding creative ways to speak to each other using the offender phone system, and ICER listens to and identifies these illegal communication events. Whether two offenders are calling an accomplice on the outside who is verbally relaying messages, or the accomplice has two speakerphones to coordinate gang conference calls, ICER identifies all of these scenarios and proactively notifies all authorized corrections staff of the event and provides details that can quickly and easily be traced back to a specific call. This call can then be listened to through Securus' industry-leading platform.

ICER uses advanced voice analysis technology to generate a call signature for each completed offender telephone call. Call signatures are then automatically encrypted and transmitted to the central data center for analysis. Because none of the original audio is used in a call signature, the ICER system is in full compliance with state laws regarding the transmission of call recordings. At the data center, the call signature is analyzed and checked against other call signatures. If an offender-to-offender communication is detected, it is logged in the ICER system database and investigators from the participating corrections administration are automatically alerted via email to log into the ICER system for the detailed report.

Sample ICER Reports

ICER Event Report

Event Identified On: Feb 07, 2022
09:46 am (CST)

An Inmate Inter-Communications Event has been detected involving an inmate at your facility. The details of which follows below:

Inmate		
Agency	NEVADA DOC NV	NEVADA DOC NV
Site	Lovelock Correctional Center, NV	Northern Nevada Correctional Center, NV
Inmate ID		
Called Number		
Station Name	UNIT 3A - East Phone	LP 77
Call ID		
Call Start Time	Feb 06, 2022 09:47 pm (CST)	Feb 06, 2022 09:52 pm (CST)
Time into Recording (H:M:S)	06m:24s (384 sec)	01m:17s (77 sec)
Duration of Event (H:M:S)	13m:59s (839 sec)	13m:59s (839 sec)

ICER Event Report

Event Identified On: Feb 06, 2022
03:15 am (CST)

An Inmate Inter-Communications Event has been detected involving an inmate at your facility. The details of which follows below:

Inmate	JOHNSON, TERRANCE	JACKSON, ISRAEL
Agency	IL DOC IL	NEVADA DOC NV
Site	Western Illinois Corr, IL	Southern Desert Correctional Center, NV
Inmate ID	R53900	1199052
Called Number	17732323738	17252081048
Station Name	HU 4 B P4	Unit 12 B-3
Call ID	15937761289	15937757688
Call Start Time	Feb 05, 2022 11:43 am (CST)	Feb 05, 2022 11:44 am (CST)
Time into Recording (H:M:S)	03m:07s (187 sec)	01m:10s (70 sec)
Duration of Event (H:M:S)	01m:21s (81 sec)	01m:21s (81 sec)

Word Alert

Securus Word Alert is a powerful speech-to-text transcription and keyword search tool for corrections agency investigators. It automatically transcribes all telephone calls and SVC video sessions to text. Investigators can search the transcripts for words and phrases either interactively or by setting up automated, continuous scans that send them alerts when matches occur.

Word Alert helps investigators quickly zero in on the calls and sessions most likely to have investigative value. Investigators can save time by skimming a transcript or jumping to matching search terms rather than listening to the whole call or session. They can quickly get an English translation of a non-English transcript. They can uncover

individuals who are talking about topics of investigative interest. Intelligent analytics reveal topics now being talked about in the facility more than in the past, uncovering problems before investigators know to look for them.

It is integrated with the Securus NextGen Secure Communications Platform. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.

Word Alert Capabilities

- Automatic speech-to-text telephone call and SVC video session transcription - transcript of each telephone call and video session is available in minutes in its original language. *
- An English translation can be requested and displayed in seconds in line with the original language text. *
- Transcripts aligned with the audio and video player - Investigators can view a transcript alone or aligned with the audio or video player while the call or session plays. Search term matches are highlighted in the transcript.
- Dictionary of search terms - Investigators can manage a dictionary of word and phrase search terms, in any language, and create categories of search terms.
- Reports - Interactive, ad hoc searches let investigators find words and phrases in past calls and sessions.
- Automated scans constantly search new calls and sessions for target words and phrases and send alerts to investigators when matches occur.
- Integrated audio and video players can control playback speed and volume.
- Interactive searches of past calls and video sessions - Search results can be exported to downloadable reports.
- Analytics include search term category frequency graphs and totals.
- Identification of Trending Topics - Word Alert's intelligent, behind-the-scenes analysis uncovers trending topics of conversation on calls and sessions in the facility.

* The supported languages for transcription, and for translation to English, are Bengali, English, French, Italian, Korean, Mandarin Chinese, Polish, Portuguese, Russian, Spanish, and Vietnamese.

Automatic Speech-to-Text Telephone Call and SVC Video Session Transcription

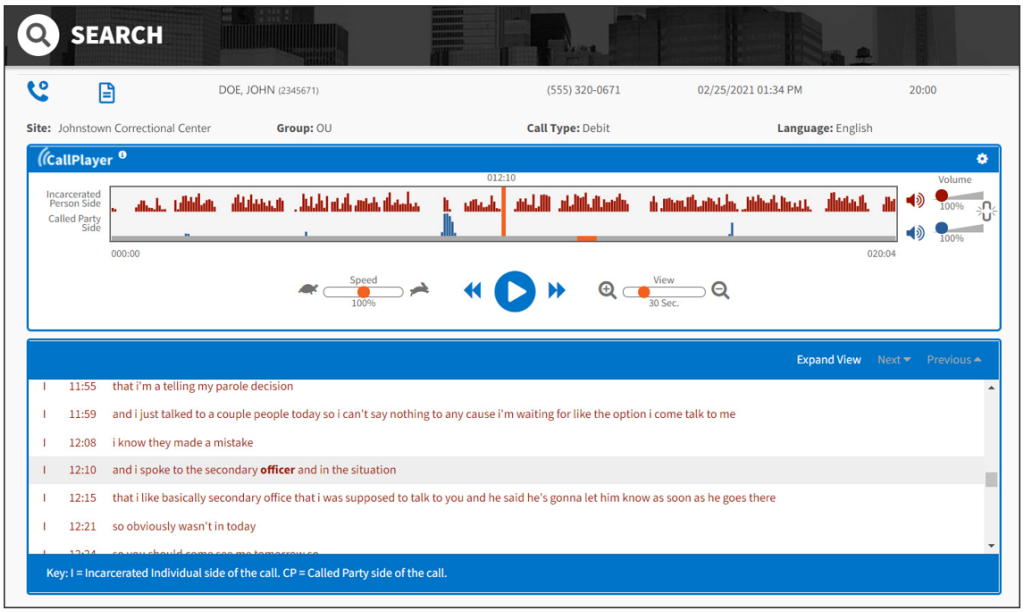
Telephone calls and SVC video sessions are automatically transcribed to text within minutes after they end. There is no need to select any for transcription. Each text

transcript is in the language the offender used when starting the call or session. Transcripts are stored in accordance with the agency's call and video session retention policies.

WORD ALERT – KEYWORD SEARCH AND TRANSCRIPTION

INTELLIGENCE
Investigative solutions

THE KEYWORD IS HIGHLIGHTED IN THE TRANSCRIPT. THE AUDIO CALL PLAYER IS POSITIONED AT THE SAME LOCATION IN THE CALL.

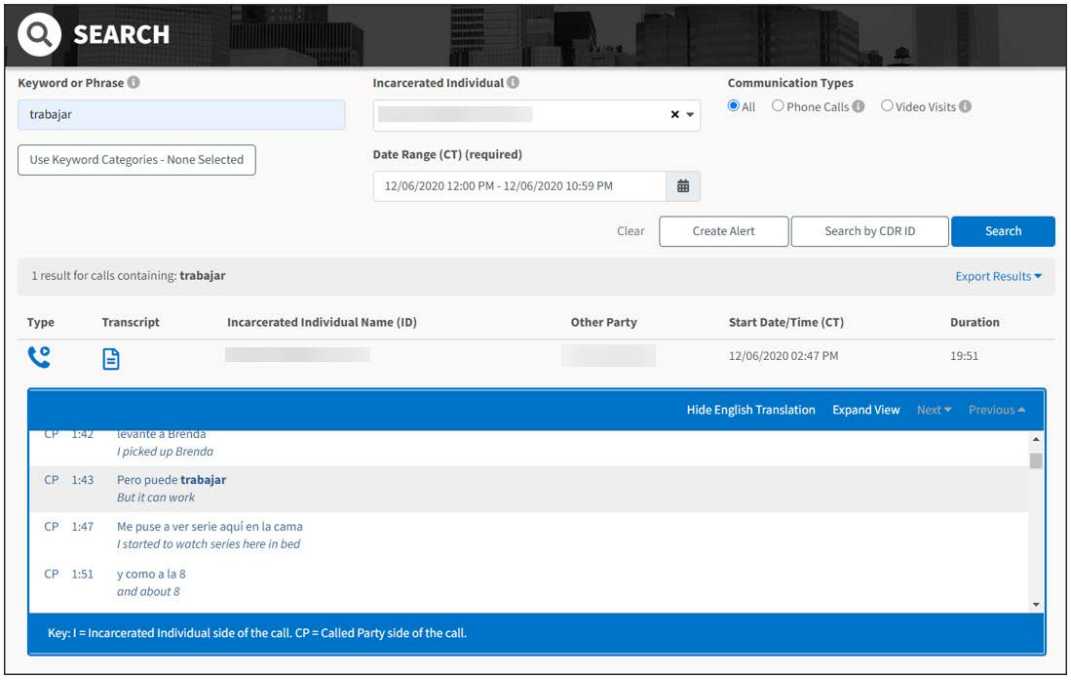


SECURUS Technologies

Rapid Translation to English

The investigator can request an English translation of a non-English transcript with just a button click. The translation appears in seconds with each line under the original language line in the transcript. The English translation is stored with the original transcript for future reference.

Sample Word Alert Translation



Transcript Aligned with the Audio and Video Player

A transcript can be viewed alone or aligned with Word Alert's audio or video player. Any search term matches are highlighted in the transcript. The investigator can jump to a section of interest in either the player or transcript and the two will move in tandem to that section. In the transcript they can jump from any search match to the next or previous match, and the player will move to that location.

Dictionary of Search Terms

Word Alert has an editable dictionary of words and phrases that can be used as search terms. Investigators can add terms in any language and create categories of terms. Individual terms, or entire categories, can be used in searches.

Interactive Searches of Past Calls and Video Sessions

Word Alert makes it easy to do one-time, interactive searches of past calls and video sessions using a date range and words, phrases, and categories of terms in any language. The search can be narrowed by offender name or ID and communication type, i.e., telephone calls and/or video sessions. Results are displayed as a list of calls and sessions, each with clickable icons to show the transcript alone or with the player.

Automated Searches of New Calls and Video Sessions with User Alerts

Word Alert lets investigators set up automated scans that continuously monitor new call and video session transcripts as they come into the system. An alert is sent each time a search term match occurs in a call or session. The investigator configures an automated scan with search terms in any language and optionally with an offender's name or ID, as well as the communication type. They can also include an end date if they choose.

At any time, the investigator can see the total number of alerts triggered so far by the scan. They can review the calls and sessions that triggered the alerts and can also stop the scan at any time interactively.

Search Results with Snippets and Highlighted Matches

Calls and video sessions with matching search terms are each listed with their communication record information: name of the offender, dialed telephone number, communication start date and time, and communication duration. Each record also shows a player icon and a transcript icon. Hovering over the transcript icon brings up one or more snippets from the transcript. The snippets show the search term matches in the transcript. The investigator can quickly decide whether to bypass that call or session or investigate it further. They can click on the transcript icon to open the full transcript, or the player icon to see the transcript with the player. The matching search terms are highlighted in the transcript.

Integrated Audio and Video Players

The integrated audio and video players have user controls to regulate playback speed and volume. The audio player also allows the investigator to mute either side of the communication independently. In both players, the transcript and player are aligned when they are displayed together. The investigator can play any portion of the call or session and read its transcript as they listen. Changing the location in either the player or the transcript changes it in both simultaneously.

Reports

The results of an interactive or automated search can be exported to a report and then downloaded. The report lists calls and video sessions that had matches, with communication record information for each one.

Analytics

Intelligent analytics reveal what people in the facility are talking about on telephone calls and video sessions without investigators having to do searches. In Analytics, the

Keyword Categories screen shows how many times, and on which calendar days, words in each of the dictionary's categories occurred. The Top Keyword Trends screen shows additional words that Word Alert discovered on its own that are occurring in calls and sessions more often now than in the recent past. This trend information can uncover problems in the facility before investigators suspect they exist.

THREADS™

THREADS' powerful data analytics engine which imports and analyzes multiple types of facility data, such as incarcerated individual communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate focused leads for investigators. THREADS is extremely robust and accurate, but is extremely intuitive, and easy to use —making it a perfect tool for busy investigative officers operating within a correctional institution.

To assist in call auditing, THREADS:

- Quickly identifies common contacts between suspects
- Creates timelines that puts events in order
- Analyzes communication calling patterns
- Assemble data in graphical representations
- Highlights interesting correlations
- Establishes information sharing opportunities
- Imports and cross references additional data sets

Importing Information

THREADS automatically imports information from NextGen SCP's telecommunications database, incarcerated individual information from OMS, and financial data.

THREADS will automatically import the following types of corrections information:

- Incarcerated individual call records
- Incarcerated individual personal information, such as name, incarcerated individual ID number, PIN, DOB, SSN, and more
- PAN lists
- Called party billing name and address information
- Video visitation
- Suspicious activity, through IPRO and ICER for example
- Financial data

THREADS can also import the following types of information from external data sources:

- Confiscated cell phones—calls, text messages, emails, videos, contacts, etc.
- Public phone records
- Events and places of interest
- Mail
- LexisNexis

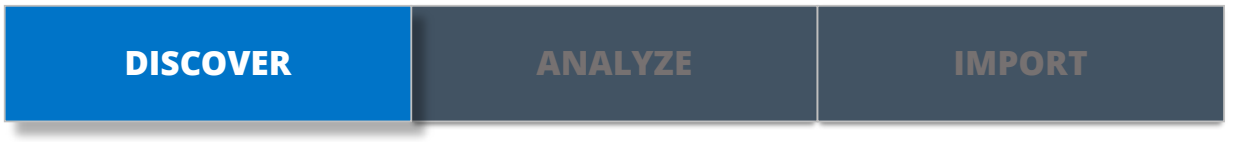
THREADS brings the power of Big Data Analytics to the investigative capabilities of correctional facilities, thereby reducing demands on Investigative personnel, while increasing their ability to identify potential criminal behavior. THREADS gathers and analyzes facility data, identifying actionable data that can be used as the basis of targeted criminal investigations.

Discover / Analyze / Import

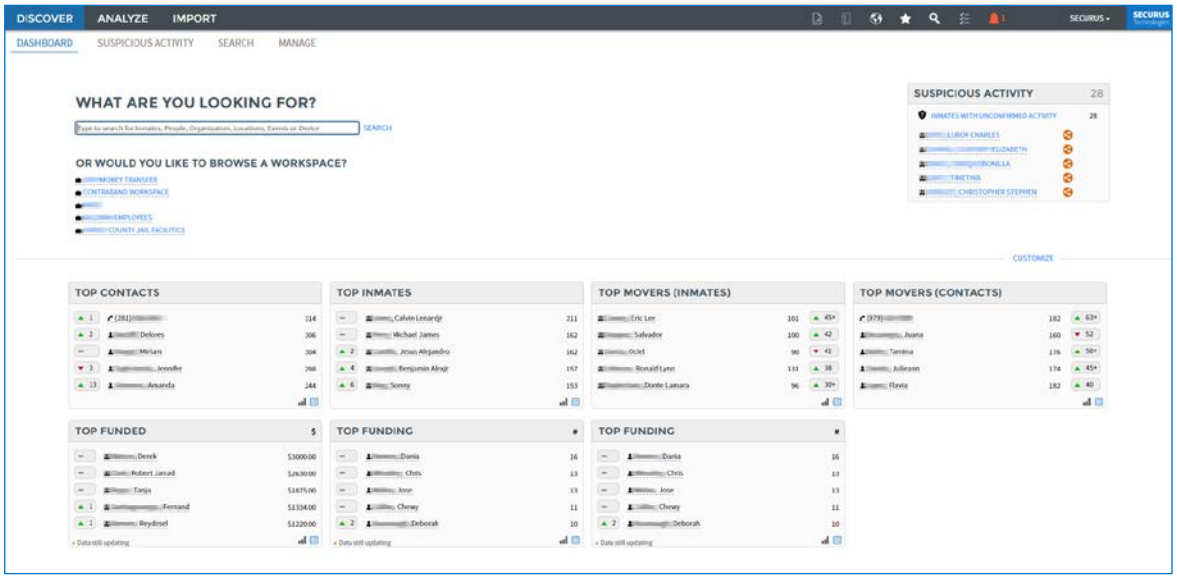
To make it easy and intuitive, THREADS is divided into three sections—**Discover**, **Analyze**, and **Import**. Each of three major activities are contained in each section, making it easy to identify which activity the investigator wants to initiate.

- **Discover**—Define, run, and view reports on information gathered and categorized by THREADS.
- **Analyze**—Define the types of analysis to be performed and runs the automated analysis built in THREADS.
- **Import**—Define sources of data to be automatically imported. This includes data from external sources, such as subpoenaed phone records; confiscated cell phone forensics; data extracted from OMS, RMS, and other systems and data.

THREADS *Discover* Landing Page (Dashboard)



DISCOVER Landing Page



Widgets

The **Discover** landing page shows customizable widgets allowing the investigator to set up information in a way that is most convenient to their investigative needs. These widgets default to the following categories: Suspicious Activities, Tasks, Top Incarcerated individuals, Top Contacts, and Recent Records.

Sharing Information through THREADS

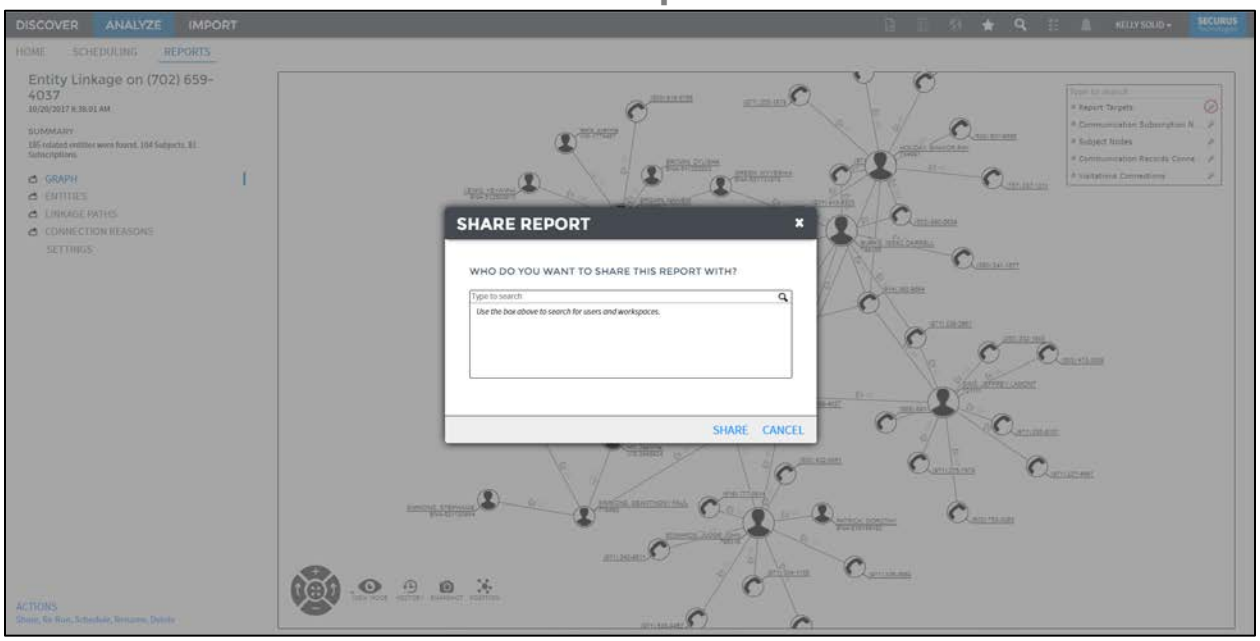
In addition to the NextGen SCP call record data and recordings, the DOC can elect to share THREADS data with partner agencies. THREADS is a powerful, accurate, easy to use, investigative tool that will automatically analyze data such as offender communication records, public phone records, and data from confiscated cell phones to automatically generate focused leads for investigators. Leads can include suspicious calling patterns, inner circles, communication events to numbers on a bounce list, associations between multiple offenders, correlations to called parties, and much more.

With THREADS, investigators can share information with other law enforcement agencies—including other departments, jurisdictions, and facilities—by granting secure

access to your data. Likewise, other agencies can grant your investigators access to their data.

THREADS has a “Shared Reports” capability allowing all authorized users—either within your facility or from other agencies—to share reports and analyses. Users can select other users with whom they wish to share results. In addition, they can allow other users to change report criteria or limit access to view reports only.

Shared Reports

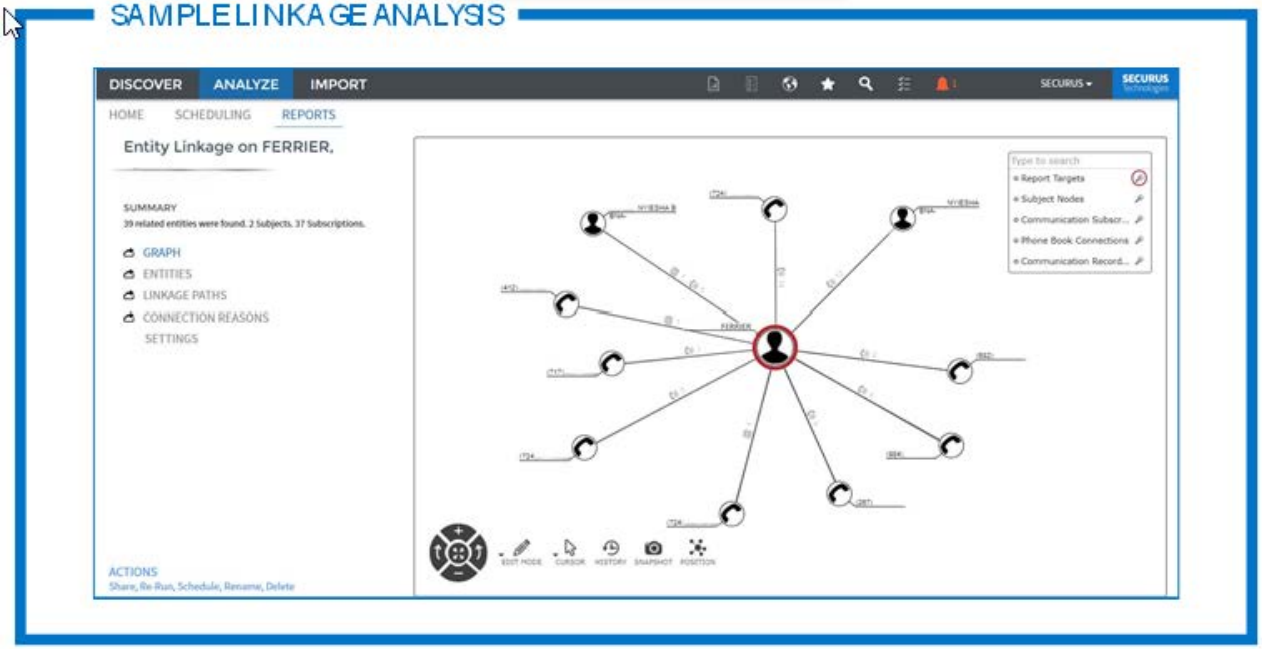


THREADS Reports

- **Statistical** - Includes all occurrences of a phone number or a bounce list of numbers in the database and the most frequently called numbers by an offender or person.
- **Linkage** - Shows how offenders and people are related. The reports in this section generate graphical results that let you explore the relationships between your targets. This visual reporting tool is a quick way to understand who offenders are talking to and how the calls are related to other known numbers or offenders.
- **Working Group** - Working Group analysis uses a person’s communication behavior and calling patterns to identify phone numbers and people of interest. By leveraging working group reports, facilities can identify gang and other organized activity.

- **Correlation** - Identifies common contacts and numbers between offenders, persons, and workspaces.
- **Time-Based Reports** - Provides reports based on the timing and frequency of an offender's or other person's communications.
- **Financial Reports** - Financial analysis identifies correlations between incarcerated individuals and people based on the funding of an incarcerated individual's accounts.

Sample THREADS Report



* The linkage chart identifies direct relationships between selected targets based solely on phone calls

ADVANCED INVESTIGATION & INTELLIGENCE PROFESSIONAL SERVICES

Securus can provide nationally recognized subject matter experts and specialists with extensive backgrounds in analytical analysis programs and development, policing, corrections (state and federal), and national security at the highest level. On the macro level they assist agency executive management with developing, building, or expanding intelligence programs through new technologies, strategies and methodologies which support agency success. They further support the agency by providing advanced technology support in terms of program integration and the development of new intelligence applications for existing Securus Technologies platforms or other platforms which support operational success. They have the proven ability to provide agencies with development or advanced case support with contraband cellular interdiction through signals intelligence and geospatial relationships.

Additional areas of Advanced Investigative and Intelligence Expertise

- Detection and identification of at-risk individuals which could compromise the safety and security of the correctional facility, it's staff, offender population and the public. Detection and identify Security Threat Group (STG) Leadership, STG membership and their co-conspirators operating inside and outside correctional facilities. Political, Socialist, Religious Extremism, Aggrieved Employees.
- Physical 3D Mapping of correctional facilities assisting with Critical Incident Management (CIM) and planning and response preparation for Emergency Response Teams (CERT/SORT).
- Provide law enforcement agencies with advanced cryptocurrency and financial investigations through training, education, and proprietary methodologies.

Dedicated On-Site Investigative Staff

Securus Technologies is in the business of assisting Investigators in Corrections with dedicated digital examiners and intelligence analyst support. These personnel are usually collocated with the State's Department of Corrections to assist in investigations to make for a more safer prison environment.

The lab investigative staff will assist jail and prison investigators with the following:

- Assist in investigations of incarcerated individuals, public safety and security
- Develop actionable intelligence
- Provide staff augmentation providing direct savings to the customer
- Provide expertise resulting in strategy development while maximizing departmental use and benefits
- Develop policy and procedure collaboration to drive operational efficiencies

Hourly Professional Services – Advance Intelligence Experts

The advanced investigative and intelligence services listed above can provide both remote and dedicated at an hourly professional services rate to build complete intelligence ecosystems utilizing Securus Technologies legacy intelligence platforms combined with new advanced technologies, strategies, and methodologies. The ecosystem approach allows Securus to assist in guiding agencies decision makers to make proactive, informed intelligent decisions on three levels: 1. Strategic 2. Operational 3. Tactical with advanced intelligence reporting.

Human Trafficking Investigative Service

Securus' has partnered with human trafficking experts in the law enforcement community to provide an investigative service focused on identifying human traffickers and returning their victims. The service includes investigative support to provide high value leads targeting sex trafficking by utilizing correctional data including, but not limited to, incarcerated call recordings, video visitations, emails, and financial activities.

- **Securus Technologies advanced investigative and intelligence team has developed a patent pending Human Trafficking Program which assists agencies in detecting and identifying human trafficking activity.**
- **The source material, which is specific to corrections and jails, combined with Securus' proprietary methodologies are the key components of the architecture, which provides the agency with a turnkey intelligence program that is sustainable and scalable. The program can stand alone or support other local, state, and federal law enforcement partners.**
- **This program is one of the first in the nation that allows the agency to take a proactive stance by identifying offenders who are potentially at risk for being groomed by human traffickers and their co-conspirators.**

This data, coupled with Securus' investigative suite of products and our proprietary trafficking investigations process, provides valuable insight into the high-profile, nationally focused efforts to end of sex trafficking.

Centralized Forensic Lab & Customer Specific Forensic Lab Services

Securus Technologies provides centralized forensic lab services that focuses on investigative tools and strategies that aid the State Department of Corrections and other law enforcement and intelligence fusion centers around the country to gather intelligence. Our forensic lab services provide a comprehensive and analytical breakdown of cellular data utilizing Cellebrite and numerous other computer forensic programs (Encase, Internet Evidence Finder, Passware, Oxygen Phone Forensic Suite, Forensic Explorer) that are also able to perform in depth forensic analysis on acquired devices as well as any form of digital media. The combined experience of our Forensic Staff along with the Industry Leading Hardware and Software ensures that the highest quality of Digital Forensic Services on mobile devices, and any digital media, will be of the highest standard. Our Georgia Forensics Lab that supports the Georgia Department of Corrections is accredited by the ANSI National Accreditation Board (ANAB). Our goal is for all our labs that supports our customers will be accredited.

Securus Technologies offers other customer specific forensic lab services to assist in investigations. Securus Technologies provide analysts that use the latest digital forensic technology to extract actionable intelligence to help prevent threats against public officials, harassment, and coordinated escape attempts. Typically, these digital forensics require a significant agency investment in equipment, training, and licensing; Securus makes it easy by doing the work for you and providing detailed reports. Our certified Forensic Examiners extract data from devices that are damaged, locked, or unsupported by other forensic tools. For the most severely damaged devices, we use methodology called Chip-Off Forensics to remove the flash memory from the printed circuit board. Then we read and analyze the raw data stored on the chip.

Specifically, Securus Technologies will provide the following Customer Specific Forensic Lab Services:

- Certified Forensic Technicians
- Dedicated professional forensics analyst
- Cellebrite Software Suite
- Chip Off Extraction Capability

- Certified Digital Forensic Services including cell phone data extraction and uploading of data into THREADS data analysis tool.
- Cellular Forensic Services – Supporting 4,000+ Device Types
- Maintained Chain of Custody
- A Forensic Process Upheld by the Criminal Judicial System

Contraband cellular interdiction services

Securus considers the following information regarding Kamea highly confidential and proprietary. This information has been submitted for CDOC to review and Securus respectfully requests that it be removed from our proposal prior to public display of proposals after opening.

Kamea

Kamea is sensor system that monitors radio frequency emissions from wireless devices within a controlled facility or a prison, utilizing proprietary proximity algorithms along with PDOA (power differences of arrival) technology.

- **Provides the agency with the location of the device(s) in near real-time within a correctional facility.**
- **Uses commercially available technology in conjunction with proprietary algorithms and/or other ancillary equipment to provide one of the most affordable cellular telephone interdiction solution**
- **Continuously monitors the RF environment within the facility and provides key indicators to the analyst for shakedown reports, number of devices seen at any one time, the location of devices seen and sometimes the actual type of device**

As a part of an installation, Securus can install equipment that will assist in the location of every tablet device in the facility. Using a proprietary technology, the Securus tablets are identified by our platform and their location proximity can be determined when they are powered on. The technology also gives us the incremental ability to see other devices broadcasting within the correctional facility, and as a result, this program can delineate between tablets and potential contraband devices that might be present within the facility. Not only can we help you locate tablets or authorized devices, but we can also assist in providing location proximities for those unauthorized devices within the walls of your facilities.

Below is an example of a test site that shows tablet location based on the KAMEA system.



Securus' KAMEA Contraband Interdiction Services is a service that uses RF sensors that monitors radio frequency emissions from wireless devices within a controlled facility or a prison, utilizing proprietary proximity algorithms along with PDOA (power differences of arrival) technology.

This service provides a situational awareness or near real-time high probability of the location of wireless devices within a correctional facility.

KAMEA uses commercially available technology in conjunction with proprietary algorithms and/or other ancillary equipment to provide one of the most affordable cellular telephone interdiction solutions to corrections; when combined with the Securus intelligence-led cellular forensics services, the combination gives the agency the upper hand in controlling contraband cellphones issues.

Below is an example of a test site that shows contraband based on the KAMEA system.



The KAMEA system and services continuously monitors the RF environment within the facility and provides key indicators to the analyst for shakedown reports, number of devices seen at any one time, the location of devices seen and sometimes the actual type of device, such as a Motorola cellphone located in Dorm A pod 1. See Remote Proximity Unit to the right.



System Functions:

- Detection of Cellular Telephones being used as Hot Spots
- Detection of Wi-Fi Enabled Cellular Telephones or other wireless Devices transmitting within the facility
- System-Wide Agency Implementation of an affordable Contraband Cellular Interdiction Program.
- Actionable Intelligence for Digital Forensic Lab, Investigators, and other Partner Intelligence Agencies.
- Total number of wireless devices active within the prison or assessment of the magnitude or number of wireless Devices present

- The KAMEA service offered includes hardware (Remote Proximity Units) for each controlled facility and a full-time analyst that provides situational analysis and identification of contraband cell phones and approximate locations for customer confiscation.

End Kamea proprietary and confidential section.

Mobile Contraband Cell Phone Assessment

Securus' Cellular Assessment Services assist the Department in identifying contraband cell phones within correctional facilities.

The service options available includes the deployment of RF based mobile assessment systems that are temporarily deployed at select facilities to capture, identify and report on all cell phones operating at a facility as well as handheld and fixed devices to augment staff efforts to detect and control contraband cell phones.

Cellphone Forensics services are also provided on any device uncovered or located by the assessment service to help support investigative and prosecutorial efforts.

Proximity, cross referencing with communications data and other investigative information is used to conduct and report on the contraband and assist agencies on the best approach to the issues the assessment uncovers.

Wireless Containment Services (WCS)

Securus Technologies advanced application group, I3 - (Investigations, Intelligence, and Insight), has developed a patented program which provides agencies with contraband cellular device intelligence which leads to proactive and predictive contraband (Cellular/Narcotics) interdiction.

The program can also aid in the detection and identification of individuals who at risk to compromise which could impact the safety and security of the correctional facility, it's staff, offender population and the public. This program can also detect and identify Security Threat Group (STG) Leadership, STG membership and their co-conspirators operating inside and outside correctional facilities.

Corrections Solutions

Securus Automated Information Services™

- 24-hour self-service access to current information with 99.9% uptime
- Significant cost savings and reduction in administrative burden
- Customize the configuration to meet the needs of your population

Securus Automated Information Services™ (AIS)—**an interactive voice response system (IVR) available to the CDOC population and the public 24x7x365**. There is no cost to call, and your normal telephone number will route to Securus AIS. 80-90% of all calls are resolved in less than 4 minutes with **no DOC involvement**. With a speed dial button on offender devices, most offender questions will also be resolved. Securus AIS is available when needed and with no wait time CDOC can **expect a 200% increase in calls answered!**

Securus Automated Information Services

Fast Facts 2018-2020

200+ Agencies Installed with AIS

$20.6+ Million in Estimated Cost Savings

25.3+ Million External Calls Answered

19.4 Million+ External Calls Resolved

9.0+ Million Inmate Calls Resolved

<75 Seconds Average Call Time for Resolved Calls w/ 80-90% of Calls < 4 Min.

460,000+ Account Funding Transactions Processed

Securus AIS updates every 15 minutes with CDOC systems information, including jail management and court systems, so you know that your population and the public access current and accurate information. Securus AIS offers an English and Spanish interface, text-to-speech playback of offender names, and a touchtone and voice recognition interface. Each month CDOC will receive a usage summary report via email highlighting total incoming calls, automation rate, and total call duration.

Securus AIS averages a 99.9% system uptime and it's easy to implement because it works with your current phone system with no additional hardware or wiring. CDOC

chooses information available and the Securus Implementation Team configures the Securus AIS system to include the options selected.

Information Configuration Options

Offender Specific Information

- Criminal charges
- Bond amounts and types
- Court dates, times, and locations
- Projected release date
- Commissary/trust account balances
- Visitation eligibility

General Facility Information

- Facility location and hours
- Directions to facility
- Policies for mail, medication, property, visitation, and money deposit
- CDOC specific information

Increased Access | Reduced Stress | Password Protected

Your team can focus on other duties while Securus takes the calls. Agencies average 1 external call or offender question every day for every offender. That's a lot of time answering questions! The Securus AIS system relieves this burden and gives you administrative savings. On average over 75% of all calls are resolved through this automated system and some agencies have a resolution rate of over 85%. You will be shocked when you receive your first monthly reports to see how many calls you receive that previously dropped due to wait times. Callers don't wait so there are fewer dropped calls resulting in less frustration and fewer complaints.

In addition to the core functionality, Securus AIS can be configured to allow friends and family to open or fund a prepaid telephone account as well as fund an offender trust account over the phone. These additional funding options make it easier and more convenient for friends and family to contribute funds and pay in advance at lower rates than standard collect calling.

Dedicated On-Site Administrators

Dedicated onsite administrators assist in managing NextGen SCP, tablets, and network equipment. Tasks include, but are not limited to managing PIN/PAN administration, ordering materials, monitoring all open trouble tickets, performing weekly walk through

with on-site employee to ensure all equipment is up and performing as intended and ensuring problems are solved in a timely manner.

Onsite administrators are also responsible for inventory management of the Securus wireless devices and will train and assist Correctional Officers on the use and operation of the Command and Control Officer tablet and portal.

Below is a list of other duties performed by onsite tablet administrators:

- Primary representative between on-site facility personnel, Account Management & other Securus personnel
- Research issues reported by Agency staff members with the purpose of achieving resolution or escalation to the appropriate department
- Assist, monitor and or issue escalations as needed with other internal departments.
- Communicate internally all client requests and issues to facilitate resolution
- Open, address, resolve and track heat tickets and advise customer and Securus Personnel of service affecting issues
- Required to attend onsite meetings as designated by facility leadership
- Perform basic Technical Support functions (password resets and handouts, user set up, etc.) and basic product training as needed or requested by the customer.
- Assist Tech Support in the maintenance of computer hardware, software and other equipment by providing troubleshooting results
- Manages and maintains assigned company inventories and assets (tablets, accessories, tools, parts inventory, laptop etc.)
- Distribute tablets and accessories to approved offenders
- Data/information analysis and integration skills.

Visitation Phone Monitoring

Search for and track leads related to criminal activity: Securus Visitation Phone Monitoring (VPM) service monitors and records all offender visitation conversations 24x7x365 at CDOC facilities. The Securus monitoring software is a scalable and upgradable investigative tool that helps uncover fraud, blackmail, intimidation, harassment, and bribery.

- Available stand-alone or integrated with a Securus Communication Platform
- Low-cost and easy to install with corrections-grade hardware

- Software tracks recordings with details to aid in investigations

Visitation phone monitoring with PINS: CDOC may choose to configure the system to use offender PIN on visitation calls so that every call requires a PIN for connection adding a layer to the search functionality and security.

Secure hardware: Securus VPM has one of the most secure systems in the industry. The hardware includes anti-tamper screws on a stainless-steel wall plate, spiral-wound stainless steel armored cable, and anti-tamper transmitter/receiver installed in a small enclosure.

Phone Calling with Tablet



The Phone application on the tablet helps users connect more often and with more privacy to family and friends, while leveraging the industry's leading offender telephone system.

The Phone application allows the tablet to function as a telephone extension of the NextGen SCP platform. All security features and restrictions apply including PIN/PAN lists, velocity controls, family and friend billing, customer service, and recording and monitoring. The Phone App has great functionality including recent call list, standard nine-key dialing pad, volume adjustment, and a visual call time.

Features and Benefits:

- Intuitive design with standard 9 key dialing pad and volume control
- Visual call timer
- Additional intelligence gathering opportunities
- Reduces confrontation in common areas
- Ability to place calls with more privacy and safety
- More opportunities to connect with loved ones

Video Remote Interpretation

Securus partners with Purple Communications to deliver VRI capabilities to facilities nationwide. Video remote interpreting (VRI) uses video conferencing technology to

access an off-site interpreter to provide real-time sign language or oral interpreting services for conversations between hearing people and people who are deaf or have hearing loss.

Calls are placed through the use a Purple P3 VRI application, through PC, Apple, or Android operating systems. Once P3 VRI application is selected, the agency will login to their account with their credentials provided by Purple post registration.



All reporting within the Purple P3 VRI system will be available to CDOC staff. When a Purple VRI session is conducted, the following information is stored and will be available: Call Date, Call Start Time, Call End Time, Caller Log ID, User ID, Terp ID, Client #, Client Name/Location, Purple Number, Reference Field1, Reference Field2, Session Mins, & Billable Mins.

Other features of Purple VRI:

- On demand 24/7/365 Video Remote Sign Language Interpreting services,
- Certified and ADA qualified sign language interpreters,
- VRI calls are monitored by the corrections officer or other staff member who is standing by the offender to assist with the VRI session. VRI calls are not recorded for later review.

AIS Voicemail

- Quick and easy for friends and family to initiate communication 24x7x365
- No cost to CDOC or Offender
- Recorded voicemails provide an additional investigative tool

Securus AIS Voicemail is a one-way communication product that allows friends and family to leave a 45-second voicemail for an offender. Any time, day or night, loved ones may initiate communication and deliver timely information. When an offender calls into Securus AIS, they may access new voicemail messages. They may play the message up to 3 times and save it for up to 60 days from the date it was created. Securus Automated Information Services Voicemail may also be listened to on Securus tablets with the phone app, reducing demand at community telephones.

As is standard with all offender telephone calls, Securus AIS Voicemail and offender statements while listening are recorded for investigative purposes.

Post Incarceration services

Securus SMS Re-Entry Tool

Securus realizes that our technology solutions must help facilitate an easier reintegration experience for returning citizens. We aim to strengthen communication between returning citizens and correctional staff and/or service providers ensuring that clients have access to critical resources in a timely manner. Our re-entry model begins during incarceration via our Securus tablet where individuals can access free education, communication, and re-entry resources that best align with their needs, search for post-release service providers and build a re-entry plan. Our model creates the opportunity for offender to be active participants in their rehabilitation process as well as the pre-parole process.

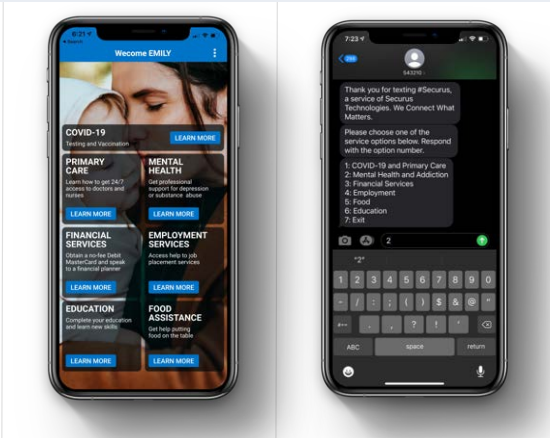
A critical step in the process of reentry is providing services, post release, that address the immediate, basic needs of the returning citizen, as well as long term support. Immediately upon release, individuals will be able to access our **re-entry platform** via SMS to gain access to resources such as virtual health care services, mental health services, financial services, employment services, education services and food assistance to be able to implement their reentry plan.

USER JOURNEY

RELEASE, PAROLE & PROBATION

CUSTOMER IN FACILITY		IN COMMUNITY	
Introduction via Tablet Reentry App	Raise Awareness& Pre-Education	Educate User and Signup	Services in Use







Televerde

Since October 2020, Securus Technologies has partnered with Televerde to provide incarcerated women opportunities in the customer service industry. Televerde has

been working with state level correctional industry agencies since 1994 and has current operations at agency facilities in Arizona, Indiana and Florida where incarcerated women provide service support from contact centers. As part of the partnership between Securus and Televerde, Securus would work with Televerde and the state of Colorado to review a potential expansion project to establish a contact center model at a female Colorado DOC agency facility similar to the Arizona, Indiana and Florida models aforementioned. All of these programs are independently managed by each state correctional industries agency. Specific to the Indiana Correctional Industries, Televerde participates in an additional program with the Department of Labor apprenticeship program to build workforce development programs with private sector industries. In addition to working with correctional industries with incarcerated women, Televerde also currently employs over 120 ex-offenders within their organization; and provides job training, transitional assistance and job placement through the Televerde Foundation (a non-profit founded by Televerde) opportunities for both pre and post release individuals associated with the Televerde programs and has proven, validated results of reducing recidivism rates for the population participating in their programs.

Q. Offeror will describe their ability to monitor a sample of offender telephone calls and provide ad hoc reports to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Through Word Alert, our speech-to-text transcription and keyword search tool, 100% of communications will be monitored. Add on our Guarded Exchange monitoring services as a force multiplier and CDOC will have the needed intelligence to keep personnel and offenders safe.

Word Alert automatically transcribes all telephone calls and SVC video sessions to text. Investigators can search the transcripts for words and phrases either interactively or by setting up automated, continuous scans that send them alerts when matches occur.

Word Alert lets investigators set up automated scans that continuously monitor new call and video session transcripts as they come into the system. An alert is sent each time a search term match occurs in a call or session. The investigator configures an automated scan with search terms in any language and optionally with an offender's name or ID, as well as the communication type. They can also include an end date if they choose. An alert is sent to the dashboard each time a search term match occurs in a call or session. The investigator can add email addresses and SMS text message phone numbers to receive alert notifications as well.

At any time, the investigator can see the total number of alerts triggered so far by the scan. They can review the calls and sessions that triggered the alerts and can also stop the scan at any time interactively. They can modify the alerts' lists of email and text message notification recipients.

The results of an interactive or automated searches can be exported to a report and then downloaded. The report lists calls and video sessions that had matches, with communication record information for each one.

Guarded Exchange System + Word Alert (GEX+)

Combining the power of AI with the aptitude of a human, we offer unmatched call monitoring services utilizing a combination of our proprietary artificial intelligence speech analytics program (Word Alert) and human-listening to produce greater targeting of highly suspicious calls to be listened to by certified communication analysts. Further increasing monitoring quality and providing industry-leading institutional safety and security.

The Process

- All calls are transcribed from a voice file to a searchable transcript of text.

- Text in all calls are processed through Word Alert
- The transcribed call text is analyzed, and a percentage of highly suspicious calls are identified for further inspection
- Escalated calls are listened to by certified communication analysts

The Benefits

- All calls are analyzed
- All calls are transcribed
- Highly targeted monitoring
- 24/7/365 agency access to call transcriptions and recordings through a permissions-based user interface
- Customizable searches to identify potential criminal activity
- Pinpoints search term matches and alerts you when they're found
- Translates foreign language transcripts to English upon request

Investigative Support Powered by Guarded Exchange (GEX)



With Guarded Exchange, Securus provides a comprehensive suite of investigative products and is the industry leader in live monitoring of offender calling. Securus Call Monitoring Powered by Guarded Exchange (GEX) is a service where every call is analyzed by sophisticated, ever evolving algorithms and any call that is suspicious is listened to by our team of Certified Communications Analysts. You get timely, actionable intelligence delivered in a detailed report from real people.

- Call Monitoring and Transcription by Highly Trained Analysts
- Over 15 million Calls Monitored to Date
- Used Daily by State and Local Agencies and DOCs, e.g., KY, MO, NM, NY, PA, TX

As calls are processed through the offender telephone system, and analyzed using Securus' Actionable Intelligence Potential (AIP™) scoring system. This data-mining software platform uses proprietary technologies that mine through phone calls, emails, financial transactions, and other information sources. This technology is used to identify and report variations in offender call patterns containing actionable intelligence information based on Six Sigma tools and statistical methods. The system utilizes a group of characteristics and attributes associated with offender behavior. Current and historical phone calls are statistically analyzed by algorithms measuring phone use, numbers dialed, frequency, ports, location, area codes, time of day, day of week and

many other offender behavior patterns and characteristics. Patterns are then identified, stored, and "learned" by the system. Securus' Live Monitoring system analyzes call patterns and other information to generate a call queue packed with Actionable Intelligence Potential.



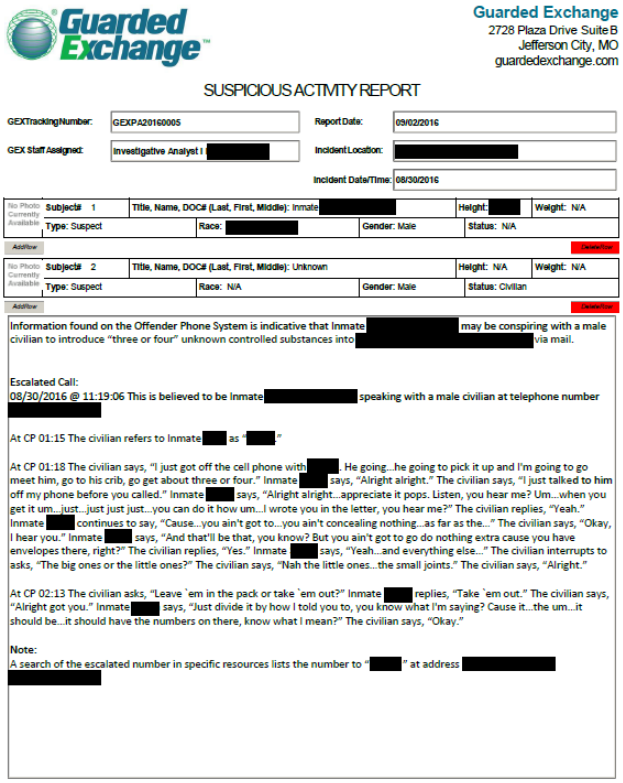
Suspicious calls receive up three levels of Securus listening and review before routing to your investigative team for action. No competitor devotes this much manpower to furthering your investigations. We are your team.

LEVEL 1 ALGORITHM RESULT ANALYSIS: The Securus Certified Communications Analysts who listen to your calls are highly trained and their speech to text transcriptions are more accurate than automated "listening" software. Securus Certified Communication Analysts are trained to focus on inflection, identify trends and anomalies, and hear what is not being said. We are looking for suspicious or suggestive keywords or phrases, calls that suggest threats to the safety and security of the facility, staff, volunteers, visitors, and population, and criminal activity inside and outside the facility.

Level 2 ESCALATION: If the Analyst reviewing the algorithm results confirms the suspicious activity, then they elevate the call to the Securus Call Escalation Team who also listen to the call and analyze it against your specific protocols for escalation. If they determine actionable intelligence is likely and that additional review is warranted, they forward the call to our investigations team for further review.

Level 3 INVESTIGATION: The Securus Investigation Team also listens to the call, uses Securus proprietary data analysis tools to further analyze and research the situation, and then drafts a Suspicious Activity Report (SAR) for your review. Our rigorous evaluation process and detailed report generation streamline your investigations and result in an extremely high level of actionable intelligence for every report you review.

Sample GEX Report



Guarded Exchange
2728 Plaza Drive Suite B
Jefferson City, MO
guardedexchange.com

SUSPICIOUS ACTIVITY REPORT

GEXTrackingNumber:	GEXPA20160005	Report Date:	09/02/2016
GEX Staff Assigned:	Investigative Analyst I [redacted]	Incident Location:	[redacted]
		Incident Date/Time:	08/30/2016

No Photo Currently Available	Subject# 1	Title, Name, DOC# (Last, First, Middle): Inmate [redacted]	Height: [redacted]	Weight: N/A
	Type: Suspect	Race: [redacted]	Gender: Male	Status: N/A

No Photo Currently Available	Subject# 2	Title, Name, DOC# (Last, First, Middle): Unknown	Height: N/A	Weight: N/A
	Type: Suspect	Race: N/A	Gender: Male	Status: Civilian

Information found on the Offender Phone System is indicative that Inmate [redacted] may be conspiring with a male civilian to introduce "three or four" unknown controlled substances into [redacted] via mail.

Escalated Call:
08/30/2016 @ 11:19:06 This is believed to be Inmate [redacted] speaking with a male civilian at telephone number [redacted]

At CP 01:15 The civilian refers to Inmate [redacted] as "[redacted]"

At CP 01:18 The civilian says, "I just got off the cell phone with [redacted]. He going...he going to pick it up and I'm going to go meet him, go to his crib, go get about three or four." Inmate [redacted] says, "Alright alright." The civilian says, "I just talked to him off my phone before you called." Inmate [redacted] says, "Alright alright...appreciate it pops. Listen, you hear me? Um...when you get it um...just...just just just...you can do it how um...I wrote you in the letter, you hear me?" The civilian replies, "Yeah." Inmate [redacted] continues to say, "Cause...you ain't got to...you ain't concealing nothing...as far as the..." The civilian says, "Okay, I hear you." Inmate [redacted] says, "And that'll be that, you know? But you ain't got to go do nothing extra cause you have envelopes there, right?" The civilian replies, "Yes." Inmate [redacted] says, "Yeah...and everything else..." The civilian interrupts to asks, "The big ones or the little ones?" The civilian says, "Nah the little ones...the small joints." The civilian says, "Alright."

At CP 02:13 The civilian asks, "Leave `em in the pack or take `em out?" Inmate [redacted] replies, "Take `em out." The civilian says, "Alright got you." Inmate [redacted] says, "Just divide it by how I told you to, you know what I'm saying? Cause it...the um...it should be...it should have the numbers on there, know what I mean?" The civilian says, "Okay."

Note:
A search of the escalated number in specific resources lists the number to "[redacted]" at address [redacted]

Securus steps up when you have an urgent situation. Daily monitoring of calls is the primary objective of GEX Call Monitoring; however, upon request, the Analysts will target a subset of calls with the ability to monitor and report on thousands of calls in a matter of hours or days. Securus delivers when you have a Targeted Customer Request. No other vendor is equipped to perform in emergency or high-security situations, such as escapes, disturbances, and gang/security threat group activities. Securus is not only equipped, but we have delivered in these types of situations for our facility partners.

Digital Forensic Services

In addition to monitoring services, we also offer Digital Forensics through GEX, giving your access to the data on confiscated communication devices. Securus analysts use the latest digital forensic technology to extract actionable intelligence, so you prevent threats against public officials, harassment, and coordinated escape attempts.

Our certified Forensic Examiners extract data from devices that are damaged, locked, or unsupported by other forensic tools. For the most severely damaged devices, we use methodology called Chip-Off Forensics to remove the flash memory from the printed circuit board. Then we read and analyze the raw data stored on the chip.

R. The Offeror may at the discretion of the CDOC:

i. Provide and maintain a computer network for offender use that is separate from the States network, enabling offenders to make phone calls from tablets, and the Offeror further should agree to:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide and maintain offender tablets and a separate computer network so offenders can use tablets to make phone calls utilizing the NextGen SCP call control platform.

ii. Provide all equipment and software necessary to provide the services requested, to include but not limited to: telephone sets, wiring, connectors, jacks, etc. The Offeror may, upon CDOC approval, utilize any existing hardware belonging to the CDOC that is available and suitable. (Note: Any materials currently belonging to the CDOC will remain the property of the CDOC.) All equipment should be of a heavy construction and considered vandal-proof by telephone industry standards. Security phone sets are to be provided by the Offeror, and all sets will be the property of the Offeror. The CDOC will determine the number of telephones at each facility along with the location of all necessary equipment. The Offeror will provide services to all facilities required by the CDOC including current, new and privatized facilities.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide all equipment and software necessary to provide the services requested, to include but not limited to: telephone sets, wiring, connectors, jacks, etc. The Offeror may, upon CDOC approval, utilize any existing hardware belonging to the CDOC that is available and suitable. (Note: Any materials currently belonging to the CDOC will remain the property of the CDOC.) All equipment should be of a heavy construction and considered vandal-proof by telephone industry standards. Security phone sets are to be provided by the Offeror, and all sets will be the property of the

Offeror. The CDOC will determine the number of telephones at each facility along with the location of all necessary equipment. The Offeror will provide services to all facilities required by the CDOC including current, new and privatized facilities

Please refer to **Attachment No. 3, OCS SOW Equipment_Software_Inventory & Rate Proposal** included in this ITN response.

iii. Repair and maintain all network hardware and software in the system, to include any currently existing hardware that the Offeror chooses to utilize. The Offeror will be responsible for all charges related to the installation, repair, or maintenance of all network hardware/software related to the network and phone system for the term of the Contract, including but not limited to: line charges, connection fees, or other charges that may be generated by local telephone companies or long-distance telephone companies that may be utilized by the Offeror. All work performed by the Offeror will be at the Offerors expense and will not be billed to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus offers a complete, turn-key offender telephone system. We install 100% of the system hardware and software for all facilities and maintain them for the life of the contract.

Securus will be responsible for all charges related to the installation, repair, and maintenance of all network hardware/software related to the network and phone system for the term of the contract, including but not limited to: line charges, connection fees, or other charges that may be generated by local telephone companies or long distance telephone companies that may be utilized by the vendor. All Securus-performed work will be at no cost to the DOC.

iv. Provide and install all additional and replacement wire and/or cable necessary for the operation of the proposed systems. All wire and/or cable installed becomes the property of the CDOC. The installation and materials used is expected to conform to industry as well as CDOC security standards.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

v. Order all lines and make all necessary connections to make the system active and for mounting all Offeror-owned equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

vi. Provide a system whereby telephone calls are not operator assisted, but are voice activated collect calls, prepaid or debit calls that include local and long-distance calls. State the options available to the CDOC and recommend a program that would require

limited administrative involvement by the CDOC. The desired system languages are English and Spanish. Further, the phone system will be compatible with the needs of deaf offenders, and offer video phones for deaf offenders. Hard of hearing offenders exist throughout the CDOC, and the phone system should accommodate such offenders. In addition, the system will:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen SCP system uses an automated operator so that offenders will not have access to an operator. NextGen SCP delivers the calls to the called party as collect, prepaid, or debit calls, including local and long distance.

NextGen SCP is a state-of-the-art, web-based system designed to provide the DOC with the ultimate in offender call control and reporting, requiring limited administrative involvement by the DOC. SCP's advanced features provide extremely powerful and flexible tools for controlling offender calling, reducing fraud, increasing investigative capabilities, and generating valuable administrative reports. The system is designed to adapt to your facilities and operations, rather than requiring you to conform to the software, and provides options for English, Spanish, as well as other languages.

In addition to providing TTY/TDD phones, Securus can provide the DOC with our Video Relay Service (VRS) for deaf and hard-of-hearing offenders.

NextGen Secure Communications Platform™ Overview

Industry-leading technology with input from corrections and law enforcement partners: Securus NextGen SCP is an integrated software platform for managing, researching, monitoring, investigating, and exporting information through Securus products and services. Built from the ground up with input from corrections and law enforcement professionals, Securus NextGen SCP has the industry-leading technology, features, and functionality you need to manage communications and support investigations at your facilities.

- Integrated interface to manage communications and investigations
- Reliable network and secure data storage with built-in redundancy
- No outsourcing—100% designed, operated, and maintained by Securus

Securus NextGen SCP Key Features
Refined User Interface ▪ Easily maneuver with action-based navigation ▪ Use Google-like single entry search fields

Securus NextGen SCP Key Features
▪ Get more information with less effort in a shorter amount of time
Custom Dashboard Configurations for Easy Data Viewing at Login ▪ See summary overview of facility communications immediately ▪ Quick access to BNA and PAN frequency search functionality ▪ Access upcoming video visitations
Improved Records Search Experience ▪ Increase the speed from request to data reducing your investigative time ▪ Get multi-product results with a single search ▪ Integrated backend technologies analyze and store data efficiently for fast access ▪ Run reports in the background while continuing to work and get notice when ready
Comprehensive Population Oversight ▪ A convenient activity stream shows all past, present, and future communication events ▪ Manage settings and suspensions for calls, video, and other products independently
Single Platform to Manage Calls, Video, and Visits ▪ Use the Contact Profile page to view visitor information and manage visits ▪ Set up facility and site level approvals custom-designed for your needs ▪ Manage visit approvals flexibly at first visit only, every visit, or automatically
Security and Access Management Flexibility ▪ Provide users with access and edit rights only to information needed to do their job ▪ Easily craft custom task-based permissions for admin. and investigative teams ▪ Protect your facility access with required strong passwords and regular updates ▪ Provide facility affiliated personnel with access to video visitation

Securus Telephone System Overview

The calling service will support NextGen SCP in safeguarding the community through proactive fraud prevention and advanced investigative capabilities. It allows our customers to operate a smarter and more efficient jail through system interoperability while providing the flexibility to interface with your current operations. The investigative tools permit a higher degree of accuracy and allow investigators to locate calling information more quickly and reliably. The system is scalable and flexible, reducing labor demands by automating many tasks. Routine calling operations can be configured to require minimal administration, allowing your staff to focus on what they do best—maintaining a safer, more secure correctional environment.

The calling service provides anywhere, anytime access for authorized personnel. All the investigative and administrative resources are available to approved personnel through the NextGen SCP user interface. Users can access calling services features any time from any Windows-based computer with access to the internet, allowing your investigators to follow the leads wherever they may go.

Calling Features

The calling service gives the DOC control over system features. That means you have complete control to customize the system to your specific needs, even as those needs change. We are committed to using technology to help you safeguard the public and solve and prevent crimes.

Key features include:

- Centralized architecture
- Anytime/anywhere system access using an internet-enabled computer from any location
- Real-time software/system upgrades three to four times per year at no cost to the CDOC
- Premium digital quality superior to that of analog-based systems, which is especially important for investigative purposes
- Remote monitoring 24x7x365 from Securus' Network Operations Center—we monitor system performance and can recognize and correct problems before you are aware of them
- Advanced call recording management through a patented technology to safeguard the chain of evidence controls on each recording, backed by free, professional testimony
- User-friendly reporting and self-help capabilities

Investigative Tools

- Monitoring and recording available on all calls that are not marked as 'private'
- Patented three-way call detection and prevention
- Patented remote call forwarding detection
- Perma-Block allows called parties to block future calls from the facility
- Covert Alert with Barge-In
- CrimeTip hotline
- Scan Patrol
- Case tracking (call notes)
- Investigative reports, such as frequently called numbers, pattern dialing reports, and more
- THREADS call analytics
- Voice biometrics, including IPRO
- Reverse Lookup

Fraud Controls

- Patented three-way call detection and prevention
- Patented remote call forwarding detection
- Dual tone multi-frequency (DTMF) detection to prevent:
  - Secondary dialing
  - Switch hook dialing
  - Black boxing
  - Hacking
- Velocity restrictions

Service Features

- 24x7x365 Network Operations Center monitoring
  - You operate around the clock, and so does Securus. We can find and fix most problems before you are aware of them and we are here to help you with your questions and requirements whenever you need us.
- 24x7x365 Technical Support through Securus' in-house Technical Support Center
  - We have the largest employee base in the industry to serve you better and to make sure we continue to lead with enhanced technology.

- 24x7x365 end-user support through our in-house Securus Friends and Family Call Center (SFFCC)
    - Securus is unique among national competitors in that we operate our call center. We do not outsource our customer experience. We find our end-user satisfaction ratings improve 22% when they use our call center. Providing good service to your constituents cuts down on complaints and provides a better experience for all. We are available to serve callers 24 hours a day.
- Ongoing training as well as training for each new software release (typically provided three to four times per year)

Call Completion

- Convenient points of sale and cost-effective terms for prepaid friends and family accounts
- Numerous funding options
- In-house SFFCC
- Lobby Kiosks
- Website funding
- Western Union funding
- MoneyGram funding
- Collect, prepaid collect (AdvanceConnect), prepaid calling cards, and debit options
- Offender PINs
- Offender PANs
    - Like all other features of NextGen SCP, the PAN lists are flexible and may be administered in various ways: PANs can be configured manually, automatically, or by importing through integration.
- Patented Automated Operator Services (AOS)
- Customizable call prompts, branding, and overlays
- Multi-lingual call prompts
- Offender name recording

Administrative Features

- Audit and activity tracking of system users
- Multi-level password controls

Call Controls

- Global blocked number lists
- Global allowed number lists
- Calling restrictions, including duration and velocity by offender, dialed telephone number, offender phone, phone group, customer, or facility
- Automatic or manual system on/off controls
- Emergency Call
- Automatic management of calling restrictions

Multilingual Language Prompts

The Securus automated operator uses clear, concise, professionally recorded voice prompts to assist the offender through the calling process. By default, the Securus calling service offers language prompts in both English and Spanish. Securus can provide additional languages on request. The NextGen Secure Communications Platform™ (NextGen SCP™) can be configured to provide prompts in as many as nine languages.

After the language prompts are configured in the calling service system, offenders select their language choice at the beginning of the call process by dialing a single digit. During call acceptance, the called party receives the acceptance instructions in English first, followed by an option to continue in the language selected by the offender. This fraud deterrent feature eliminates offender attempts to confuse called parties with a language they do not understand.

Securus also provides durable printed dialing instructions at each offender telephone location in English, Spanish, and any other languages specified by the DOC. As a security measure, Securus will use materials and techniques appropriate for the corrections environment that explains the process in a clearly defined and easy to read manner.

The language options supported by NextGen SCP include:

English	Haitian Creole	Somali
Spanish	Vietnamese	Mandarin
Polish	French	Korean
Russian	Navajo	Italian

Portuguese	Hmong	Bengali

Video Relay Services

NextGen SCP provides support for hearing-impaired offenders through both Video Relay Service (VRS) and TTY/TDD. The Securus VRS solution is a complete solution for correctional grade

VRS services that incorporate FCC regulations, as well as the offender call controls, management, and investigative abilities expected for offender calls.

VRS offers unique challenges to the correctional industry due to its reliance on American Sign Language (ASL), which requires visual communication, the automatic insertion of an ASL interpreter when needed, and adherence to FCC regulations that prohibit VRS service providers from interfering with or recording the communication.

Securus VRS addresses all of these challenges so as to provide the State with a VRS solution that does more than meet the requirements of ADA compliance—Securus VRS meets these challenges through a high-level integration with SCP. The high level of integration between Securus VRS and SCP provides hearing-impaired offender with "equal access" to communication services while allowing the DOC to provide, manage, and investigate offender VRS calls in a manner consistent with traditional offender calls.

Securus VRS provides equal access by allowing the DOC to:

- Provide VRS-capable offender call devices that fully conform to the rigorous needs of the correctional environment
- Manage VRS calls using the same controls as are used for traditional offender calls
- Record VRS calls in accordance with the same recording controls that govern whether or not to record traditional offender calls
    - Securus VRS can record VRS calls due to the fact that Securus is not a "VRS Provider". Instead, Securus is partnered with ZVRS/Purple to be the "VRS Provider". The nature of this relationship, along with the proprietary integration of technologies, allows SCP to record VRS calls while still remaining compliant with FCC regulations.
- Include VRS call recordings in investigations including inclusion in CD images and individual downloads.

Securus VRS call recordings include the visual component of the offender call for both the offender and the other end of the video portion of the VRS call. The other end of the VRS call might be the offender's called party (if they are a registered subscriber to the public VRS service) or the VRS interpreter (if the called party is not a registered subscriber to the public VRS service). Since the public VRS service automatically bridges in a VRS interpreter when necessary, Securus VRS fully accommodates the various scenarios the public VRS service may encounter. These scenarios include the potential that a VRS Service provider supports Voice Carry-Over (VCO). When VCO is supported, the Securus VRS call recording will include the audio component of the VRS call.

Securus VRS uses SCP's the same standard offender call management control structures as for traditional offender calls, including the following call controls:

- Calling schedules
- Max call duration controls
- Calling Restrictions
- Calling Velocity
- Called party phone number control—both globally and on offender PAN lists
- Call recording
- Collecting VRS calls in offender calls for investigations and evidence

This level of integration between Securus VRS and SCP means that the State can set offender calling policies that apply equally to all offender calls, including VRS calls, or set unique policies for VRS calls.

Offender access to Securus VRS is provided as an application available through ConnectUs—the controlled offender interface provided on offender kiosks. ConnectUs can be configured to present numerous applications to the CDOC offender, which allows offenders to use the same multi-function terminal for Securus VRS calls as for standard offender calling, Securus Video Visitation, Offender Forms, and more.

Because VRS calls are required by the FCC to be free, all offender VRS calls will be provided at no cost to the offender. To ensure the CDOC can prevent the unauthorized use of Securus VRS to place free calls, the Securus VRS is also integrated with SCP to allow the CDOC to designate which offenders are allowed to place VRS calls. The Securus VRS ConnectUs application requires offenders to enter their designated offender ID and their calling PIN before placing calls. To accommodate the needs of the hearing-impaired, Securus VRS can be configured to work without PINs in designated booking and/or intake areas. With these controls, the DOC has security over VRS calling

as well as the flexibility to allow VRS calls in situations where detainees have not yet been issued a PIN.

Securus VRS represents the ultimate solution for accommodating conformance to ADA compliance and FCC regulations, and the necessary call controls and investigative abilities to ensure safe communications.

a. Offer a programmable time limit restriction on calls with a notification of cut-off.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The system can set a maximum time limit for any or all calls related to either an individual PIN or all PINs. The phone system automatically manages all imposed durations and time limit restrictions, reducing the workload for facility personnel.

The system announces the upcoming time limit to the offender and called party at one or two minutes prior to end of their call, and then enforces the facility policy with a hard stop.

b. Assign a permanent ID number to each offender to allow system access and use. Upon CDOC request, CDOC offender ID #'s may be changed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP enables a facility to set up Personal Identification Numbers (PINs) for each offender. The system can be configured to require offenders to enter their PIN before making a phone call.

PIN generation can be uploaded from a JMS, OMS, or Commissary provider using the Securus E-Imports application, web services or a custom integration. PINs can also be manually input through the SCP user interface.

PINs can be linked to an Offender ID (Custody Account ID) for all offender information including allowed calling schedule, call durations, and more. The number can be configured as a number from 4 to 16 digits in length. Each offender can be issued a unique PIN.

Additionally, some OMS or JMS platforms can generate a 4 to 16 digit PIN randomly and send it to SCP via an integration. This option is beneficial because it enables intake staff or booking officer to give an offender their PIN, so they can begin making calls immediately.

PIN Operations

PIN operations through NextGen SCP are highly flexible. Facilities can enable or disable PIN operations at the facility, offender account, or phone level. For example, facility personnel may choose to enable PIN operations for maximum security or long-term areas, and disable PIN operations for overnight, work release, or trustee areas. SCP has no limit on the number of PIN or non-PIN offender telephones operating at the facility.

For phones programmed for PIN operations, each offender must enter their PIN before making a telephone call. By using their PIN, they create an audit trail that that shows the offender that placed the call, the date and time of the call, and the number that called.

PINs also enable facility staff to authorize or restrict specific offenders from calling specific numbers.

PIN Restrictions

PINs can be used to restrict offender calls at the facility, phone, or offender account level. For example, facilities can identify and lock PINs to a phone or group of phones within a facility. Site administrators also have the ability to transfer PINS, or a single PIN, when offenders change housing units. Transferring PINs can also be automated through the Securus E-Imports application, web services or a custom integration.

OMS / JMS Integration

NextGen SCP can be integrated with a facility's offender management system (OMS), jail management system (JMS), or Commissary system so that the offender PINs are automatically transferred, activated and deactivated based on the offender's status. If an offender is released, the offenders' PIN is stored and can be reactivated along with call detail records and offender recordings if the offender returns to the facility.

Examples of fields that can be automatically populated in NextGen SCP from an OMS, JMS, or Commissary integration include:

- First Name -Offender's first name
- Middle Name - Offender's middle name
- Last Name - Offender's last name
- Birth Date - Offender's date of birth
- Social Security Number (SSN) - Offender social security number

- Account Number - Offender ID, jail ID, or docket number, to be used as the SCP offender custody account number. Any number permanently assigned to an offender that does not change if they are released and booked back into the facility.
- PIN - 4 to16 digit code used by the offender to place phone calls.
- Activate Date - Date in which the offender account became active in the system
- Book Date - Date that the offender entered the facility
- Gender - Offender gender
- Housing - Location of the offender
- Race - Offender race
- Alert Level - Typically used for security status such as maximum, minimum, low risk, and death row
- Max Call Duration - Call duration applied to each phone call placed by this offender
- Three-Way Detection - Setting to enable or disable three-way call detection for this offender
- Language Preference - Language in which the offender speaks for reporting purposes (does not dictate the language of phone prompts)
- Suspended - Setting to allow or prevent the offender from placing calls
- Suspend Start Date - Start date of calling privileges suspension
- Suspend End Date - End date of calling privileges suspension

c. Include a remote cut-off switches at each installation site and/or administration sites to allow the system to be disengaged by the CDOC. The Offeror will provide and install cut-off switches.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide and install remote cut-off switches at each installation site and/or administration sites to allow a manual cut-off of the NextGen SCP system.

d. Provide a system capable of furnishing a maximum of 25 numbers to each offender.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Personal Allowed Number (PAN) feature in the NextGen SCP system provides an approved calling list for each offender.

Securus built this feature with the awareness that each facility has unique needs for implementing allowed calling lists. Like all other features of NextGen SCP, the PAN lists can be administered manually, automatically, or by importing through E-Imports. The PAN configuration options include:

- Auto Pan: Allows the first "X" numbers (defined by CDOC) to be added to the offender's PAN list automatically. The quantity of numbers allowed is configurable and can easily allow for up to 15 numbers for each offender.

  This is the most popular method of PAN administration. Numbers are loaded immediately without the intervention of staff, maximizing revenue potential.
- Offender Managed PAN: Allows offenders to manage their list, including adding a new number, removing a number, checking the status of a phone number, or hearing the phone numbers on their list. When an offender adds a phone number to their list, the automated system conducts a real time billing name and address (BNA) lookup on the phone number. If NextGen SCP finds a valid BNA, it will call the phone number and ask the called party to accept being on the specific offender's PAN list. No staff time is required to administer this process. With the extra step of validation, the DOC has maximum control of each added number. Again, this feature easily allows for up to 15 numbers for each offender.
- Manual PAN Entry: Authorized facility personnel can accept calling lists from offenders, verify the phone numbers, and enter them into the calling services user interface. This form of PAN administration allows a hands-on approach to approval and control of each number added to an offender's allowed number list.
- PANs by System Integration: NextGen SCP allows for the importing of PAN through our E-Imports application to add, create relationships, and deactivate numbers. There is no staff time required to administer this process. This is a specialized form of PAN administration, based on specific integration requirements of a facility.

Additional PAN Features

NextGen SCP provides administrators additional features to maximize efficiency, control, and inspection of PAN lists:

- Global Allowed List
- Automated List Refresh
- Verified/Not Verified PAN
- Speed Dial for PANs
- Associate PANs to PINs
- PAN Management Report
- PAN Change Log Report
- PAN Frequency Report

The following table provides descriptions of each PAN features and their primary benefit to the CDOC.

PAN Features

PAN Feature	Primary Benefit	Description
Global Allowed List	Efficiency	Certain phone numbers, such as attorney numbers, can be authorized for all offenders by including them on the calling services "global allowed list."
Automated List Refresh	Efficiency	With this automated feature, PAN lists can be configured to refresh every month on a certain day, such as the first of every month.
Verified/ Not Verified PAN	Safety and control	This feature flags numbers added to the offender's PAN list as "verified" or "not verified." If the PAN is "not verified", the offender can call the number for a configurable number of days before it is blocked. Once the threshold number is reached and the number is blocked, a facility administrator must verify the number and if appropriate, allow calls to that number again.
Speed Dial for PANs	Safety and control	Setting up speed dial numbers for PANs is a preventative measure that reduces an offender's ability to steal or use other PINs or PANs.
Associate PANs to PINs	Safety and control	NextGen SCP associate PANs with specific PINs. Administrators can apply restrictions to PINs giving facilities control over when and where an offender can place a call, how long they can talk per call, and how many calls they can make by day, week, or month.

PAN Management Report	Efficiency	This user-friendly, interactive report provides a dashboard view of all PAN entries in the system. The report indicates PAN entries entered into the Offender Managed PAN System. Users can select from more than 20 criteria to produce reports with multiple data points. All reports are exportable to Excel, CSV, and PDF.
PAN Change Log Report	Safety and control	PAN Change Log functionality records all actions that NextGen SCP users make to the verified field in the calling services user interface. It also allows administrators to examine all PAN list changes—specifically, when changes occur, and by whom, helping administrators and investigators track user accountability.
PAN Frequency Report	Safety and control	Shows phone numbers that appear in multiple PAN lists. Users can enter threshold numbers to define search criteria. For example, a threshold of "four" will show phone numbers that appear in PAN lists more than four times. This report also allows users to create a detail report with specific detail for each call.

e. Brand each call with the name of the facility and the name of the offender placing the call.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

When a called party answers, the system announces a collect call from an offender and states the name of the facility where the offender is located. The offender's recorded name is played to the called party as part of this call acceptance message to provide identification of the calling offender.

For example, a typical announcement would say, "You have a collect call from an offender, "John Doe," at the Colorado State Penitentiary. This telephone call may be monitored or recorded."

Each facility can customize the facility name used in call announcements.

f. Deny all incoming calls

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

To ensure maximum security to the system, Securus provisions the trunks in the Secure Call Platform (SCP) data center as outgoing only, ensuring that no incoming calls can reach the offender.

Securus has performed full testing of these trunks, verifying compliance with this requirement.

g. Detect and prevent a call to be transferred to a third party within the limits of current technology. No calls to pager numbers or pay telephones are allowed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

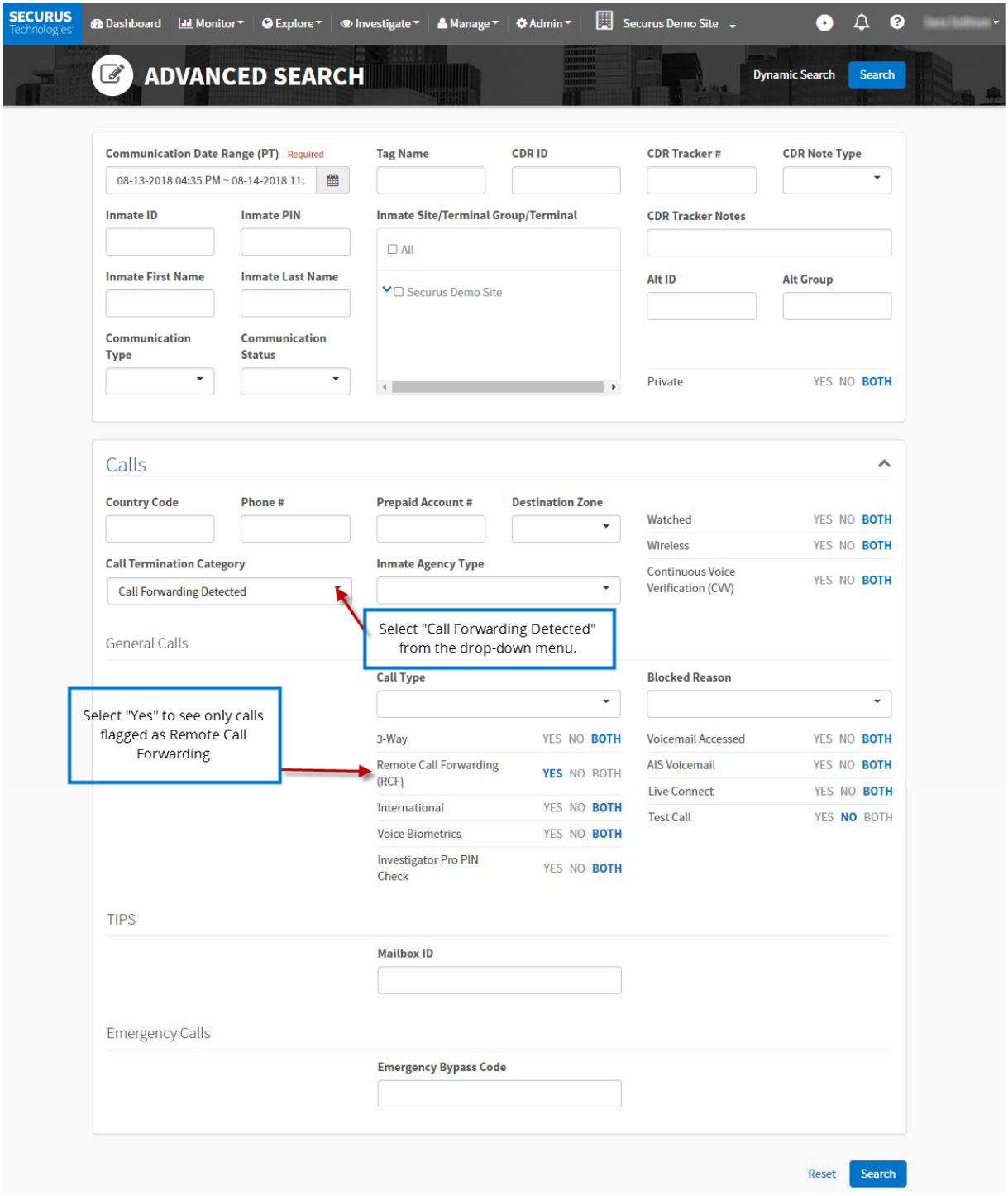
Securus leads the industry in fraud detection and prevention through real-time Remote Call Forwarding (RCF) detection. Our RCF solution can immediately terminate a call if it detects that a called party's telephone number is call forwarded or transferred to another telephone number.

The calling service can also be configured to allow the call to continue with one of the two following options:

- Announce to the offender and called party that remote forwarded calls are not allowed, and mark the call in the call record
- Mark the call in the call record, without an announcement to the offender and called party

NextGen SCP™ user interface allows authorized users to create Call Detail Reports for those RCF calls by selecting "YES" under the "RCF" attribute, using the specific termination code "Call Forwarding Detected," as shown in the following image.

Call Forward Detection



Calls to Pagers and Payphones

Securus uses a sophisticated, intelligent validation network in the industry. The system analyzes all dialed numbers before the call can proceed. This includes determining if the area code and exchange are valid, checking the number against restrictions such as customer requested blocks, and verifying through the national Line Information Database (LIDB) that the number can receive collect calls, and is not a cellular phone, pay phone, or pager. Only after passing all these tests will our system dial the number. This process is very effective in reducing fraudulent and illicit calling.

h. Provide offenders in segregation with mobile headsets or tablets to place phone calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus accommodates offenders in segregation with several different solutions, including a standard offender phone mounted to a mobile, cordless phones, and tablets. Securus will work with the DOC to provide the best solution at each facility and within each specific location.

i. Terminate a call completely when the caller hangs up, the called party hangs up, when the system's time limit parameter is reached or when a third-party call or call forwarding is detected if designated by the CDOC. The offender will be required to go through the automated operator or voice activator to initiate another call. The entire dial command sequence must be repeated.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP terminates a call completely when either party hangs up the phone or when the predetermined maximum call time is reached. In addition, detection of a three-way call or a remotely forwarded call will result in call disconnection, depending on the facilities preferences.

Any time the call is terminated, the offender must hang up the handset before attempting another call with a new dialing process. Securus' dual-tone-multi-frequency (DTMF) detection makes this all possible.

DTMF Detection, Collection and Prevention

NextGen SCP includes DTMF detection as a fraud prevention tool with every installation. The system, by default, does not allow the offender to press additional digits.

The system uses our patented DTMF collection techniques to collect and only act upon digits that the system is expecting. Unlike traditional premises-based systems, our NextGen SCP controls the call and buffers digits between pressing and sending.

For example, when SCP asks for language selection, it expects a one-digit answer; when asking for a PIN it expects the maximum PIN length. The system does not expect digits after call connection and will not accept any extra pressed digits. This makes it impossible for offenders to receive a secondary dial tone or call anyone by dialing additional digits after call connection.

j. Offer each facility or authorized CDOC staff the capability of remotely monitoring calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With integrated recording and monitoring applications, authorized DOC users as well as other agencies, such as authorized State Fusion Center personnel, can also access these functions. Any authorized user with an approved username and password can easily, and remotely, access recording and monitoring of offender calls from any computer or device with access to the Internet. Securus has tested and certified the playback of calls and live monitoring on:

- Operating Systems/Devices
  - iOS
  - Android OS
  - OS X
  - Windows
- Browsers
  - Internet Explorer
  - Firefox
  - Chrome

k. Offer a monitoring system that incorporates a Security Threat Group (STG) component that will include but is not limited to: identification and tracking of STG member calls and their call patterns, reporting capabilities identifying all calls made by STG members and indicating STG affiliation by facility, and identify phone numbers that multiple STG members call.

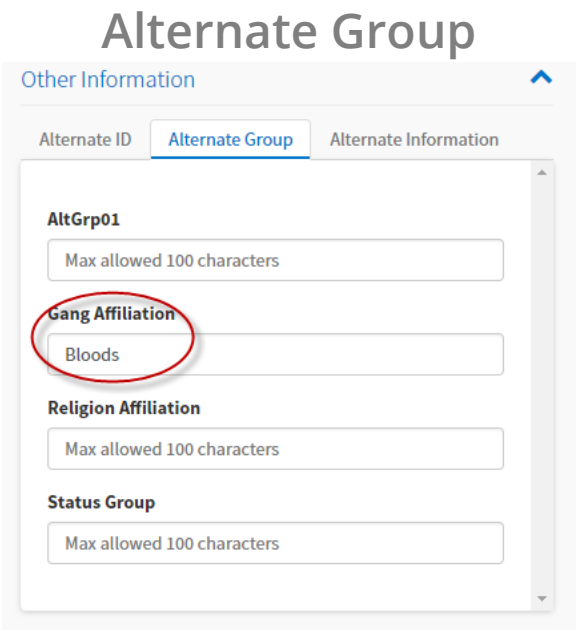
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP can monitor calls based on Security Threat Group (STG) affiliation using data provided by the DOC. CDOC will also have the investigative tools of THREADS, IPRO and ICER to assist investigators in identifying STG members and their communication patterns.

Special Threat Group Affiliation Tracking

Securus NextGen SCP provides a powerful tool to track an offender based on a Security Threat Group, such as gang affiliation. Tailored for the individual needs of each facility, authorized personnel may associate an offender with their respective Security Threat Group in the system and then track all associates in the Special Threat Group and monitor their call patterns collectively resulting in actionable intelligence.

The NextGen SCP offender record includes an “Other Information” section that includes options for Alternate ID, Alternate Group, and Alternate Information that identifies the appliable Security Threat Group. This field may be captured during intake or an update to the record at any time when information is learned. Alternate Groups are associated with the communication detail records (CDR) created when an offender makes a call or participates in a video session; this means that CDOC easily may search NextGen SCP for all communication records affiliated with a Security Threat Group.



Maximize Investigations with THREADS:

The combined capabilities of NextGen SCP, Investigator Pro, and THREADS identify and track Special Threat Group calls and their call patterns, which maximizes investigative leads.

Harnessing the power of THREADS, authorized personnel can search NextGen SCP for the following information:

- All offenderss associated with the same Security Threat Group
- Security Threat Group member calls and their call patterns
- Calls made by Security Threat Group members, and indicate gang affiliation by facility
- Phone numbers that Security Threat Group members call and indicate whether other offenders are calling the same numbers

Only authorized users can edit and/or see the Security Threat Group fields. In addition, CDOC users can identify unknown Security Threat Group offenders using THREADS, iPRO and NextGen SCP data.

Investigator Pro - Continuous Voice Identification

The voice biometric identification capabilities in Investigator Pro (IPRO), together with our Offender Intercommunications Evaluation & Reporting (ICER) capabilities, will give the agency a well-integrated and focused tool to uncover and identify offender attempts to hide their identities or to communicate with other offenders either inside a facility or in other facilities across the country.

IPRO is fully integrated into Securus' Secure Calling Platform (SCP) and does not require any 3rd party software.

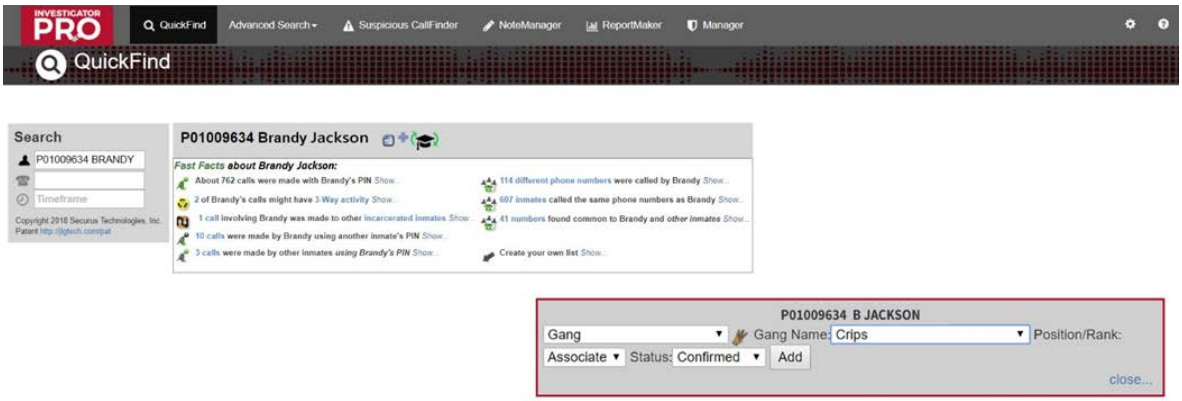
The following overview of features and STG (High Interest Group) monitoring is included here to describe the capabilities of IPRO and how they benefit investigators.

Custom High-Interest Group (HIG) Labelling

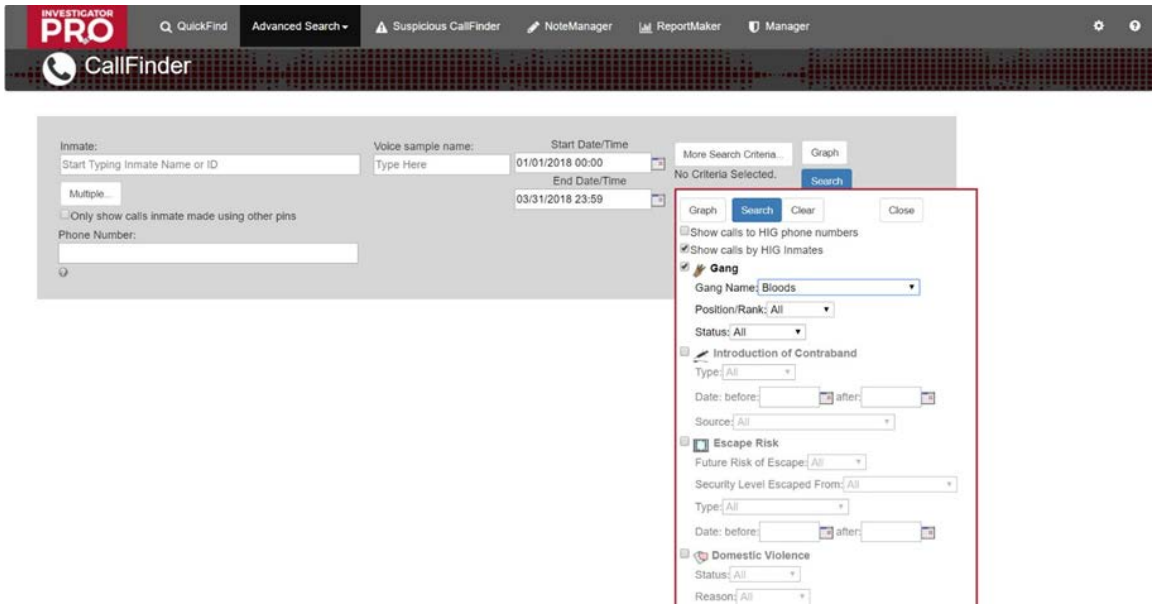
Investigator Pro lets investigator add their own custom High Interest Group (Strategic Threat Group) labels, such as particular gang names, contraband risk groups and activities like narcotics trafficking to offenders and called party numbers. This allows them to easily search and find these communications later.

Icons representing those labels then appear in call tables and QuickFind Fast Facts whenever those offenders and telephone numbers appear. The labels can be used as search criteria in CallFinder.

QuickFind provides an easy way to add HIG information about an offender after clicking the plus sign to the right of his name:



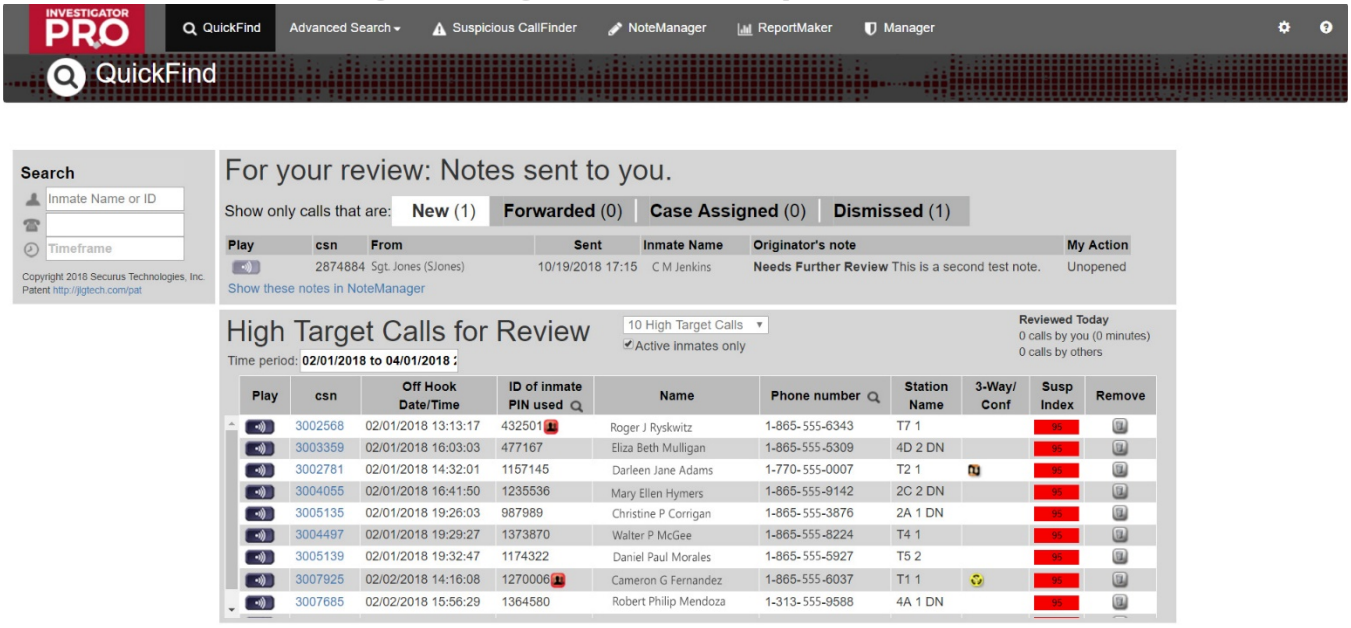
CallFinder makes it easy to search the call database by the agency's custom HIG names using the High Interest Groups criteria menu. The search results include a HIG icon next to offender names/IDs and called numbers previously tagged with a HIG label. This type of search lets the investigator quickly zero in on calls made by members of particular gangs or high interest groups.



Custom Gang Data Feeds

IPRO can be customized to automatically import the agency's own gang data, removing the need for investigators to manually add High Interest Group labels to offenders and called numbers.

High Target Calls Report



Investigator Pro Highlights

- QuickFind™ puts the smartest, most requested analytics on offenders, phone numbers and calls at your fingertips.
- High-Target Calls for Your Review presents the calls offenders most want to hide— ideal for random listening requirements.
- CallPlayer Pro™'s unique investigator-friendly screen features key information along with the ability to control the playback speed, skip over silent portions of the call and make notes.
- VoiceSearch™ finds and ranks any offender's voice on all calls, placed with or without his PIN. Investigators can also search on a called party's voice and identify the calls on which that voice appears.
- CallFinder™ puts call criteria at your fingertips to find the calls you need for your cases.
- MyCallReview™ lets you find, filter, manage and return to calls you've listened to.

- Suspicious CallFinder™ generates leads from suspicious call activity and lets you validate IPRO's results.
- NoteManager™ lets you organize, view and report on notes across calls.
- ReportMaker™ effortlessly runs reports to uncover patterns of telephone system use that may indicate illicit activities.
- IPRO flags and tracks high interest groups such as gangs, high profile offenders, institution drug dealers, escape risks, and mail-monitored offenders.

l. Provide the capability of automatically recording all calls made from the ITS, but not attorney calls, and the capability to track and retrieve recorded conversations via offender ID number, destination number, time of call, point of origin, or duration of call. The system should also offer the ability to query based on specific words and/or phrases. The system should allow for storage of this information for the current year plus 60 months. The Offeror will provide the necessary equipment to meet the required storage needs.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has the capability to automatically record all calls, but not attorney calls. NextGen SCP automatically bypasses monitoring and recording of special calls by designating phone numbers, such as those to attorneys, clergy or doctors, as "private."

Securus will work with the DOC on best process for making attorney calls private (do not record). This could include importing all known attorney numbers from your existing system or a list provided by the State Bar Association to the system. The web-based user interface, SCPTM makes it easy for administrators to maintain this database and, as always, Technical Support and Account Management is available 24 hours a day, seven days a week to assist with any service needs in maintaining this data.

Recording Search and Retrieval

NextGen SCP™ streams call recordings on an investigator's computer to play the recording through the attached speakers. While it is possible to make a recording from the speakers, this is only a copy of the original. Chain of Evidence safeguards are in place to prevent access to the actual digital copy of the recording and to eliminate any chance of manipulation, whether intentional or accidental, that could later challenge the authenticity of the call recording.

Word Alert – Key Words and Phrases

Word Alert will allow DOC staff to search call recordings for certain key words or phrases and much more. Word Alert is commercially available and can provide the following advantages for the agency and its investigators:

- A transcript of each telephone call and video session is available in minutes in its original language. *
- An English translation can be requested and displayed in seconds in line with the original language text. *
- Investigators can view a transcript alone or aligned with the audio or video player while the call or session plays. Search term matches are highlighted in the transcript. A button click jumps to the next or previous match in the transcript, moving the player automatically as well.
- Transcripts and their translations can be saved to PDF files.
- Investigators can manage a dictionary of word and phrase search terms, in any language, and create categories of search terms.
- Interactive, ad hoc searches let investigators find words and phrases in past calls and sessions.
- Automated scans constantly search new calls and sessions for target words and phrases and send alerts to investigators when matches occur.
- Alert notifications can be sent to email addresses and SMS text phone numbers.
- Snippets of matches in transcripts appear when the investigator's mouse hovers over a list of calls and sessions. Mouse clicks jump to those locations in the player and transcript.
- Integrated audio and video players can control playback speed and volume.
- Search results can be exported to downloadable reports.
- Analytics include search term category frequency graphs and totals.
- Word Alert's intelligent, behind-the-scenes analysis uncovers trending topics of conversation on calls and sessions in the facility. This can reveal illicit activity before investigators realize it exists.
- Users' call and video session playback events are logged in the NextGen SCP system, giving agencies information for auditing.

* The supported languages for transcription, and for translation to English, are Bengali, English, French, Italian, Korean, Mandarin Chinese, Polish, Portuguese, Russian, Spanish, and Vietnamese.

Communication Recording Storage

Securus facilitates anytime, anywhere, immediate access to stored recordings online for the contractually-required length of time. Securus stores all communication recordings in centralized, disaster-resistant, carrier-class data centers. All equipment used to store recordings is monitored by the Securus Network Operations Center (NOC) 24x7x365.

The NextGen Secure Communications Platform™ (NextGen SCP™) provides a unique set of features and advanced technologies to store communication recordings. NextGen SCP writes all recorded communication events to a Network Attached Storage array (NAS) in our primary data center. Each NAS array is also replicated to the secondary data center for redundancy and failover. All recordings created on the platform reside in at least two of our data centers. Recordings can be downloaded from NextGen SCP in various, widely-used formats and copied to a CD, DVD, or other portable media.

The NAS architecture makes all storage available to all servers on the network. The NAS solution delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network. The NAS devices can scale by adding another node of dense SATA disk to the storage array. Within the NAS, NextGen SCP uses a software-defined storage platform of very dense disk nodes. Even if three individual hard disk drives fail or one node fails during the disk or node recovery process, the system will continue to operate without data loss.

The Securus NAS has more than seven petabytes of storage space in each carrier-class data center and is continuously monitored and managed through automated processes and storage policies. When these very large storage systems approach designated thresholds, Securus expands capacity to ensure all authorized communication records and recordings are retained in secure, disaster-resistant locations.

The Securus data center storage solutions provide facilities with technology that is:

- **Scalable** to meet any facility's contractually required storage demands
- **Resistant** to local disasters through multiple copies stored within the data centers and off-site
- **Highly available** through the unique architecture and design of the data storage model
- **Partitioned** and **compressed** to run queries faster
- **Secure, protected**, **and monitored** to enable total recall of data

NextGen SCP records and stores basic communication data with the capability to provide management reports. Securus does not limit the communication data storage

time. Since every site's requirements are different, Securus works with each facility customer to define their optimal data storage timeframe. All recordings are stored online within both carrier-class data centers. Typically, communication detail records are stored for seven years.

m. Offer biometric voice identification technology to enroll, validate, monitor and continuously identify all offenders speaking on phone calls. The biometric voice identification system will include comprehensive investigative features.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus offers Investigator Pro™ (IPRO) continuous voice identification for the DOC. The voice biometric identification capabilities in Investigator Pro (IPRO), together with our Offender Intercommunications Evaluation & Reporting (ICER) capabilities, will give the State a well-integrated and focused tool to uncover and identify offender attempts to hide their identities or to communicate with other offenders either inside a facility or in other facilities across the country.

It is currently installed at several hundred state, county, and local agencies across the United States.

IPRO includes a wide range of tools that identify voices by name, deter offender PIN abuse, and provide leads for investigators to identify and prevent illegal activity carried out over the offender telephone system.

Investigator Pro is a Securus solution and Securus manages the solution roadmap. It is fully integrated with the Securus communications platform and is hosted in Securus' data centers. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.

Investigator Pro Advantages

Investigator Pro provides these advantages for the agency and its investigators:

- A choice of offender enrollment methods - supervised or covert - with the ability to mix the two or change from one to the other at any time.
- Real-time initial pre-call PIN check voice biometrics to reduce PIN theft.
- Continuous voice biometrics throughout the call to identify offenders by name no matter how many offenders are on the call or whose PIN was used.
- Ability to identify called parties by name when they are known to the system, to help find calls to released offenders.
- Voice search for offenders and called parties on both sides of calls using voice samples taken from either side.

- Offender-to-offender communication reporting through the seamless integration of ICER™, the Offender Intercommunication Evaluation and Reporting System, into IPRO.
- A call player rich in features such as the ability to skip pauses, control playback speed, mute one side, and learn more about the voices on the call.
- Ability to add custom gang information and high-interest group labels to offenders and phone numbers, and to search on that information.

Investigator Pro Capabilities

Offender Enrollment Method Choices

The agency can choose supervised or covert enrollment to create a voice-ID/PIN pair for each offender. It can switch from one method to the other at any time. It can also choose to enroll existing offenders covertly and new ones through a supervised process.

Supervised enrollment creates a staff-verified voice sample for each offender ID/PIN. Investigators then have a known audio file of each offender to play. In covert enrollment IPRO learns a voice and associates it with an offender ID/PIN. There is no staff involved and offenders are not asked to record their voices. Offenders are unaware of when and how covert enrollment occurs.

Pre-call PIN Check Voice Biometrics

IPRO's real-time pre-call PIN check feature, which the agency can elect to enable or not, reduces PIN sharing and theft. When an offender begins a call IPRO verifies in real time that the offender's voice matches the sample associated with the ID/PIN used to make the call. If it does, the call goes through. If not, the call is blocked.

Continuous Voice Identification

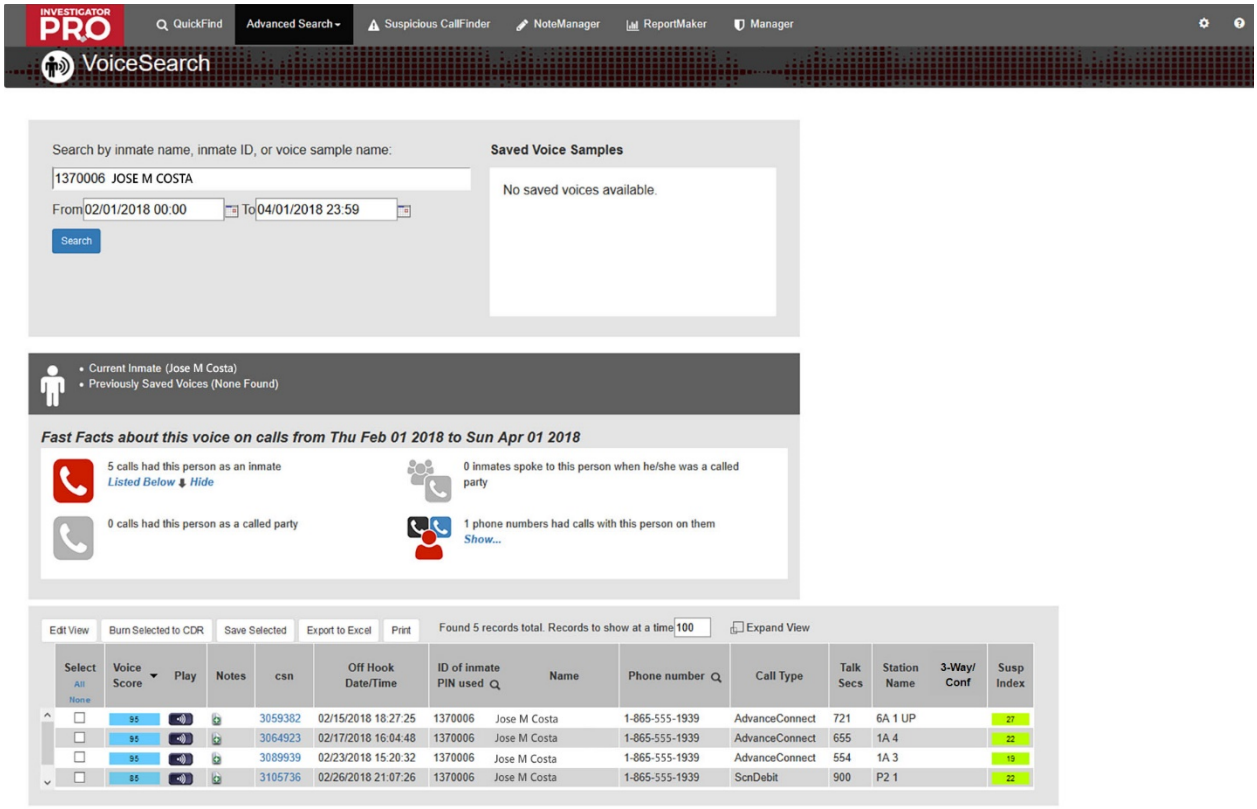
Investigator Pro does continuous voice identification throughout a call. It identifies all the speakers on the offender side of the entire call by name, no matter how many there are, which one started the call, or whose PIN was used. It covers 100% of every call without tipping off the offender(s) or called party. IPRO constantly "learns" and improves its voice identification accuracy. IPRO identifies called party voices by name when the names are known to the system, as in the case of released offenders.

Voice Search

The investigator can search for calls that have a particular voice on the offender or called party side of the call. He can do a voice search by offender name, offender ID, or a voice sample that he saved from either side of a call in the call player. Search results

include facts about that voice on those calls. With just a click the investigator can get a listing of the calls, offenders, or phone numbers involved.

IPRO Voice Search



Voice search results include facts about the voice and links to the relevant calls, offenders, and called phone numbers.

Identification of Likely PIN Abusers/Imposters by Name

Investigator Pro flags calls that are likely cases of PIN sharing/theft. It names the likely imposters and gives the investigator tools to pursue those offender names, calls, and voices further.

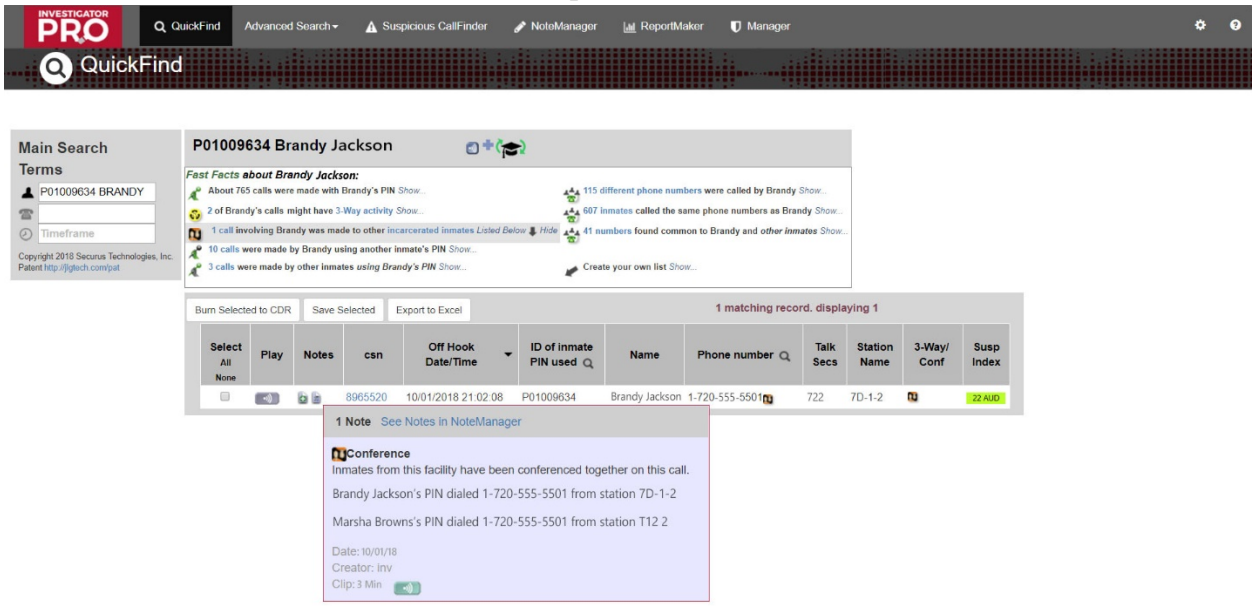
Offender-to-Offender Communication Reporting

IPRO detects offender-to-offender calls no matter how or where they happen, because ICER, the Offender Intercommunication Evaluation and Reporting System, is integrated into Investigator Pro. ICER finds these calls whether the offenders are within a facility or

in different facilities across the country, and whether the two offenders called the same or different outside numbers to make the connection.

IPRO puts ICER information at the investigator's fingertips on the home screen, in the results of call and offender searches, and in the call player.

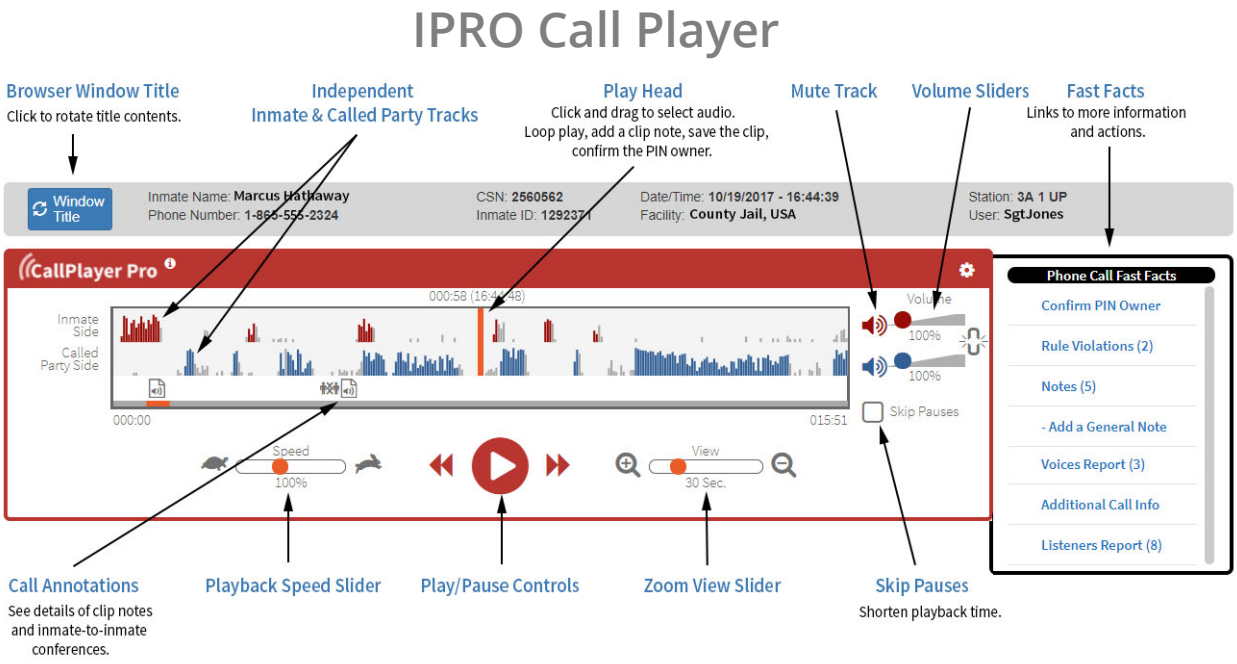
IPRO Quick Find



An offender search from the home screen gives valuable information, including details about offender-to-offender calls.

Call Player

Investigator Pro has a full-featured call player that makes listening to offender calls quick and easy. Some of the things investigators can do in the call player are: skip pauses, mute either side of the call, slow down/speed up playback, create audio clips, create and distribute call and clip notes with case numbers and category assignments, learn about the voices on the call, save voice samples for later voice searches, and learn about any rule violations on the call.



Investigator Pro's call player makes listening easy and efficient. The Fast Facts box beside it has links to more information and actions for the investigator.

3-Way Call Detection

When IPRO suspects 3-Way activity on a call it flags it in the call player and in lists of calls.

Database Search

Investigator Pro has a large database of information about calls, offenders, voices, and telephone numbers. Investigators can search the database by criteria such as offender name, offender ID, date range, saved voice sample, custom High Interest Group label, offender-to-offender (ICER) calls, 3-Way calls, originating station, and case number.

Custom High-Interest Group Labelling

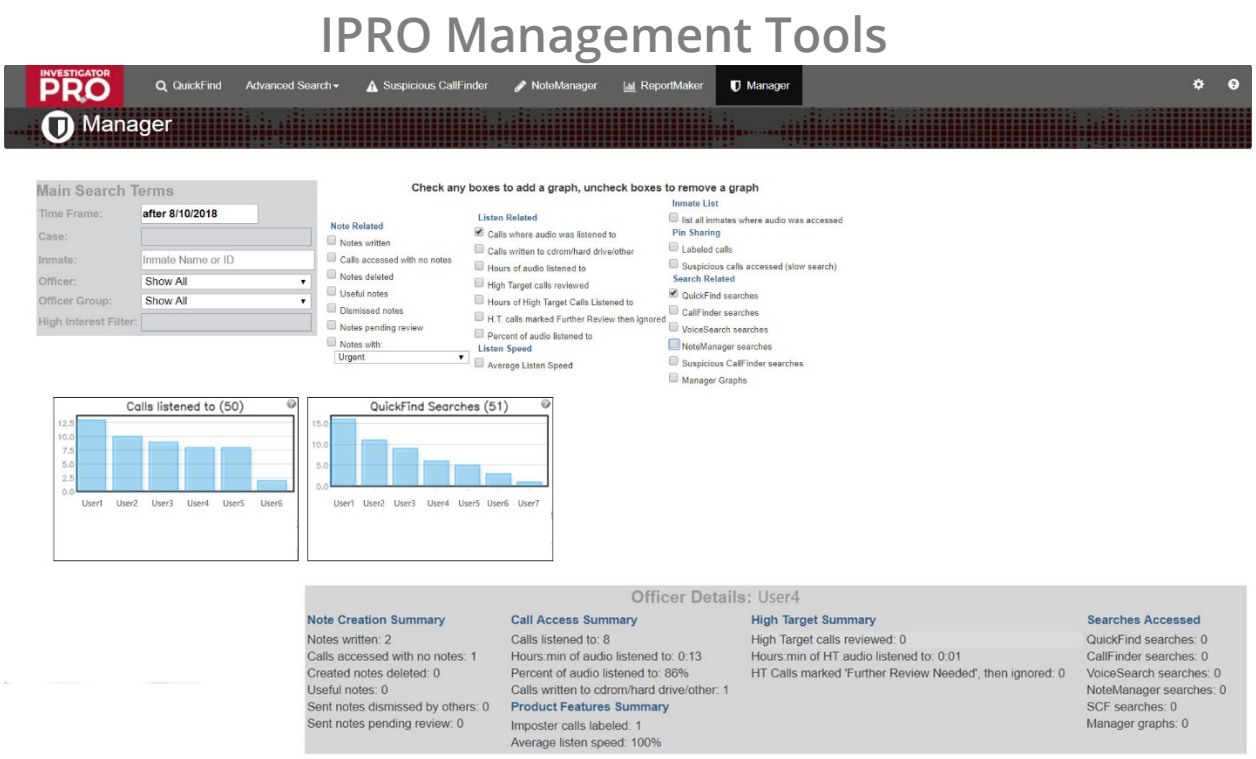
Investigator Pro lets investigators add their own information to the database and find it in searches later. They can tag offenders and phone numbers with their agency's own custom High Interest Group labels. They can also add notes and case numbers to calls, identify and label imposters' voices in cases of PIN abuse, and confirm the voices of PIN owners on calls.

Custom Gang Data Feeds

IPRO can be customized to automatically import the agency's own gang data, removing the need for investigators to manually add High Interest Group labels to offenders and called numbers.

Management Tools

Investigator Pro has management tools such as role-based access permissions, the ability to see officers' use of individual IPRO features, and the ability to create, organize, search for, and forward notes on calls/call clips.



Agency management can readily see any officer's use of the different features in Investigator Pro.

Reports

Investigator Pro can generate many useful reports with data such as pre-call PIN check results, likely PIN abusers, the most common called party numbers, and IPRO's voice learning results.

n. Offer a blocking feature to ensure that specific numbers are not called (i.e. 800, 888, 911, or toll-free numbers, etc.). In addition, the system will allow for individual telephone numbers to be blocked based upon subscriber request.

o. Offer a feature for blocking large number ranges, such as for State college dormitories.

p. Not require CDOC personnel to assist with the placing of a call.

q. Include capability for access to the Prison Rape Elimination Act (PREA) Sexual Abuse Hotline, which is operated by a designated outside reporting entity along with access to an identified emotional support entity and any other special need hotline numbers identified by the CDOC. Calls to the Hotline will be at no charge to offenders or the CDOC. CDOC to designate applicable staff with access to monitor the hotline.

r. Provide a telephone hotline to allow an offender to dial #55 (preferred number) where the offender hears a recording (English/Spanish) stating they can report sexual abuse or sexual harassment using this system. The offender's voice message is attached to an email that is sent to either the English shared mailbox account or to the Spanish shared mailbox account for review and handling; the mailbox is expected to have the capability to send out emails. CDOC is expected be able to confirm the location where the call originated.

s. Provide a system that does not violate any federal, State, or local laws.

t. Obtain all required Federal Communications Commission (FCC) licenses or any other approvals needed to utilize the system at a CDOC facility.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is licensed with the Federal Communications Commission to provide interstate and international telecommunications services, assigned Federal Registration Number ("FRN") 0006222319, provided as Securus Attachment No. 3, "Regulatory Documents".

u. Provide a system that does not interfere with any wireless equipment (two- way radios, Wi-Fi equipment, etc.) already operating at either facility. This includes but is not limited to two-way radio systems, telephone and data systems (other than applicable cellular devices), fire alarm systems, environmental control systems, lighting, motors, pumps, and electrical equipment. Should any damage occur, the Offeror will be responsible for any repairs required.

26. ITS INMATE IDENTIFICATION NUMBER (ID) APPLICATION

A. The Offeror will establish an offender account on the ITS that includes:

i. CDOC offender ID numbers are generated at intake and will be updated on the ITS daily.

ii. The ITS will provide the offender the ability to choose a minimum of a four (4) digit password for logging into the ITS. The Offeror will describe the procedures to implement and reset an offender's password.

iii. Authorized CDOC staff will have authority to modify or review any privileges or restrictions pertaining to an offender. Level of authority should be password/user account/password-based.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. The ITS offender ID number application will work with the ITS using all the features and functionalities described herein. No calls will be made without an ITS offender ID number.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. The ITS must allow each ITS offender ID number to have a "class of service" assigned. An adjustable default setting will be provided. Setting will apply to all calls unless modified for a special ID. For example, each ITS offender ID number will have the maximum duration of each call, etc. The proposed ITS must provide call restrictions by ITS offender ID number and provide the following restrictions at a minimum:

i. Location: Offenders can only make calls from the location designated identified in the data transfer file from CDOC.

ii. Placing of Calls: Offenders can be either approved or not approved to make telephone calls by ITS offender ID number.

iii. Use of Specific Telephones: Offenders, via the ITS offender ID number, will be restricted to a specific telephone or group of telephones, at the authorized CDOC staff's option; (i.e.: unit, wing, etc.).

iv. Duration of Call: Limit the duration of the call by facility, by individual, and by type of call, (local, Interlata, etc.).

v. Time of day calling.

vi. Any combination of the above.

vii. Once an offender is released, the ITS offender ID number and password will be deactivated.
viii. The ITS will interface with the CDOC EOMIS system to ensure the CDOC offender ID will be automatically transferred to the ITS.
ix. The ITS offender ID numbers will be accessible to authorized CDOC staff.
x. The Offerors ITS will document any changes to an individual ITS offender ID number.
xi. The Offeror will provide technology to restrict communication from those individuals who are not on the offender's approved phone list.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

27. SYSTEM RESTRICTION, FRAUD CONTROL AND NOTIFICATION EXPECTATIONS

A. The security and confidentiality of offender-placed telephone calls is of critical importance. Security features, which prevent unauthorized access to any information held by the Offeror, will provide for restriction to the ITS, fraud control for prevention purposes, and notification capabilities for attempted security violations or breaches. Secure access to the ITS will be maintained at all times. The ITS will have security capabilities that include, but are not limited to:

B. Each completed call from the ITS, except registered attorney telephone calls, will include a pre-recorded announcement at the beginning of the call that the call is subject to monitoring and recording.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. The Offeror will be able to detect unusual or suspicious number sequences dialed or dialing patterns, which the ITS identifies as possible attempts to commit fraud.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

D. The Offeror must briefly describe how the ITS will perform and/or prevent such fraudulent dialing attempts.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

E. The proposed ITS will provide a call alert and notification feature. An alert is an immediate visible indication of a suspected event that can be set by authorized CDOC staff. A notification is an e-mail or phone call to an identified event selected by authorized CDOC staff. The event can include but is not limited to:

i. A certain offender placing a call,

ii. A certain number is called by an offender, or

iii. A CDOC unauthorized call attempt is made.

F. The Offeror will briefly describe the alert feature proposed with the proposed ITS and the options available to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. The Offeror will be able to identify and report, three (3) way or conference calling and call forwarding. The Offeror is expected to have features that allow authorized CDOC staff options to manage identified calls. If authorized CDOC staff chooses to disconnect the call, the ITS will interject a message stating "This call is being disconnected in ten (10) seconds".

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

28. SYSTEM NETWORK STATUS MONITORING COMPONENT

A. The ITS will provide a system network status monitoring component within the ITS.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. The ITS' status monitoring component will, at a minimum:

i. Show graphically, in real-time, the status of the ITS components at each CDOC facility and other locations, to include but not limited to:

ii. Calls;

iii. Processor equipment;

iv. Call monitoring equipment;

v. Call recording equipment;

vi. Telephone station equipment; and

vii. Network circuit connections.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. Show component status for the ITS in a minimum of two (2) conditions:

i. "Green" for normal operation; and

ii. "Red" for failed operation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

D. Provide automatic reporting of component status changes (not manual input) for calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

E. Display and record event times, i.e., when any component changes status from "Red" to "Green", or vice-versa.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

F. The ITS provider will provide the service technicians the ability to log acknowledgements of but not limited to:

i. Component failures;

ii. Log acceptance of responsibility for repair; and

iii. Log comments on action taken for calls.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. Authorized CDOC staff will be allowed to observe the ITS status display at any time upon demand. All event records and technician logs will be maintained by the Offeror for

a minimum of thirty (30) days and will be available to authorized CDOC staff upon request.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

29. TRANSITION PLAN

A. The Offeror will work with the authorized CDOC staff and the incumbent Offeror(s) to ensure an orderly transition of the OCS and responsibilities under the Contract and ensure the continuity of the system required by the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. The Offeror will propose and include a transition plan for a smooth "cutover" to the new ITS with their proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

C. The Offeror will maintain the current ITS database information including offender profiles and call records. These will be retained during conversion to the new ITS. The Offeror will explain how the database is maintained.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

D. Upon expiration, termination, or cancellation of the Contract, the Offeror will cooperate in an orderly transfer of responsibility and/or the continuity of the services required under the terms of the Contract to an organization designated by the authorized CDOC staff. The Offeror will provide and/or perform any or all of the responsibilities outlined in this Scope of Work.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

E. The Offeror acknowledges that the call records, call recording, documentation, reports, data, etc., contained in the ITS are the property of the CDOC. The Offeror is responsible for providing all call records, call recordings, documentation, data, etc., in a CSV format or format that authorized CDOC staff can maintain and utilize as an operational database and is designated by the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

F. Upon termination, all call detail records, call recordings, documentation, reports, data, etc. will be provided to the authorized CDOC staff by the Offeror within one hundred twenty (120) days of request or termination of the Contract. The data will be in a workable, software-compatible format, to be determined by authorized CDOC staff, at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. The Offeror agrees to continue providing all of the services in accordance with the terms and conditions, expectations and specifications of the Contract for a period not to exceed one hundred twenty (120) calendar days after the expiration, termination or

cancellation date. Upon termination, the Offeror will discontinue providing service or accepting new assignments under the terms of the Contract, on a date specified by the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

30. DIGITIZED MAIL

A. The Offeror will deliver a comprehensive digitizing mail solution by:

B. Providing an automated mail digitizing solution for both postal and legal mail.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus offers eMessaging and Digital Mail Center to meet CDOC requirements under the Paperless Mail System.

Digital Mail Center

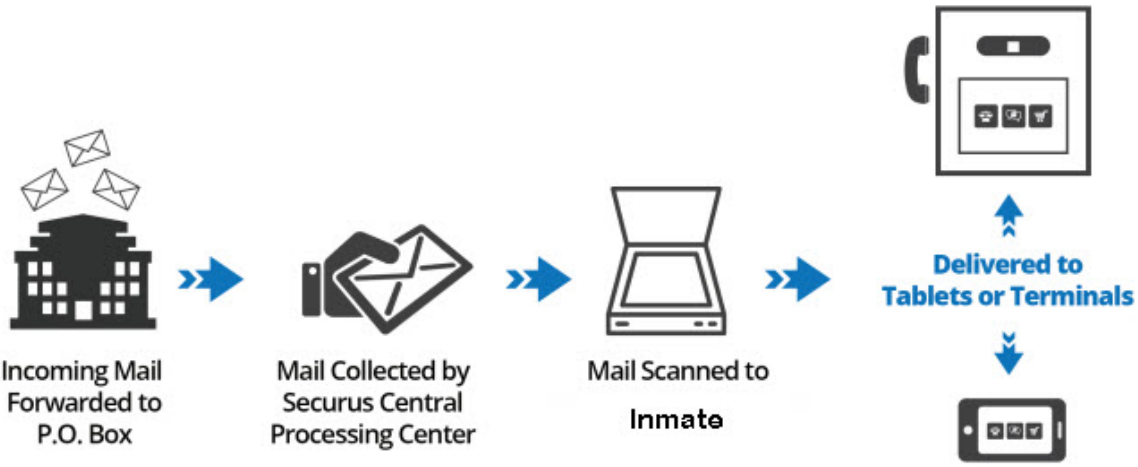
The Securus Digital Mail Center (DMC) processes your offender postal mail, scans it to digital format, and delivers it electronically to your population.

- Reduces contraband, disease, and chemicals entering the facility through the mail
- Reduces staffing costs and operational burden of postal mail processing
- Provides timely intelligence for investigations and monitoring

The Securus DMC uses the Securus ConnectUs Terminals and Tablets to deliver electronic copies of all offender postal mail. By accessing the Digital Mail Portal CDOC may manage the scanned mail, set suspension parameters to control delivery, set alerts for when a specific offender receives mail, and audit of activity logs for increased administrative oversight.

CDOC has flexibility in system configuration—you set up the system to automatically release scanned mail to offenders, allow for administrative approval for all mail prior to delivery, or require administrative approval for certain or all mail. CDOC can even block an offender from receiving mail.

The Securus DMC software will store all information associated with the letter, including sender name, time, date, address, and content, for the term of the contract creating investigative intelligence that is impossible to achieve through standard physical mail processing. Using the Bulk Export Feature, in one action CDOC may create a PDF with all documents in a search result for easy investigation documentation.



Upon release, an offender may use the Downloadable Mail Feature to securely download and print all previously approved, scanned communications from a Securus hosted website.

This service will allow all the functionality that is offered within eMessaging. This means that we have the ability to flag mail items by:

- Offender receiving mail item
- Mail sender
- Word List
- Suspicious Content (e.g. alternate languages/non-English vernacular)

Based on these flags, mail can be routed to the “censored”, “security”, or “requires approval” buckets for processing. Here groups/users may be assigned to work and process these items accordingly. Reasons for why items are censored or marked for security may be configured and made available for selection when processing mail.

CDOC will utilize the Facility System portal where they will also be managing their eMessaging. The Securus system uses a mailbox flag icon to indicate that it is postal mail. This will be accessed t through their user access within NGSCP

Process Details

- The Agency will receive ‘privileged’ mail at the existing location/address (e.g., legal, medical).
- Securus will establish a P.O. Box for each facility in the Securus DMC.

- CDOC updates outward facing mailing instructions stating that all non-privileged postal mail should be mailed to an offender at the new DMC P.O. Box address.
- CDOC forwards any non-privileged mail that arrives at the facility to the P.O. Box for processing at client expense.
- Upon receipt at the Securus DMC, all eligible mail will be processed. Eligible mail includes any envelope that contains traditional 8.5. x 11 paper sizing including manilla legal style envelopes. Cardboard (including USPS priority and express mail envelopes), rigid paper products, and magazines are not eligible for processing and will be returned.
- Within 48 hours of receipt, the Securus DMC will open the mail and inspect for contraband or any suspicious material. If contraband is found prior to scanning, the mail will not be scanned and, if contraband is found after the mail is scanned, the mail will be "revoked." All contraband will be given to local law enforcement and Securus will notify CDOC.
- Approved mail, including envelope and content, will be scanned.
- Contents of mail will be placed back in envelope to be stored for a period of 30 or 60 days. CDOC chooses whether to have mail returned to it or destroyed after this storage period.

All mail item will scanned in for agency review and approval for release to the incarcerated individual population. We do not review and approve postal mail items. By only processing the mail and leaving the agency with the responsibility of approval, we negate carrying any liability. Users may be assigned either "read-only" or "write/edit" access to certain buckets (censored, requires approval, security) so that only particular individuals or groups of individuals can process and take action on digital mail items.

From a mail handling perspective in the event of contraband being received, we have a protocol that manages that aspect of the service.

Contraband Protocol:

- Staff notifies Supervisor
- Photograph the contraband with an ABFO (American Board of Forensic Odontologists Scale)
- Photograph the contraband with envelope
- Seal contraband in an Evidence bag sealed with evidence tape
- Complete chain of custody of custody form
- Contraband is then locked in safe

- Supervisor contacts local Law Enforcement for destruction or processing of contraband (according to customer defined directives)



Privileged Mail Processing

Our approach to legal mail is to use a system of Copy & Shred approach with the individual receiving the legal mail present, as opposed to Encrypted Scanning and Electronic delivery.

When an offender receives Privileged Mail, either sent directly to the institution or forwarded by our Digital Mail Facility, an authorized CDOC employee opens the mail in the presence of the addressed offender and inspects it for contraband. The mail is opened by the employee for the sole purpose of ensuring that the contents are free of any contraband.

Once the mail is checked for contraband, the offender makes a copy of the contents using the provided copy machine and shreds the original using the dedicated shredder. This is all done under the supervision of the authorized CDOC employee. This ensures that the only copy of the Privileged Mail is solely in the possession of the offender. It also ensures that the original Privileged Mail is NOT retained by the offender or the State.

Securus will provide copiers, roll around carts and shredders in all key locations and. These devices can be mounted on mobile carts at the CDOC's request or installed in fixed locations.

C. Providing intelligent mail solutions to CDOC personnel for investigative purposes (keyword/watchword search capabilities on both incoming and outgoing messages).
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

D. Providing digitized mail services that offer the ability to restrict senders and receivers.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

E. Providing digitized mail technology to allow for separate viewing of letters and photos as well as the ability to reject/accept any combination of letters and/or photos.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

F. Providing both electronic viewing of messages and the ability for facilities to print messages and photos. For printing physical mail, the Offeror supplies printers and consumables, including, but not limited to, toner and paper at no additional cost.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

G. Providing tracking and logging receipt and delivery of all received mail.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

H. Ensuring offender electronic mail is storable by Offeror and/or transferrable to CDOC storage.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

I. Keeping all mail processing data current and made available upon request by authorized CDOC staff.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

J. Providing reporting of received contraband to CDOC and local law enforcement agencies.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

K. Providing a remote management platform through a security access designation.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

L. Installing and/or providing any necessary printer equipment and consumable supplies related to the printing and distribution of physical copies of mail within CDOC facilities including any related hardware and software/firmware without cost to the CDOC (if required).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

M. The Offeror will adhere to any and all municipal, State or Federal expectations for the handling and delivery of mail throughout the duration of the Contract. Should violation of codes, laws, statutes or ordinances occur relating to the digital mail system, the selected Offeror will correct the situation at no cost to the CDOC, including payment of any fines or penalties associated with the violation.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

31. ADDITIONAL COMMUNICATION SERVICES

A. Offeror may provide any additional features, functionality and technology available through the Offerors product that the Offeror believes would be useful to the CDOC.

i. Offender Cellular Phones

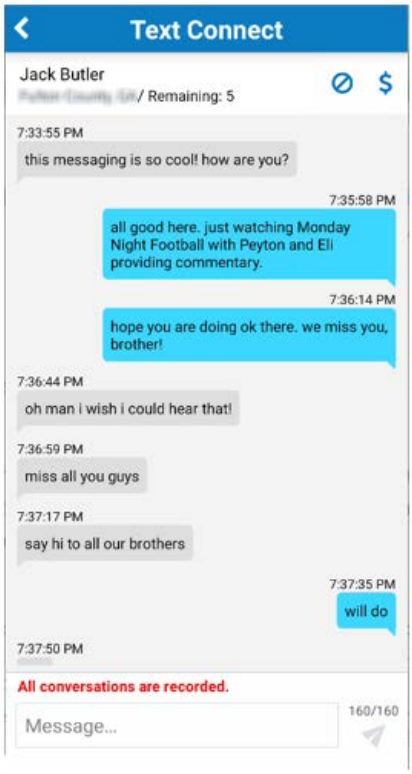
ii. Fully secured and tamper proof smartphone

iii. Remote monitoring and offender location tracking

iv. Text and voice/video calling capabilities

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Text Connect (STC) provides real-time texting for offender and their families and friends, using familiar technology that is safe and secure for facilities.



To make keeping in touch with their incarcerated loved ones as easy as possible, STC offers several features for family and friends, including:

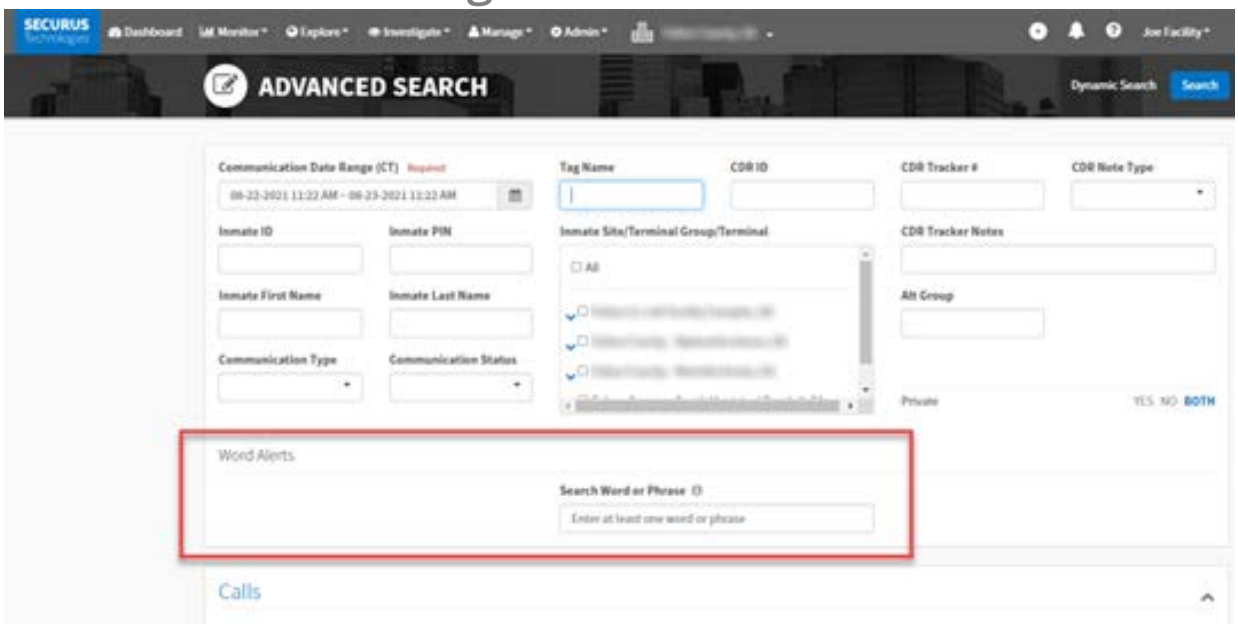
- Family and friends-initiated communication
- 100% funded by family and friends with a nominal charge per text message
- Real-time text messaging
- User interface mimics the traditional texting experience via a smartphone
- Simple access to STC through the familiar Securus mobile app
- Safety features that include the ability to block offender contacts
- Administrative functions including access to text message purchase history and more

STC was designed and developed with a focus on security. STC features robust safety and security capabilities for facilities, including:

- Consistent user experience—STC was built on the familiar NextGen SCP to make managing the product simple for administrators
- Archived conversation history—all messages are saved, and facilities have direct access to all conversations
- No photo or video attachments—no need to review and approve content

- Text search capabilities—facility staff can search by word, phrase, or by offender
- Blocking functionality—facilities, offender, and family and friends can block unwanted texts or prevent texts from facility restricted contacts
- Total control over STC—administrators at the site and facility level can suspend offenders from using the service or block friends and family from communicating entirely
- Integration with Securus' Word Alert product—adds an additional layer of security not offered by any competitor providers

Searching Text Connect CDRs



For an added layer of security and monitoring, we recommend that STC be used in conjunction with our text message monitoring tool, Word Alert.

v. Offender check-in technology
vi. ADA compliant phones
vii. Reentry Services/Apps

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is offering several services that will provide assistance of offenders in the reentry process.

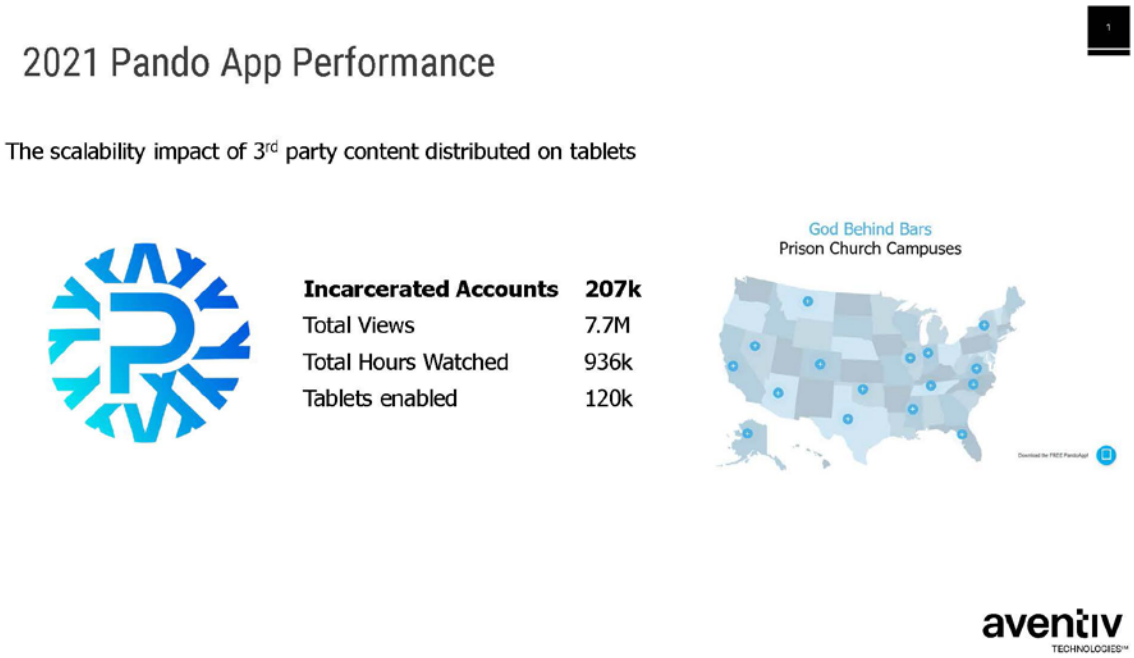
God Behind Bars (GBB) on the Pando App

God Behind Bars (GBB) on the Pando App provides offenders with the opportunity to develop a vibrant and meaningful spiritual/church life before they rejoin mainstream society. This app, being rolled out successfully in prisons in Colorado, Allows offenders to participate in church services on a regular bases, participate in church with family and friends on the outside via the Panda App, and allows them to gather in small groups for personal spiritual development. In addition, they are provided opportunities to serve and to learn which helps them prepare for a positive and constructive transition. A statement from GBB provides a good overview and some statistics on how offenders and families are being effected:

> "On September 22nd, 2013 we launched our first church service in a prison in Colorado. Today, we now have the honor to serve the least of these in four different prisons in the state of Colorado including Sterling Correctional Facility, Colorado Territorial Correctional Facility, Limon Correctional Facility, and Denver Women's Correctional Facility.
>
> What does God Behind Bars (GBB)Provide?
>
> God Behind Bars takes a three phase approach that helps offenders get to know Jesus, grow deeper with Him, and live out walking with Him. We get them connected to the church through a weekly experience. The weekly experience is a high quality worship environment where they can hear some uplifting music backed by an encouraging message. We then encourage them to have their family watch the same service through our Pando app, so they can connect with their loved ones. In our second phase we help them grow deeper in their faith by gathering in small groups. They learn about overcoming their hurts, habits, and hang ups. In our third phase they live out their faith by learning what it means to serve others, and gain knowledge on leading a life centered around Jesus. Our hope for those reentering society is that GBB is a season of their life, and the Church is the rest of their lives.
>
> Since 2013, we have seen some overwhelming success with our program in the state of Colorado. We have seen 64,000 offenders attend a GBB service. Over 5,500 offenders have made Jesus the leader of their lives, and 414 chose to get water baptized. We love our volunteers, and have gratefully seen over 3,100 volunteers serve inside of prisons in Colorado. Through the family reunification events we have seen (getting this number) families reconciled.
>
> God has moved in the state of Colorado and continues to do so. Covid has brought some challenging times, but through that adversity a God idea was

birthed and that idea is the Pando app. Let me introduce you to the greatest resource that has ever been given to offenders behind bars".

In Securus Attachment No. 4, "God Behind Bars Panda App," we have provided additional information on the GBB program and how it can have a positive influence on the CDOC system and population.

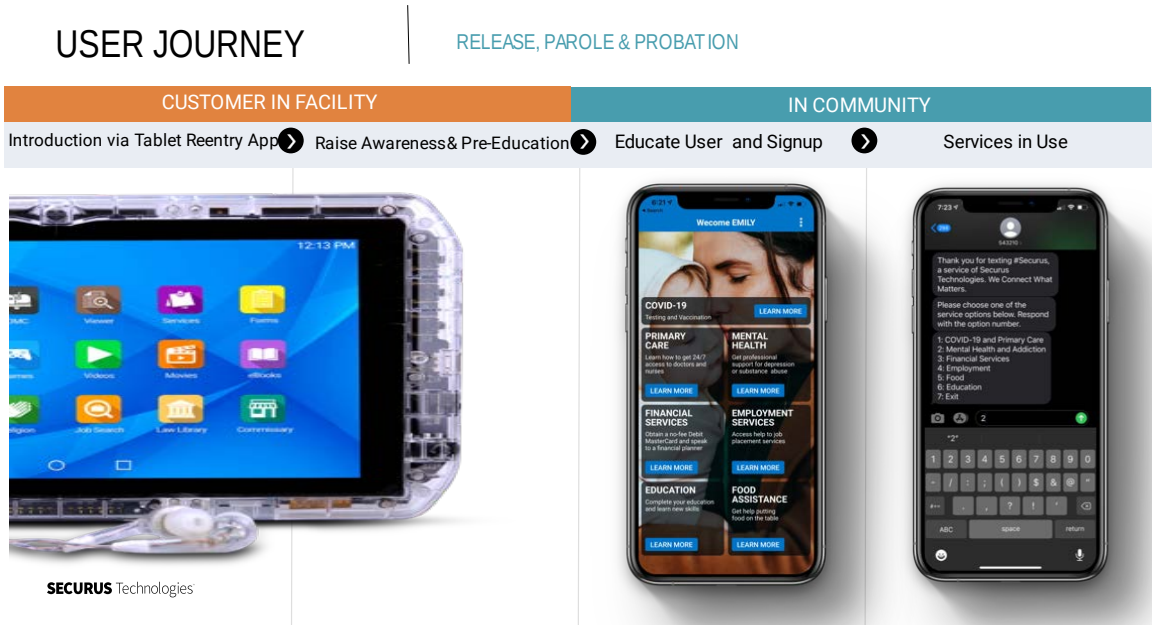


Post Incarceration Offerings

Aventiv realizes that our technology solutions must aid in facilitating an easier reintegration experience for returning citizens. We aim to strengthen communication between returning citizens and correctional staff and/or service providers ensuring that clients have access to critical resources in a timely manner. Our re-entry model begins during incarceration via our Securus tablet where individuals can access free education and re-entry resources that best align with their needs, search for post-release service providers and build a re-entry plan. Our model creates the opportunity for offenders to be active participants in their rehabilitation process as well as the pre-parole process.

Immediately upon release, individuals will be able to access our re-entry platform via SMS to gain access to resources such as virtual health care services, financial services, employment services, education services and food assistance. It is through the lens of the risk, needs, responsivity model that we understand that successful re-entry is driven by more than compliance with the terms of release. We are committed to delivering

technology to meet client needs to facilitate an ecosystem of behavior modification which will lead to reduction in recidivism. When combined with our robust, no cost, tablet deployment program and the associated embedded free programming and educational content; Securus leads the industry in providing the most comprehensive communication, educational and post incarceration program in the country.



For the first time in the history of our industry, Securus is moving in a new direction with respect to support of families and incarcerated individuals by partnering with Televerde.

This is a program we are deploying today in Indiana DOC and Arizona DOC. **Televerde** provides the opportunity to allow incarcerated individuals within the IN DOC and AZ DOC systems to handle call center duties for friends and family support, paying them a living wage and supporting their reentry with savings and job skills.

Televerde has a proven track record of helping develop knowledge and worker skills in incarcerated populations with a 3-year post graduation recidivism rate of only 5.4%. Together this holistic program of services will ensure participants have the opportunity to **gain work experience**, **develop personal accountability, and earn a fair wage** to help support their re-entry.

Post Incarceration Ambassadors (Proof our programs work)

Securus Technologies is proud to provide products and services that allow incarcerated individuals to maintain connections with those that mean the most, as well as free educational and re-entry programming that helps prepare the incarcerated to reenter society, including the opportunity to earn a college degree. We've even had the honor of meeting a growing number of many individuals who have used our technologies to create a successful second chance. Some of those inspiring people include:

- **Ronnie Hopkins** – In January 2014, Ronnie was sentenced to 3 years in the Grafton Correctional Institution on drug related charges. Ronnie was expecting to feel anger with his new reality, but instead, he felt at peace and used this opportunity to transform himself from the inside out. Starting his educational journey while serving his sentence, Ronnie took his first leap of faith by studying to earn his GED. After a lot of hard work, he earned such high marks that he was asked to teach his peers. With access to the Lantern platform, he was able to enroll in classes through Ashland University's correctional education offerings. Ronnie was released after 2 semesters of classes, completed his coursework from home through Lantern and earned his Associates Degree in General Studies from Ashland University. He is now earning his Master's Degree and working a Team Lead for Member Services at Christian Healthcare Ministries. See more of his story here, https://twitter.com/SecurusTech/status/1372642855488004102
- **Michael Baldwin –** In 1992, shortly after moving from Chicago to California, Mike was convicted of Kidnapping for robbery and assault charges landing him 26 years in prison. At a time where technology was not the foundation of communication, Mike lost contact with his children and most of his family members for 20 years. Baldwin was transferred to a facility that offered Securus tablets and was able to reconnect and with his family, which was rebuilt through emails and loving VideoGrams. He committed to being a better father, a disciplined student and pledged to be a better person. Due to his good behavior, Mike was eligible for parole. Mike was happily reunited with the outside world, his children and even the new additions to the family in October 2018! Now living in California, Baldwin has made tremendous strides in his career and the incarceration community since his release. He is now employed as the Director of Outreach for Prison & Grace Advocacy Group, a Professional Development Trainer for the Modesto School District, and a personal Assistant at the Law Office of Tracy R. Lum. In addition, he serves as the Criminal Justice Chairman for both the Modesto and Stanislaus Chapters of the NAACP. See video of him reuniting with his family and more of his story here,

https://vimeo.com/367313291/f6b64fe54e
https://vimeo.com/582604649/653ef56d7f

- **Benito Castro** - While serving a 4 year sentence at the Elayn Hunt Correctional Center in St. Gabriel, Louisiana, Benito enrolled in our Lantern post-secondary education program and diligently worked to earn his Associate's Degree with Ashland University before his release. After his incarceration experience, Benito started a non-profit organization called Freedom Rides, helping formerly incarcerated individuals obtain a car, insurance and license legally upon return home. Benito also gain employment in the meat department of a local supermarket before he eventually approached Ideal Supermarkets. Though he initially applied to be their Meat Department Manager, his interview paired with his Ashland University degree helped secure a promotion on the spot to Store Manager. Fast forward to today, Benito has worked his way up to being the Director of Operations not just for his store, but the entire chain with dozens of locations across the state. See more of his story here, https://twitter.com/SecurusTech/status/1375235936104120322

Recently, Securus deployed **JP6S devices to offenders in Oklahoma DOC**. The response was overwhelming.

- https://www.youtube.com/watch?v=P-rHe8xYXAs&feature=youtu.be
- KOCO Oklahoma: Oklahoma inmates receiving tablets will lead to better outcomes for those incarcerated, DOC says
- iHeart Radio: Oklahoma Prisoners Will Soon Be Getting Tablets To Use On Prison Property
- CNN: Inmates at Oklahoma prisons begin receiving computer tablets
- https://www.youtube.com/watch?v=O983jsMxxyw

viii. Educational platform
ix. Job skills
x. Employment resources
xi. Vocational building
xii. Creative content
xiii. Additional rehabilitative apps and technology or opportunities for offenders to gain skills.
B. Offeror may provide Cellular Phone Detection technology within CDOC facilities.
C. Additional offender communication services and/or applications may be limited to certain offender populations, facilities, programs, and/or geographic areas.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Viii. Educational Platform

Education

As an added benefit to the offenders, Securus has partnered with Ashland University, Prison Entrepreneurship Program (PEP), and God Behind Bars, to provide customized solutions.

These partnerships provide opportunities to create positive outcomes for post-incarceration. **Securus has included with our offer the opportunity to provide some of our premium services at no cost as a reward system to offenders who complete designated coursework.** We look forward to working with CDOC to build a program that maximizes utilization of the education content we provide.

KA Lite



KA Lite is a **user-friendly *offline* education application** that allows offenders to access more than 6,000 **K-12 educational content** options such as math, science, history, computing, and much more. KA Lite offers practice exercises, instructional videos, quizzes, and test prep. CDOC will have control over the subjects available to the offender.

KA Lite offers self-paced learning, suiting multiple learning styles and needs. Offenders can work at their own pace, allowing harder concepts to be practiced more efficiently. Offenders can plan their use around any schedule. Self-paced learning puts the ownership on the offender, forcing them to have internal motivation and learn time management skills. There is no cost to agency or offenders for this product.

Via a **personalized dashboard**, offenders can take courses, take practice exercises and quizzes, track progress, and explore real world applications. KA Lite provides an up-to-date educational curriculum based on **Common Core Standards**, offering thousands of instructional videos and interactive exercises.



Languages Available:

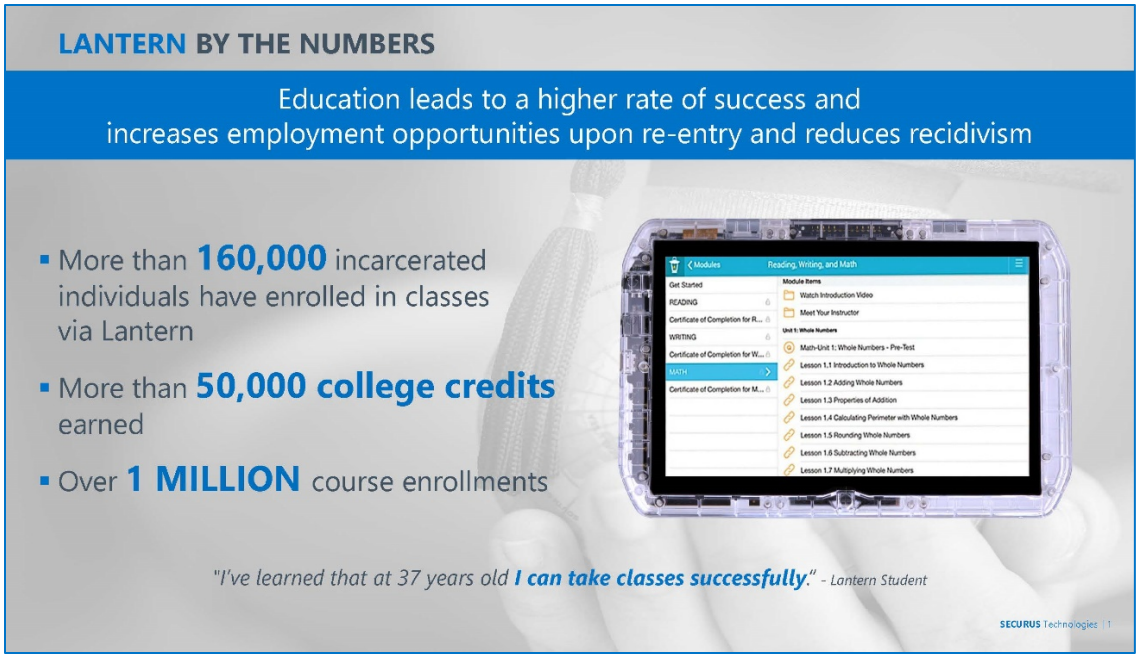
KA Lite via Securus has multilingual capabilities that support both English and Spanish. Some content is also available in French. **Closed captioning** is also available on a majority of the videos.

Unlimited Learning Opportunities with Lantern

Lantern is a Canvas-based Learning Management System (LMS). Canvas is used by multiple education agencies and schools throughout the nation, and Securus has modified this program to produce a **secure, corrections based LMS**.

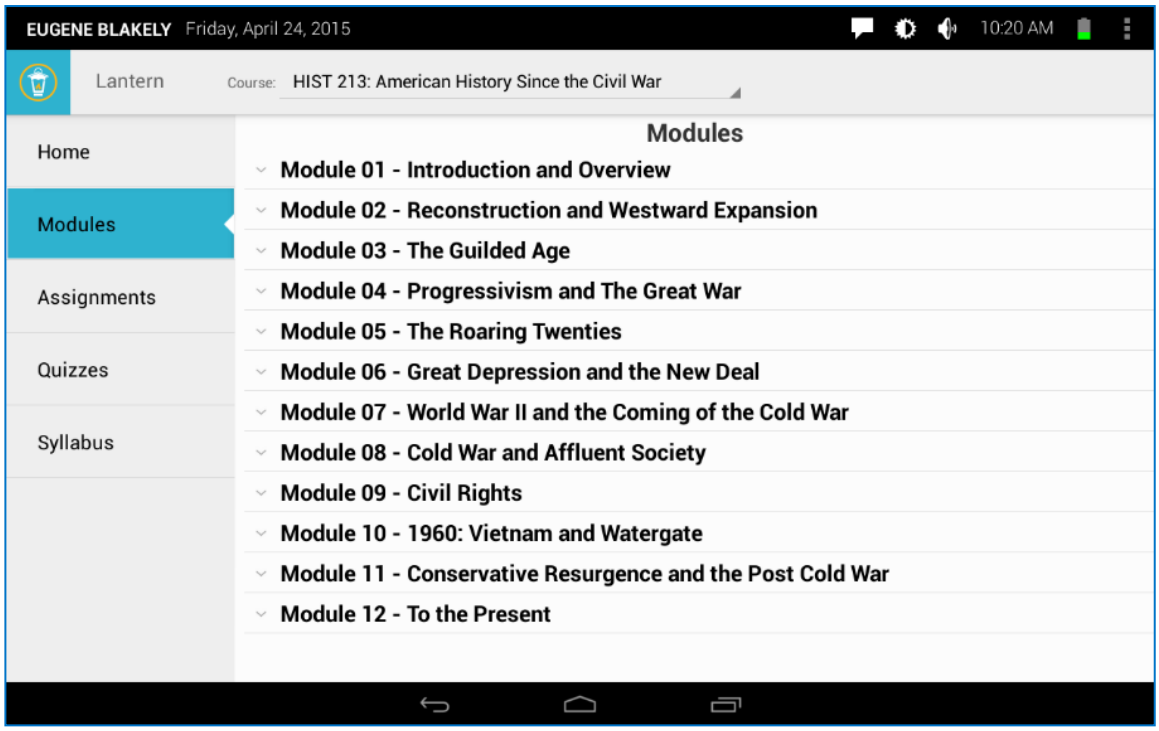
Securus' Lantern platform leverages secure tablet-based content delivery to increase the availability, scale, and variety of existing educational programs. Our open infrastructure platform is suited to building an education initiative from the ground up with courseware and educational partnerships. The education platform is a **free service** available on Securus' correctional tablets.

Lantern can be used to host facility-approved content, which is downloaded and consumed by offenders on their prison-grade Unity tablets.



Modules

Courses are split into multiple sections called modules, with each module consisting of approximately one week of coursework. Each module's course content is available on the tablet.



This may include, but not limited to, PDF files and ePub reading assignments, video lectures or voice-over PowerPoint presentations, and other downloaded content such as diagrams and audio files.

Within each module, students will also have assignments and quizzes to complete. The Unity Tablet also includes a customized, secure Mobisystems Office Suite product, so assignments can be completed using Word, Excel, or PowerPoint available directly from the Securus Lantern application.

Each course will also include a home page that displays the course objectives and overview for the student, along with a syllabus outlining the material to be covered and the due dates for each item.

All student coursework is completed and saved directly on the tablet. When a student syncs their tablet, all submitted coursework is uploaded to the Securus' LMS website for teachers/staff to access, grade and provide feedback. Once assignments are graded on the Securus' LMS website and the student again syncs with the kiosk, the students will receive all new grades and communications from their teachers. This allows module completion and coursework to be tracked on both the tablet and the Securus' LMS website.

Lantern hosts facility-approved content that offenders can access on their Unity tablets. Offenders have a real chance of equipping themselves with the education needed for success upon release.

Lantern is an adaptable system that allows instructors to upload coursework and correspond with students through a messaging option.

Functional Overview

- Screen elements are read aloud based on user touch on the tablet screen
- Screen reader reads aloud the navigational elements of the application as well as web view contents such as Assignments and Quiz Questions

College Credits through Ashland University

If your agency chooses to participate in offering college courses, Securus partners with Ashland University, an accredited university that offers free college courses to offenders using second chance Pell Grants. Securus and Ashland provide a turnkey solution, so no extra staff time is needed to support this education option.

Benefits of the Ashland University program include:

- Students enrolled in Ashland University courses access their courses from an Ashland University app on the tablet.
- The app launches a browser that only accesses corrections-grade Blackboard LMS site, or, alternatively, CDOC can choose our exclusive Lantern learning system.
- Students also use Mobisystems Office Suite, which includes Word, Excel, and PowerPoint, to create assignment files. This special office suite was customized for Securus to meet the security needs of our customers.
- All of this is exclusive to Securus' Ashland University partnership.

CourseShare



CourseShare offers a **no-cost solution** for agencies to **share educational curriculum** that can help offenders in any facility. Educational courses are proven to decrease recidivism by 40%; however, four out of five individuals in custody do not have regular access to educational content.

With CourseShare, agencies can give and receive custom courses created from respected agency peers across the U.S. through **Lantern, a Learning Management System that hosts facility-approved content.** Agencies can offer meaningful **rehabilitative programs** by leveraging educational content created from other agencies, saving time, money, and resources to create new course content. Offenders can access and download content directly to their tablets to begin their **path to successfully re-enter society.**

How CourseShare Works

STEP 1	STEP 2	STEP 3	STEP 4
Approval to share courses are granted. Appropriate content for sharing: • Basic Education • Life Skills • GED Prep, Post-Secondary/College • Substance Abuse • Vocational	A team of content specialists review the approved courses for appropriateness and external links. External links are removed if found.	Course content is imported to the new agency through Lantern.	Agency assigns new coursework to the students.



Google
Applied Digital Skills

CourseShare is now offering teachers and students access to **Google for Education - Applied Digital Skills.** The platform is a free, flexible video-based curriculum accessed by learners. The project-based units help students practice basic digital skills. With hundreds of hours of free lessons and instructional videos for 7th – 12th grade learners, lessons will equip them with the skills to be successful.

ix. Job skills, x. Employment resources, xi. Vocational building

Televerde

Since October 2020, Securus Technologies has partnered with Televerde to provide incarcerated women opportunities in the customer service industry. Televerde has been working with state level correctional industry agencies since 1994 and has current operations at agency facilities in Arizona, Indiana and Florida where incarcerated women provide service support from contact centers. As part of the partnership between Securus and Televerde, Securus would work with Televerde and the state of Colorado to review a potential expansion project to establish a contact center model at a female Colorado DOC agency facility similar to the Arizona, Indiana and Florida models aforementioned. All of these programs are independently managed by each state correctional industries agency. Specific to the Indiana Correctional Industries, Televerde participates in an additional program with the Department of Labor apprenticeship program to build workforce development programs with private sector industries. In addition to working with correctional industries with incarcerated women, Televerde also currently employs over 120 ex-offenders within their organization; and provides job training, transitional assistance and job placement through the Televerde Foundation (a non-profit founded by Televerde) opportunities for both pre and post release individuals associated with the Televerde programs and has proven, validated results of reducing recidivism rates for the population participating in their programs.

Job Search

Securus' Job Search application, **Jobview**, is specifically designed for use in the correctional environment. Jobview gives offenders secure access to over 2 million daily updated job opportunities. Each month, over a million job searches are conducted from the hundreds of correctional agencies where Jobview is available and being used today.

With Jobview, offenders have free and unlimited access to search for employment opportunities directly through their Securus Unity Tablet. The application's intuitive design requires no staff involvement, freeing up critical time and resources to focus on other needs of the correctional facility.

As an added benefit, Securus provides monthly reporting that tracks ongoing usage of Jobview allowing you to easily review the job search activity of the offenders at your agency.



Screenshot of Jobview on Tablet

Securus' exclusive secure job search app is already being utilized by hundreds of correctional facilities to allow individuals returning to society the ability to search for employment opportunities and prepare for a successful reentry.

Additionally, Securus Unity Tablets supplement the job search capabilities with free content that focuses on finding employment such as interview tips, how to create a resume and more.

xiii. Additional rehabilitative apps and technology or opportunities for offenders to gain skills.

Post Incarceration services

Securus SMS Re-Entry Tool

Securus realizes that our technology solutions must help facilitate an easier reintegration experience for returning citizens. We aim to strengthen communication between returning citizens and correctional staff and/or service providers ensuring that clients have access to critical resources in a timely manner. Our re-entry model begins during incarceration via our Securus tablet where individuals can access free education, communication, and re-entry resources that best align with their needs, search for post-release service providers and build a re-entry plan. Our model creates the opportunity for offender to be active participants in their rehabilitation process as well as the pre-parole process.

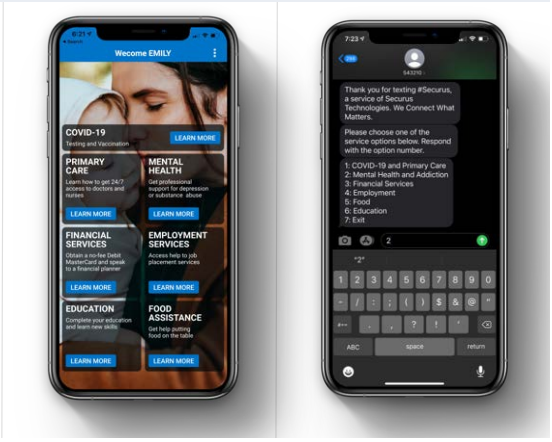
A critical step in the process of reentry is providing services, post release, that address the immediate, basic needs of the returning citizen, as well as long term support. Immediately upon release, individuals will be able to access our **re-entry platform** via SMS to gain access to resources such as virtual health care services, mental health services, financial services, employment services, education services and food assistance to be able to implement their reentry plan.

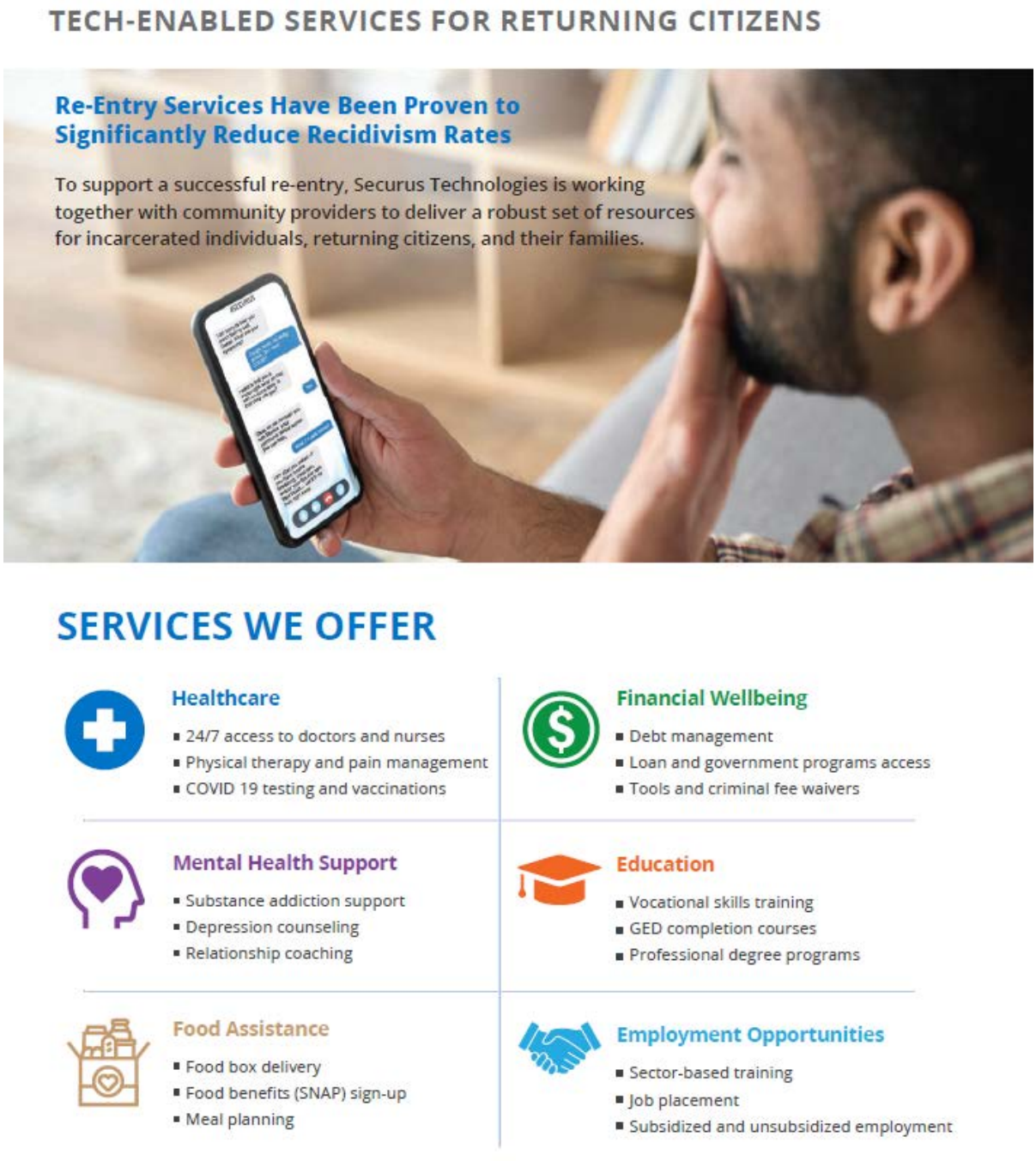
USER JOURNEY

RELEASE, PAROLE & PROBATION

CUSTOMER IN FACILITY		IN COMMUNITY	
Introduction via Tablet Reentry App	Raise Awareness& Pre-Education	Educate User and Signup	Services in Use







Televerde

Since October 2020, Securus Technologies has partnered with Televerde to provide incarcerated women opportunities in the customer service industry. Televerde has been working with state level correctional industry agencies since 1994 and has current operations at agency facilities in Arizona, Indiana and Florida where incarcerated

women provide service support from contact centers. As part of the partnership between Securus and Televerde, Securus would work with Televerde and the state of Colorado to review a potential expansion project to establish a contact center model at a female Colorado DOC agency facility similar to the Arizona, Indiana and Florida models aforementioned. All of these programs are independently managed by each state correctional industries agency. Specific to the Indiana Correctional Industries, Televerde participates in an additional program with the Department of Labor apprenticeship program to build workforce development programs with private sector industries. In addition to working with correctional industries with incarcerated women, Televerde also currently employs over 120 ex-offenders within their organization; and provides job training, transitional assistance and job placement through the Televerde Foundation (a non-profit founded by Televerde) opportunities for both pre and post release individuals associated with the Televerde programs and has proven, validated results of reducing recidivism rates for the population participating in their programs.

Pando App / God Behind Bars

Securus is offering several services that will provide assistance of offenders in the reentry process.

God Behind Bars (GBB) on the Pando App

God Behind Bars (GBB) on the Pando App provides offenders with the opportunity to develop a vibrant and meaningful spiritual/church life before they rejoin mainstream society. This app, being rolled out successfully in prisons in Colorado, Allows offenders to participate in church services on a regular bases, participate in church with family and friends on the outside via the Panda App, and allows them to gather in small groups for personal spiritual development. In addition, they are provided opportunities to serve and to learn which helps them prepare for a positive and constructive transition. A statement from GBB provides a good overview and some statistics on how offenders and families are being effected:

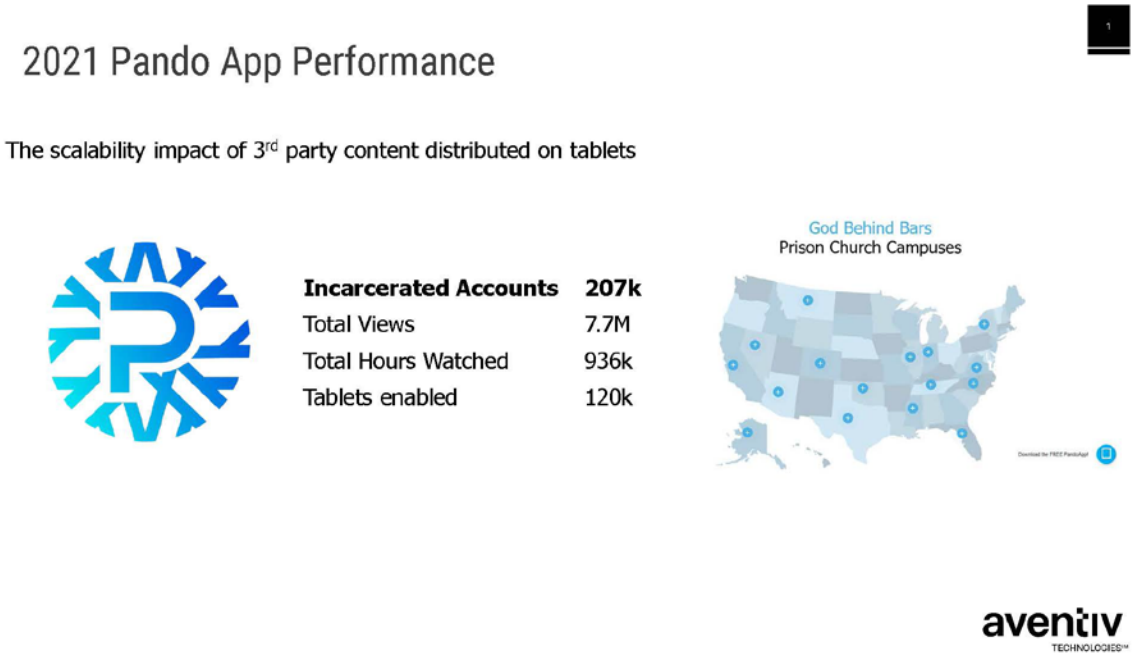
> “On September 22nd, 2013 we launched our first church service in a prison in Colorado. Today, we now have the honor to serve the least of these in four different prisons in the state of Colorado including Sterling Correctional Facility, Colorado Territorial Correctional Facility, Limon Correctional Facility, and Denver Women's Correctional Facility.
>
> What does God Behind Bars (GBB)Provide?
>
> God Behind Bars takes a three phase approach that helps offenders get to know Jesus, grow deeper with Him, and live out walking with Him. We get them connected to the church through a weekly experience. The weekly experience is

a high quality worship environment where they can hear some uplifting music backed by an encouraging message. We then encourage them to have their family watch the same service through our Pando app, so they can connect with their loved ones. In our second phase we help them grow deeper in their faith by gathering in small groups. They learn about overcoming their hurts, habits, and hang ups. In our third phase they live out their faith by learning what it means to serve others, and gain knowledge on leading a life centered around Jesus. Our hope for those reentering society is that GBB is a season of their life, and the Church is the rest of their lives.

Since 2013, we have seen some overwhelming success with our program in the state of Colorado. We have seen 64,000 offenders attend a GBB service. Over 5,500 offenders have made Jesus the leader of their lives, and 414 chose to get water baptized. We love our volunteers, and have gratefully seen over 3,100 volunteers serve inside of prisons in Colorado. Through the family reunification events we have seen (getting this number) families reconciled.

God has moved in the state of Colorado and continues to do so. Covid has brought some challenging times, but through that adversity a God idea was birthed and that idea is the Pando app. Let me introduce you to the greatest resource that has ever been given to offenders behind bars".

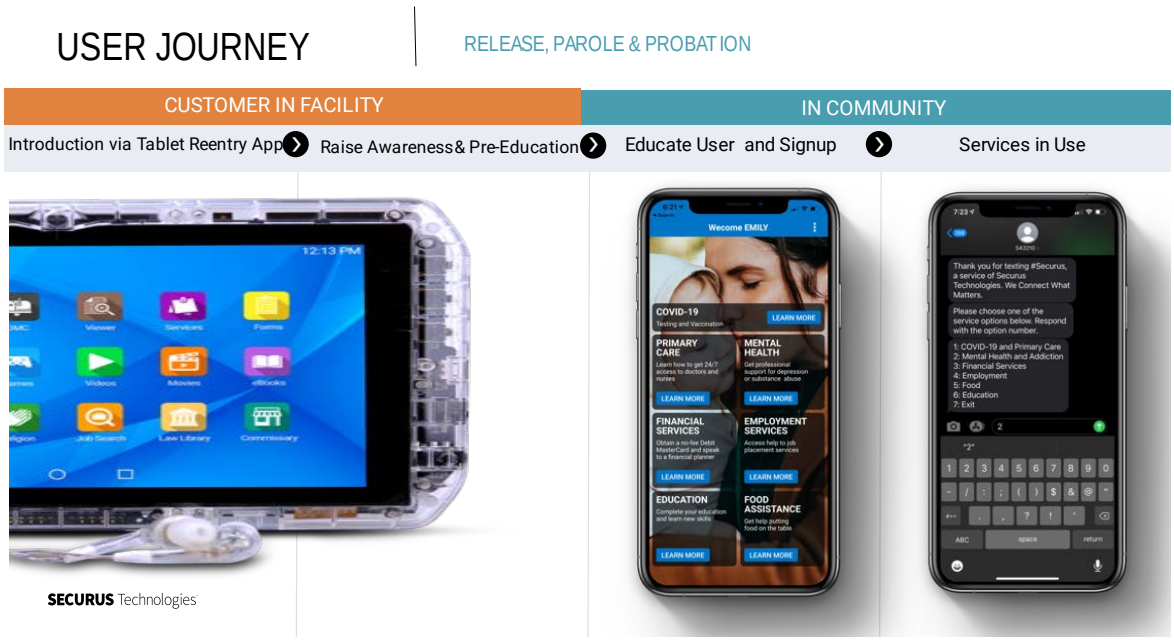
In Securus Attachment No. 4, "God Behind Bars Panda App," we have provided additional information on the GBB program and how it can have a positive influence on the CDOC system and population.



Post Incarceration Offerings

Aventiv realizes that our technology solutions must aid in facilitating an easier reintegration experience for returning citizens. We aim to strengthen communication between returning citizens and correctional staff and/or service providers ensuring that clients have access to critical resources in a timely manner. Our re-entry model begins during incarceration via our Securus tablet where individuals can access free education and re-entry resources that best align with their needs, search for post-release service providers and build a re-entry plan. Our model creates the opportunity for offenders to be active participants in their rehabilitation process as well as the pre-parole process.

Immediately upon release, individuals will be able to access our re-entry platform via SMS to gain access to resources such as virtual health care services, financial services, employment services, education services and food assistance. It is through the lens of the risk, needs, responsivity model that we understand that successful re-entry is driven by more than compliance with the terms of release. We are committed to delivering technology to meet client needs to facilitate an ecosystem of behavior modification which will lead to reduction in recidivism. When combined with our robust, no cost, tablet deployment program and the associated embedded free programming and educational content; Securus leads the industry in providing the most comprehensive communication, educational and post incarceration program in the country.



B. Offeror may provide Cellular Phone Detection technology within CDOC facilities

Contraband cellular interdiction services

Securus considers the following information regarding Kamea highly confidential and proprietary. This information has been submitted for CDOC to review and Securus respectfully requests that it be removed from our proposal prior to public display of proposals after opening.

Kamea

Kamea is sensor system that monitors radio frequency emissions from wireless devices within a controlled facility or a prison, utilizing proprietary proximity algorithms along with PDOA (power differences of arrival) technology.

- **Provides the agency with the location of the device(s) in near real-time within a correctional facility.**
- **Uses commercially available technology in conjunction with proprietary algorithms and/or other ancillary equipment to provide one of the most affordable cellular telephone interdiction solution**
- **Continuously monitors the RF environment within the facility and provides key indicators to the analyst for shakedown reports, number of devices seen at any one time, the location of devices seen and sometimes the actual type of device**

As a part of an installation, Securus can install equipment that will assist in the location of every tablet device in the facility. Using a proprietary technology, the Securus tablets are identified by our platform and their location proximity can be determined when they are powered on. The technology also gives us the incremental ability to see other devices broadcasting within the correctional facility, and as a result, this program can delineate between tablets and potential contraband devices that might be present within the facility. Not only can we help you locate tablets or authorized devices, but we can also assist in providing location proximities for those unauthorized devices within the walls of your facilities.

Below is an example of a test site that shows tablet location based on the KAMEA system.



Securus' KAMEA Contraband Interdiction Services is a service that uses RF sensors that monitors radio frequency emissions from wireless devices within a controlled facility or a prison, utilizing proprietary proximity algorithms along with PDOA (power differences of arrival) technology.

This service provides a situational awareness or near real-time high probability of the location of wireless devices within a correctional facility.

KAMEA uses commercially available technology in conjunction with proprietary algorithms and/or other ancillary equipment to provide one of the most affordable cellular telephone interdiction solutions to corrections; when combined with the Securus intelligence-led cellular forensics services, the combination gives the agency the upper hand in controlling contraband cellphones issues.

Below is an example of a test site that shows contraband based on the KAMEA system.



The KAMEA system and services continuously monitors the RF environment within the facility and provides key indicators to the analyst for shakedown reports, number of devices seen at any one time, the location of devices seen and sometimes the actual type of device, such as a Motorola cellphone located in Dorm A pod 1. See Remote Proximity Unit to the right.



System Functions:

- Detection of Cellular Telephones being used as Hot Spots
- Detection of Wi-Fi Enabled Cellular Telephones or other wireless Devices transmitting within the facility
- System-Wide Agency Implementation of an affordable Contraband Cellular Interdiction Program.
- Actionable Intelligence for Digital Forensic Lab, Investigators, and other Partner Intelligence Agencies.
- Total number of wireless devices active within the prison or assessment of the magnitude or number of wireless Devices present

- The KAMEA service offered includes hardware (Remote Proximity Units) for each controlled facility and a full-time analyst that provides situational analysis and identification of contraband cell phones and approximate locations for customer confiscation.

End Kamea proprietary and confidential section.

Mobile Contraband Cell Phone Assessment

Securus' Cellular Assessment Services assist the Department in identifying contraband cell phones within correctional facilities.

The service options available includes the deployment of RF based mobile assessment systems that are temporarily deployed at select facilities to capture, identify and report on all cell phones operating at a facility as well as handheld and fixed devices to augment staff efforts to detect and control contraband cell phones.

Cellphone Forensics services are also provided on any device uncovered or located by the assessment service to help support investigative and prosecutorial efforts.

Proximity, cross referencing with communications data and other investigative information is used to conduct and report on the contraband and assist agencies on the best approach to the issues the assessment uncovers.

Wireless Containment Services (WCS)

Securus Technologies advanced application group, I3 - (Investigations, Intelligence, and Insight), has developed a patented program which provides agencies with contraband cellular device intelligence which leads to proactive and predictive contraband (Cellular/Narcotics) interdiction.

The program can also aid in the detection and identification of individuals who at risk to compromise which could impact the safety and security of the correctional facility, it's staff, offender population and the public. This program can also detect and identify Security Threat Group (STG) Leadership, STG membership and their co-conspirators operating inside and outside correctional facilities.

32. MAINTENANCE

A. Software Modification by the Offeror and Release Management.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

B. Department initiated modification to the software; the Offeror will provide the following:

i. Reasonable delivery date for enhancements, as mutually agreed upon.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has included a preliminary summary Implementation plan, which is included in **Securus Attachment No. 1, Preliminary Project Plan.** More detailed implantation and project plans will be mutually developed to ensure all elements of contractual requirements are included and time-lined to meet CDOC requirements.

C. The Offeror will prepare software releases and stages for testing, validation and acceptance in a test environment. The Department will perform testing for authorization prior to migration to the production environment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

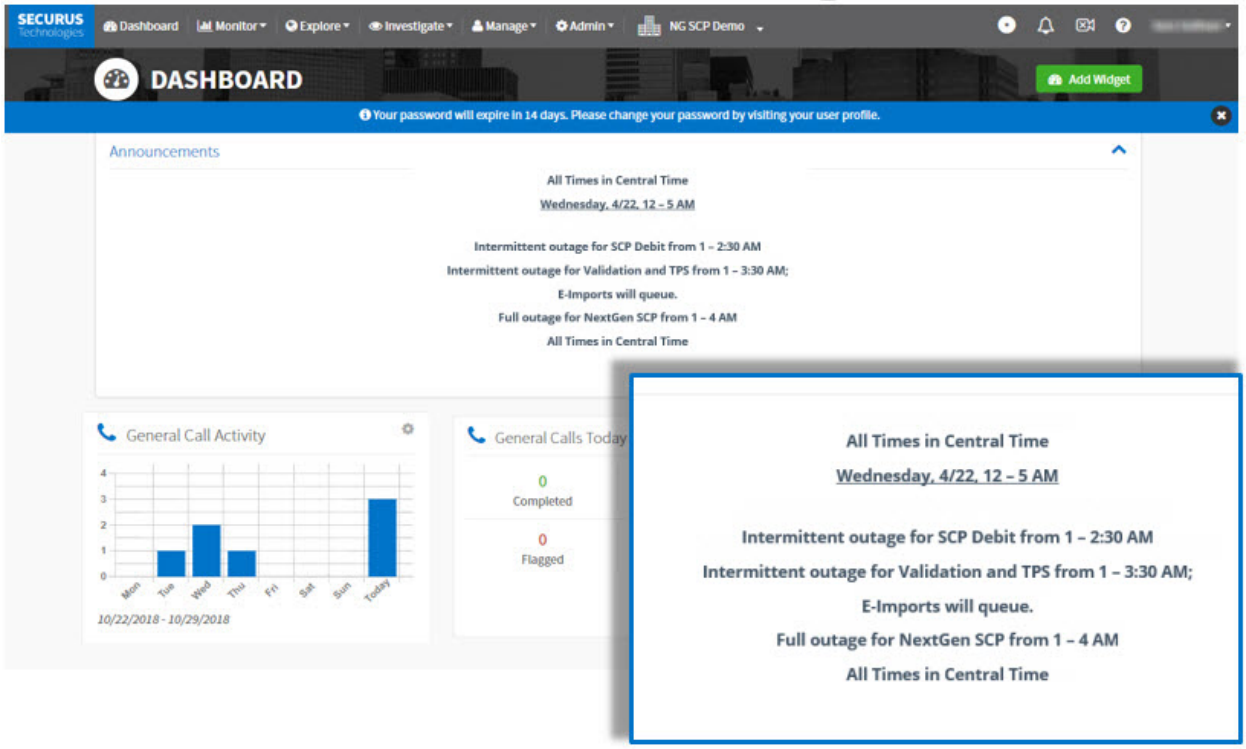
Securus has provided software upgrades on a quarterly basis for years. These will be announced in advance to the CDOC. When required, Securus will work with CDOC personnel to ensure any required testing and validation are done before any software upgrades are made so all upgrades meet the requirements of the CDOC. Before releasing to the CDOC for either testing or migration in production, software goes through testing at Securus in order to ensure the software fully meets the objectives of the enhancements.

Software Upgrades

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCPTM software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



D. The Offeror will provide a maintenance schedule to include frequency, location of service technicians and response time. Downtime will not extend past a 24-hour period.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including the NextGen Secure Communications Platforms™ (NextGenSCP™), network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

Securus Primary Network Operations Center



Securus Network Operations Center



Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including

Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches, and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes to ensure proper operation, and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Infrastructure Inspections

System Administrators make scheduled inspections of all systems and routinely perform preventive maintenance and software enhancements as directed by a Production Change Control steering group. In addition, Securus change control practices have been reviewed and are compliant with PCI DSS and our Internal Controls for Financial Reporting.

E. The Offeror will provide support for the equipment Monday through Friday 8:00 am to 5:00 pm MST.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Support for the equipment will be available Monday through Friday 8:00 am to 5:00 pm MST.

F. The Offeror will provide a toll-free customer support telephone number when service is needed.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides superior customer service from a state-of-the-art operations center located in Carrollton, Texas. More than 50 technicians staff the Securus Technical Support Center (TSC) to ensure prompt problem resolution. The average tenure of our technicians is 8 years and the average tenure for our technical support management is 10 years.

The Securus TSC serves as a single point of contact for facility staff to request service **24 hours a day, seven days a week, 365 days per year.** There are three ways to contact the TSC:

- Telephone: 866-558-2323
- E-Mail: technicalsupport@securustech.net
- Fax: 800-368-3168

The TSC uses a call distribution system to manage the flow of inbound customer calls automatically routing calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our objective of providing timely resolution to each request.

Technicians assign each service request one of three initial priority levels, each with resolution and escalation timelines. Every effort is made to resolve the problem remotely within the designated timeframes, and Securus resolves most service requests during the initial request. If necessary, a field service technician is dispatched to the facility to expedite resolution.

The TSC uses an event tracking system that logs, tracks, manages and assures appropriate response to all service requests. The service request generates a trouble ticket with priority level assignment that drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem and either resolves the problem or engages an appropriate party for problem resolution. The TSC retains ownership of all service requests and is responsible for the escalation and update functions.

Service Response Times and Escalations

Priority Level	Service Priority Description	Response Time	Customer Communication Guideline	Escalations
P1	A P1 is our highest service level defined as 30% or more of the functionality of the System being adversely affected by the System Event. Examples of P1 service assignments would include items such as no voice prompts, features not operating appropriately, inability to	2 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required, Securus	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request

	burn CD's, issues with listening to live calls, inability to access NextGen Secure Communications Platform™ UI, all phones down.		Dispatch or Field Service Technician contacts the customer with an estimated time of arrival	• Technical Support Manager & Field Service Manager • Director, Customer Success & Director, Field Operations • Chief Operating Officer
P2	A P2 assignment defined as 5% to 29% of the functionality of the System being adversely affected by the System Event. Examples of a P2 service assignments would include items such as workstation, specific system ports, LEC circuits, unblocks, block numbers, missing CDRs, call searching.	24 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager • Director, Customer Success & Director, Field Operations • Chief Operating Officer
P3	A P3 assignment defined as less the 5% of the functionality of the System being adversely affected by the System Event. Single and multiple phones related issues. Examples of P3 service assignments would include items such as static on the phone, a party not being able to hear, unable to dial, a broken phone, dial pad not working, cutoff switches not working, and	72 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager

	inability to generate reports.		an estimated time of arrival	• Director, Customer Success & Director, Field Operations • Chief Operating Officer

G. The Offeror will provide a detailed plan for customer support during non-business hours. Non-business hours are; 5:00 pm to 8:00 am Monday through Friday, with 24- hour availability on weekends and holidays.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Through the Technical Support Center, detailed above in requirement "F," customer support is available 24/7/365.

H. The Offeror will maintain the maintenance schedule and equipment installation at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Maintenance and equipment installation are included in the RFP response and is provided at no additional charge.

I. There will be no additional installation cost to the CDOC for changing out equipment that need repair or replacement. The Offeror will be responsible for any expenses required for the repair of the equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All repairs and equipment replacements are included in the RFP response and are provided at no additional charge.

J. The Offeror will coordinate all services, maintenance and repairs in advance with the approved CDOC personnel. Offeror will contact the affected facility for entry approval regarding maintenance and repairs.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work closely with CDOC personnel to ensure all service and maintenance are coordinated to meet the requirements of the CDOC. CDOC personnel will be contacted prior to any on=site visits to ensure all safety and regulatory protocol are followed and to best meet the needs of CDOC personnel.

K. The Offeror will provide all necessary labor, parts, materials, and transportation to maintain the hardware and software of the OCS equipment and maintain compliance with the equipment manufacturer's specifications throughout the life of the Contract. No

charge will be made to the CDOC for maintenance of the OCS equipment and/or environment infrastructure.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide all necessary labor, parts, materials, and transportation to maintain the hardware and software of the OCS equipment and maintain compliance with the equipment manufacturer's specifications throughout the life of the Contract. No charge will be made to the CDOC for maintenance of the OCS equipment and/or environment infrastructure.

L. The Offeror will provide for continuous on-line diagnostics and continuous oversight as well as local remote offline control access for advanced programming and diagnostics of the tablet environment. Access to the built-in advanced diagnostics and program control will be accessible via the network by service center personnel and will provide failure reports, service history and other diagnostics.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Within the function of the Network Operations Center, on-line diagnostics and continuous system oversight is on an on-going basis.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including the NextGen Secure Communications Platforms™ (NextGenSCP™), network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches, and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes to ensure proper operation, and their vital operating statistics sent every 10 minutes.

Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

Reports

Securus offers a wide array of reports to meet CDOC needs and provide for effective data necessary to efficiently manage the system. In addition, Securus will work with the CDOC to create and provide additional reports as necessary.

The NextGen Secure Communications Platform™ (NextGen SCP™) is very flexible and easy to use, and allows the user to create almost limitless reporting. Should customized reports be needed, Securus will provide them to CDOC at no charge except in those cases where the customized report would require a significant allocation of resources or material changes to Securus systems and procedures.

In the small number of instances where development is needed (e.g. capturing additional information from other systems), Securus will provide the development free of charge unless the request involves significant cost to Securus. In such cases CDOC will be given the option to pay for the additional services without markup by Securus.

M. The Offeror will provide their on-site repair time, method and proposed level of services for the facilities. Offerors will detail their ability to handle emergencies.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides superior customer service from a state-of-the-art operations center located in Carrollton, Texas. More than 50 technicians staff the Securus Technical Support Center (TSC) to ensure prompt problem resolution. The average tenure of our technicians is 8 years and the average tenure for our technical support management is 10 years.

The Securus TSC serves as a single point of contact for facility staff to request service **24 hours a day, seven days a week, 365 days per year.** There are three ways to contact the TSC:

- Telephone: 866-558-2323

- E-Mail: technicalsupport@securustech.net
- Fax: 800-368-3168

The TSC uses a call distribution system to manage the flow of inbound customer calls automatically routing calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our objective of providing timely resolution to each request.

Technicians assign each service request one of three initial priority levels, each with resolution and escalation timelines. Every effort is made to resolve the problem remotely within the designated timeframes, and Securus resolves most service requests during the initial request. If necessary, a field service technician is dispatched to the facility to expedite resolution.

The TSC uses an event tracking system that logs, tracks, manages and assures appropriate response to all service requests. The service request generates a trouble ticket with priority level assignment that drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem and either resolves the problem or engages an appropriate party for problem resolution. The TSC retains ownership of all service requests and is responsible for the escalation and update functions.

Service Response Times and Escalations

Priority Level	Service Priority Description	Response Time	Customer Communication Guideline	Escalations
P1	A P1 is our highest service level defined as 30% or more of the functionality of the System being adversely affected by the System Event. Examples of P1 service assignments would include items such as no voice prompts, features not operating appropriately, inability to burn CD's, issues with listening to live calls, inability to access NextGen Secure Communications	2 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager • Director, Customer Success & Director, Field Operations

	Platform™ UI, all phones down.		an estimated time of arrival	• Chief Operating Officer
P2	A P2 assignment defined as 5% to 29% of the functionality of the System being adversely affected by the System Event. Examples of a P2 service assignments would include items such as workstation, specific system ports, LEC circuits, unblocks, block numbers, missing CDRs, call searching.	24 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager • Director, Customer Success & Director, Field Operations • Chief Operating Officer
P3	A P3 assignment defined as less the 5% of the functionality of the System being adversely affected by the System Event. Single and multiple phones related issues. Examples of P3 service assignments would include items such as static on the phone, a party not being able to hear, unable to dial, a broken phone, dial pad not working, cutoff switches not working, and inability to generate reports.	72 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager • Director, Customer Success & Director, Field Operations • Chief Operating Officer

Emergency Response

The Securus Disaster Recovery Plan is designed for rapid response with unmatched service and support in any circumstance. Our goal is to prevent or minimize down-time and remove your administrative burdens. **Securus takes care of communications and technology while you take care of your population and facilities.**

- Robust network architecture designed to mitigate issues before they occur
- Field service team readily positioned close to your facilities and on-call 24/7
- A plan for escalating issues, adding resources, and recovering quickly

If a natural disaster or other significant adverse event occurs, CDOC has the full support of the Securus Network Operations Center, the Securus Technical Support Team including engineering resources, and the Securus Field Service Team, including over 290 Field Service Team members with an average of seven years tenure, supported by a centralized field dispatch team. **Our Field Service Technicians are fully trained in our disaster recovery plan and processes**, and they are strategically positioned to support your ongoing maintenance and fast response in emergencies.

Response operations begin as soon as personnel safety is assured, and all emergency recovery operations are prioritized by critical facilities and equipment locations. For situations that are expansive in nature, we prioritize maximum-security sites and facilities with high offender phone usage.

Securus' Three-Tiered Approach to Disaster Response and Recovery

1. **Facility-Specific Emergency Response Checklists**
   For every facility, Securus develops an emergency response checklist to protect equipment and personnel in the event of an emergency. These procedures may be as simple as using sandbags to stabilize equipment and placing tape on windows exposed to high winds. Your checklists will focus on mitigation and recovery with contingencies for extreme conditions such as earthquakes, flash floods, power outages, etc. Each checklist will be coordinated with CDOC for consistency with your policy and procedures.
2. **Systemwide Disaster Response Plan**
   Securus works with you to declare emergencies for situations that are catastrophic and may impact a localized area or wide-spread region. Recovery plans are triaged based on the extent of impact and recovery operations may last a few hours, days, or weeks. Securus prioritizes recovery of premise-based equipment by facility type and equipment location. The Securus Local Recovery Team will continue recovery

operations until operations are restored. Retrospective reports are completed for all declared emergencies to advance our emergency recovery planning efforts for the future.

3. **A Foundation of Network and Equipment Preventative Measure**s
   CDOC avoids many communications-related disasters because we are prepared: Securus provides a network and infrastructure tested to withstand adverse conditions, minimize outages, and protect your data. We research what works and then we implement continuous improvements. Securus adds layers of redundancy at the local and national level to our core network and operations centers. We stock your facility and our Field Service Team with spare parts. We back up your data at three geographically diverse Securus data centers and layer redundancy throughout each component of our network. Information is routed through geographically diverse and route-diverse network paths, all while we monitor operations and communications 24x7x365.

Additional details on the Securus Disaster Recovery Plan and our preventative measures are outlined on the following pages. It's difficult to contemplate every contingency, but with 30+ years of experience providing communications and technology services to the corrections industry, **Securus has the experience to take care of CDOC even when the unexpected occurs.**

CDOC Emergency Condition Declaration

If you encounter a catastrophic adverse event or disaster at your facility, immediately call the Securus Emergency Numbers that you are provided. Your call will be answered 24x7x365. Then with your Securus Account Manager you will request that Securus General Manager declare an emergency condition. Operations management then establishes an immediate conference bridge with the appropriate participants to gather information substantiating that an emergency status is warranted and determines the Disaster Level.

A single event trouble ticket is used to track all recovery efforts. The Securus Technical Support Team will open a new trouble ticket in our ticket tracking system, indicating the declared condition level and the date and time of the declaration. All open tickets pertaining to the ongoing emergency recovery effort will be linked so that all recovery efforts are tracked as a single incident to facilitate complete resolution. This is critical for efficient and complete resolution in situations of extended recovery.

If needed, Securus will deploy and pull resources from our nationwide network and engage our vendors to supply additional resources, equipment, or manpower.

Securus Emergency Response Disaster Levels

Disaster Level 1

Securus provides a full-headquarters response and may deploy a Headquarters Response Team to the region to coordinate and assist local recovery efforts. Securus Local Recovery Team activated, and your Account Manager will work with you to initiate a Command Center, including Securus Leadership. Necessary skill levels and geographic proximity are matched to your site's needs; additional personnel are dispatched as needed.

Disaster Level 2

Securus Headquarters Response Team assists Securus Local Recovery Team as needed; onsite technician requirements assessed, and additional personnel dispatched as and when needed.

Disaster Level 3

Securus Local Recovery Team coordinates all recovery operations. Headquarters assistance beyond standard Network Operations and Technical Support Teams likely not required.

Risk Mitigation and Proactive Monitoring

The Securus Network Operations Center (NOC) continuously monitors all data centers, infrastructure components, platform systems, and network/communication systems using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.



The Securus NOC also monitors real-time video surveillance and environmental alerts for the Securus data centers. In the event there is an issue at the Securus Network Operations Center, Securus maintains a fully redundant backup Network Operations Center at a separate physical location.

The Securus Technical Support Team monitors all facility-based equipment and connectivity 24x7x365 including firewalls, integrated access devices (IADs), visitation phone monitoring (VPM) units, routers, switches, on-site systems, wireless access points, user interfacing kiosks and terminals, and uninterrupted power supply (UPS) systems.

The systems are polled every two minutes and their vital operating statistics sent every 10 minutes. In addition to real-time monitoring and alerting, Securus Technical Support also leverages network performance monitor tools to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. This ongoing, proactive, in-depth analysis of your systems' performance enables our Technical Support Team to prevent and mitigate facility issues.

Data storage redundancy is a key component of Securus' Risk Mitigation and Disaster Recovery Plan. Securus maintains three data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.995% availability.



Securus' data centers meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier III, with some Tier IV (highest level) attributes, for data centers including:

- ability to withstand a 96-hour power event
- multi-layer physical security
- multiple power delivery paths

Each data center has redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity.

Securus' data centers are staffed 24x7x365 for immediate physical assistance inside the data center.

Data is no longer susceptible to loss due to an individual drive failure or issues at your location: The Securus communication platform uses technology that is much more advanced than traditional local onsite storage. Securus uses a mix of Storage Area Network (SAN)—a high-speed sub-network of shared storage devices—and Network-Attached Storage (NAS). This architecture avails all storage devices to all servers on Local Area Networks (LANs) or Wide Area Networks (WANs). Data is stored in Redundant Arrays of Independent Disk (RAID) formats, spreading the data across multiple drives, which provides additional protection. Accordingly, this architecture provide facilities with the ultimate protection against single drive or server failures, as well as increased security. **Securus maintains hardware replacement inventory on your site, in our Field Service Team vehicles, and at centralized locations.** In

addition, we have distribution agreements with our vendors so that in the event of disaster recovery efforts, we can get replacement equipment to your facilities quickly.

Localized Event Affecting Only Securus Facilities

In the event of a disaster impacting Securus, the local Securus Network and systems, or NextGen SCP, Securus immediately assembles a team of engineers to investigate and restore services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and a list of third-party vendors to engage if needed. Our priority is fast resolution and minimal downtime. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Upon confirmation of a service-impacting event, the Network Operations Center will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

The Securus Executive Team and the Securus Account Management Team receive SIRs and communicate with you directly. In addition, the Securus Technical Support Team may communicate a service-impacting event via a splash screen on the NextGen SCP user interface introductory page. Securus updates you regularly throughout resolution. Securus investigates every service-impacting event, completes a root-cause analysis, and provides the analysis to you upon request.

33. ESCALATION PLAN

A. Offerors will provide all priority 1, 2, 3 and 4 tickets as they are opened, updated and closed by the field technicians, providing details to show the problem and final resolution of said problem.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide all priority tickets as they are opened, updated and closed by the field technicians. They will include details to show the problem and final resolutions of the problem addressed by the ticket. A detailed overview is provided in requirement No. "J" below.

B. The Offeror will provide the authorized CDOC staff with a complete list of business, cellular and pager numbers for its Offerors/subcontractors, managers, administrators, technicians, etc. The Offerors management home and emergency telephone numbers must also be furnished.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Upon contract award, Securus will provide authorized CDOC staff with a complete list of business, cellular and pager numbers for its Securus'/subcontractors, managers, administrators, technicians, etc. Securus's management home and emergency telephone numbers will be furnished, with the expectation these numbers will only be shared within legitimate fulfillment of the contract.

C. Either party will report to the other party any misuse, destruction, damage, vandalism, liability, etc. on all Offeror installed OCS equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will report to CDOC any misuse, destruction, damage, vandalism, liability, etc., on all Securus-installed OCS equipment.

D. All issues surrounding the OCS environments will be reported by the Offeror to the authorized CDOC staff.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All issues surrounding the OCS environment will be reported to appropriate CDOC staff as they occur and on any regular basis agreed to in establishing the implantation plan.

E. The Offeror will have the ability to perform remote diagnostics to the ITS to determine if a problem is with the telephone or with the telephone line.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus employees continuously monitor our NextGen Secure Communications Platform™ (NextGen SCP™) from our Network Operations Center (NOC) at our headquarters in the Dallas, Texas, metro area. The NOC is staffed 24x7x365 by network experts certified in the systems and software used to monitor all NextGen SCP functions and equipment, as well as the associated network. The NOC maintains failure reports, service history, and other diagnostic information, which are available to the CDOC when requested.

The NextGen SCP platform provides continuous online supervision and diagnostics—as well as offline system access—for advanced programming, diagnostics, troubleshooting, and call traffic analysis. The Securus service center personnel can access the NextGen SCP advanced diagnostics and program control for failure reports, service history, and other diagnostic information.

The NOC reports any actions required to prevent or repair any outages to each Securus employee supporting CDOC. Securus will follow CDOC's protocols for communicating outages or repair actions in the unlikely event they occur.

F. The Offeror will be responsible for any expenses required for the repair of the equipment.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All repairs and replacements are covered in the maintenance provided to the CDOC under the contract fulfilling the terms of this ITN.

G. Describe methods of dealing with problems, complaints and response time.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

H. The successful Offeror is expected to provide the following support services for equipment placed within the CDOC that include but are not limited to:

i. Unlimited phone support;

ii. Updates and upgrades;

iii. Security-related updates to their proposed solution, which may be called updates, upgrades, patches, service packs, hot fixes, or workarounds.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Maintenance and support will include unlimited phone support, updates and upgrades, and security related updates to the phone, video, and tablets solutions Securus

provides. This includes updates, upgrades, patches, service packs, hot fixes or workarounds.

I. The Offeror will propose, provide, and describe their solution for change management. These must include at a minimum:

i. Version number;
ii. Description of the change;
iii. How the change was initiated (i.e. user or system support);
iv. Person requesting the change;
v. Person responsible for the change; and
vi. Date and time of the change.

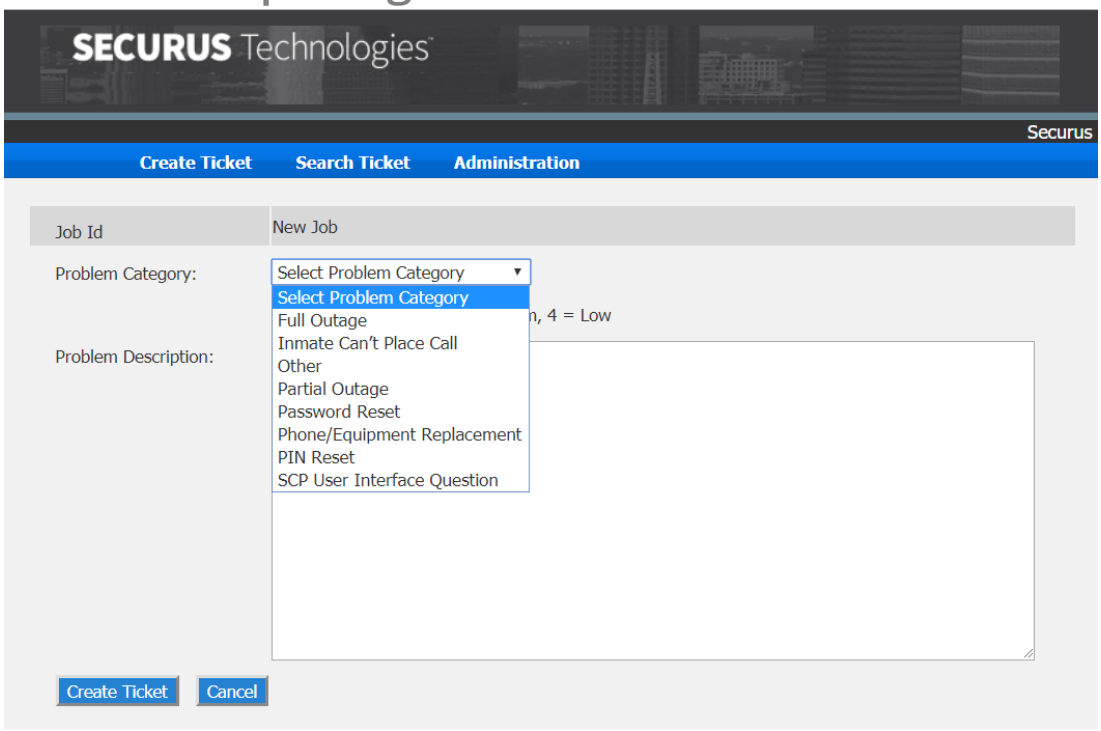
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Change management is generally accomplished through the upgrades process or the ticketing process (described in requirement "J" immediately following this response.

Ticketing Process and fields addressed:

As shown here, the ticketing process provides a drop-down menu for the description of the issue being addressed.

Opening a New Service Ticket



Upgrades

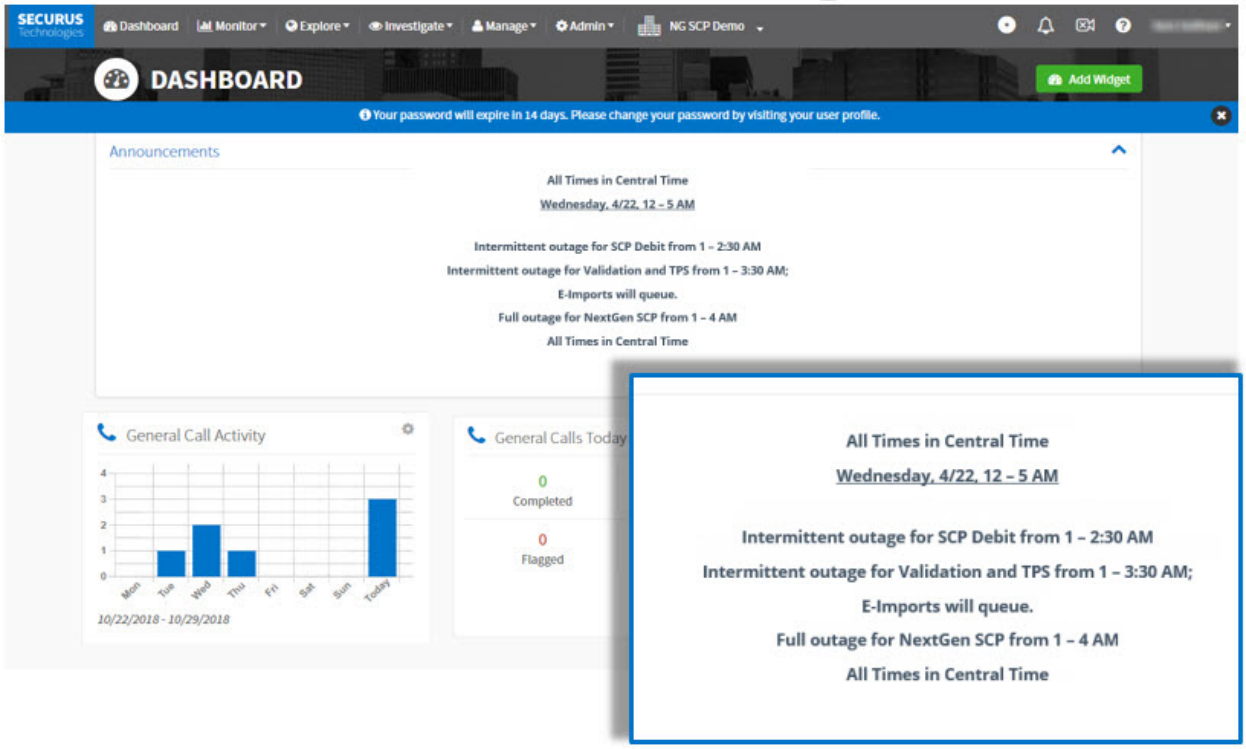
Securus has provided software upgrades on a quarterly basis for years. These will be announced in advance to the CDOC. When required, Securus will work with CDOC personnel to ensure any required testing and validation are done before any software upgrades are made so all upgrades meet the requirements of the CDOC. Before releasing to the CDOC for either testing or migration in production, software goes through testing at Securus in order to ensure the software fully meets the objectives of the enhancements.

Software Upgrades

Current technology provides better support and higher satisfaction: Securus delivers NextGen SCPTM software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

Minimize disruptions to communications and your work: To deliver updates and perform maintenance events, Securus uses an after-hours process. CDOC will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

Announcement Widget



J. Offeror is expected to include proposed escalation plan with their proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

In 2009, Securus made a strategic decision to centralize management of all technical support. Today, Securus provides superior customer service capabilities from a state-of-the-art technical support center located in the Dallas, Texas, metro area.

Approximately 50 technical professionals staff the Securus Technical Support Center (TSC) which handles approximately 8,000 inbound queries per month. The TSC provides a single-point-of-contact for Securus customers for issues ranging from minor maintenance issues to service outages. Clients can contact the TSC 24x7x365 by any of the following convenient methods:

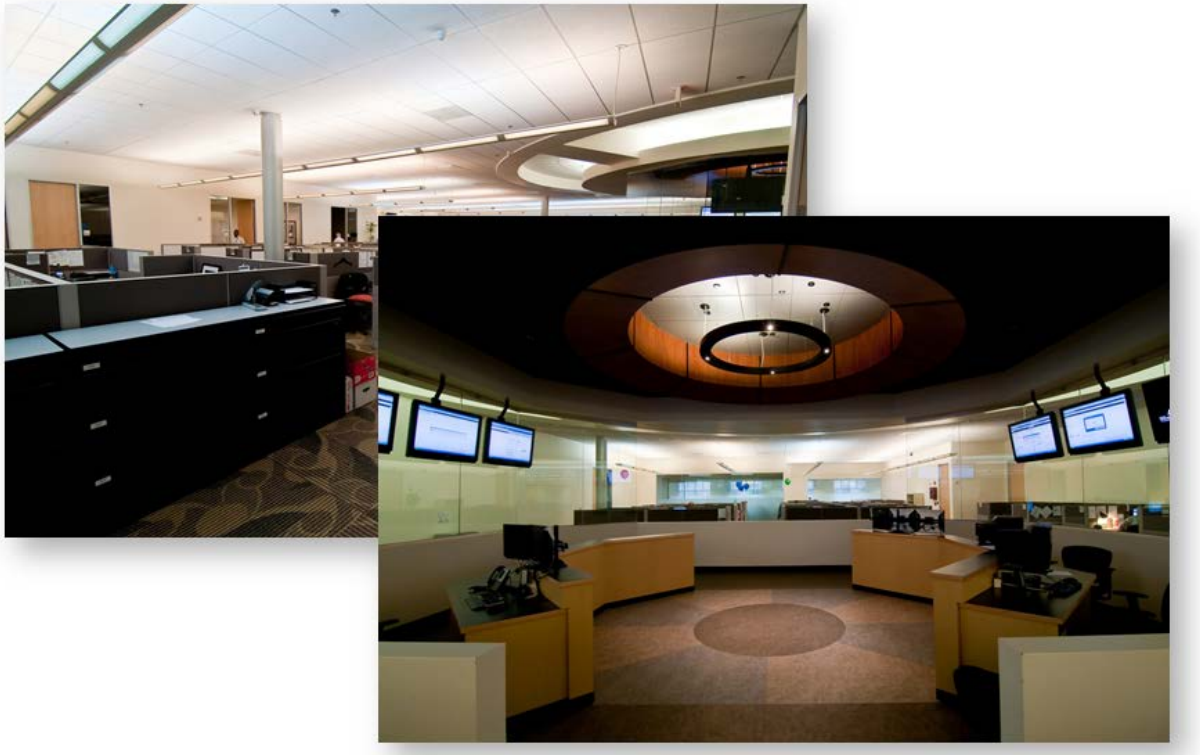
- **Telephone** – 866-558-2323
- **E-Mail** – technicalsupport@securustech.net
- **Fax** – 800-368-3168
- **Web portal** - http://www.securustech.net/facility/Default.asp

The technical service center offers our clients:

- Technical support and field dispatch 24x7x365

- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure achievement of Service Level Agreements
- Certified technicians to provide quick problem resolution
- System and individual site connectivity monitored 24x7x365

24x7x365 Securus Technical Support Center



Securus technicians receive internal Securus certifications, based on our business and the products and services we support.

Service Levels

When a facility calls Securus, an event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a prescribed resolution timeline and escalation procedure. In all cases, Technical Support will respond to the customer within the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects 30 percent or more of system functionality. Examples of P1 service assignments include:

- Voice prompts not operating
- Features are not operating appropriately
- CD-burning abilities disabled
- Live call monitoring is not operating appropriately
- NextGen SCP access denied
- All phones out-of-service

The response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

A P1 events escalate to:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If the problem resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment—our mid-level priority assignment—occurs when a system event adversely affects 5 to 29 percent of system functionality. Examples of a P2 service assignment include problems or errors with related to:

- Workstation
- Specific system ports
- Local Exchange Carrier (LEC) circuits
- Unblocks
- Blocked numbers
- Missing call detail records (CDRs)

- Call searching

The response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P2 events escalate to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment—our lowest priority assignment—occurs when a system event adversely affects 5 percent or less of system functionality. System events adversely affecting some of available facility phones. Examples of P3 service assignments include:

- Static on the phone
- A party's inability to hear
- An offender's inability to dial
- A broken phone
- Non-functioning dial pad
- Non-functioning cutoff switches
- An inability to generate reports

The response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P3 events escalate to the Technical Support Department.

Escalations

If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

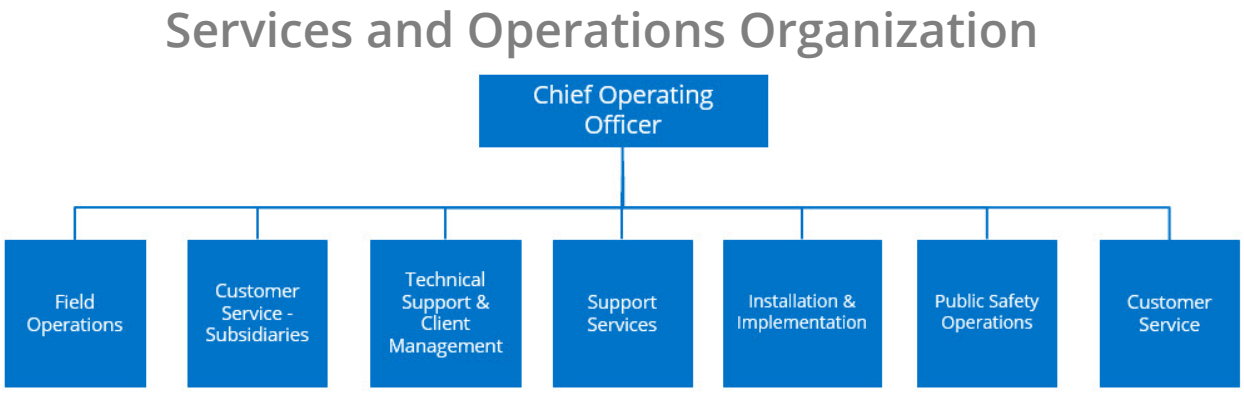
The supervisory escalation chain is:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Chief Operating Officer

Centralized Services Operations Model

All Securus services and operations are managed centrally, from our Service and Operations organization in Dallas, Texas. The Operations team's responsibility is supporting external customers, including Customer Service, Field Services, Installation and Engineering, and Technical Support. The Support Services team provides internal support services including Quality, Training and Customer Satisfaction, and Reporting and Analysis.

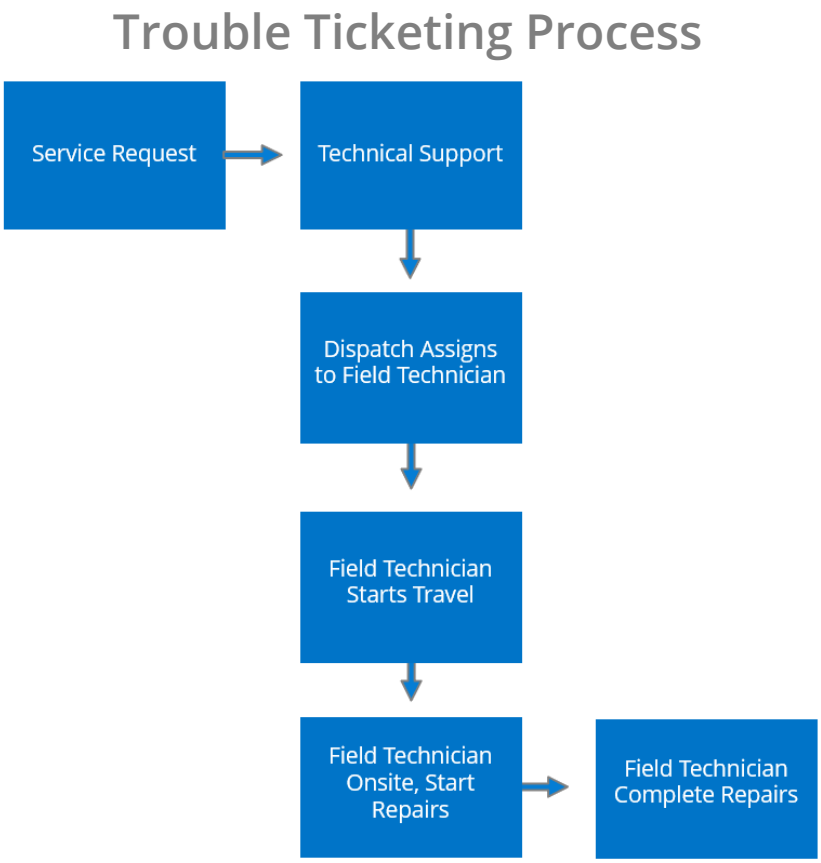
The following figure illustrates the Securus Service and Operations organization, which is staffed by full-time Securus employees.



Securus adopted this operational model because of the natural interaction between functional groups. Having our support services integrated and centrally managed enables cross-functional group interaction, improving the response time, and efficiencies of our services.

Call Routing

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.



In all instances, service will be requested through the TSC and field service personnel will be dispatched through trouble ticketing system to ensure documentation and timely resolution of all service tickets.

Event Tracking System

The Securus event tracking system logs, tracks, manages, and assures an appropriate response to all service requests. The service request generates a unique trouble ticket number linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.

The TSC maintains ownership of all service requests and responsibility for the escalation and update functions. Every effort is made to resolve problems remotely and within the framework of resolution timeframes. However, if the problem requires on-

site service, a technician is dispatched. Securus will contact the facility to arrange for the on-site service at the convenience of the facility.

Facilities can also use Securus' request portal to create self-help tickets and monitor and track ticket status.

Facility Service Request Portal

CDOC can access Securus' service request portal as an alternative to calling Securus Technical Support to create new service requests or to track the status of existing service requests.



Securus' service request portal is an automated ticketing system that logs, tracks, manages, and assures appropriate responses to all service requests for a correctional facility, regardless of whether the request was initiated from a call to Securus Technical Support or entered directly into the service request portal.

The service request portal is one of the major tools in our arsenal to meet service level agreements with confidence, increase overall operational effectiveness, solve problems, streamline repetitive tasks, and improve customer satisfaction.

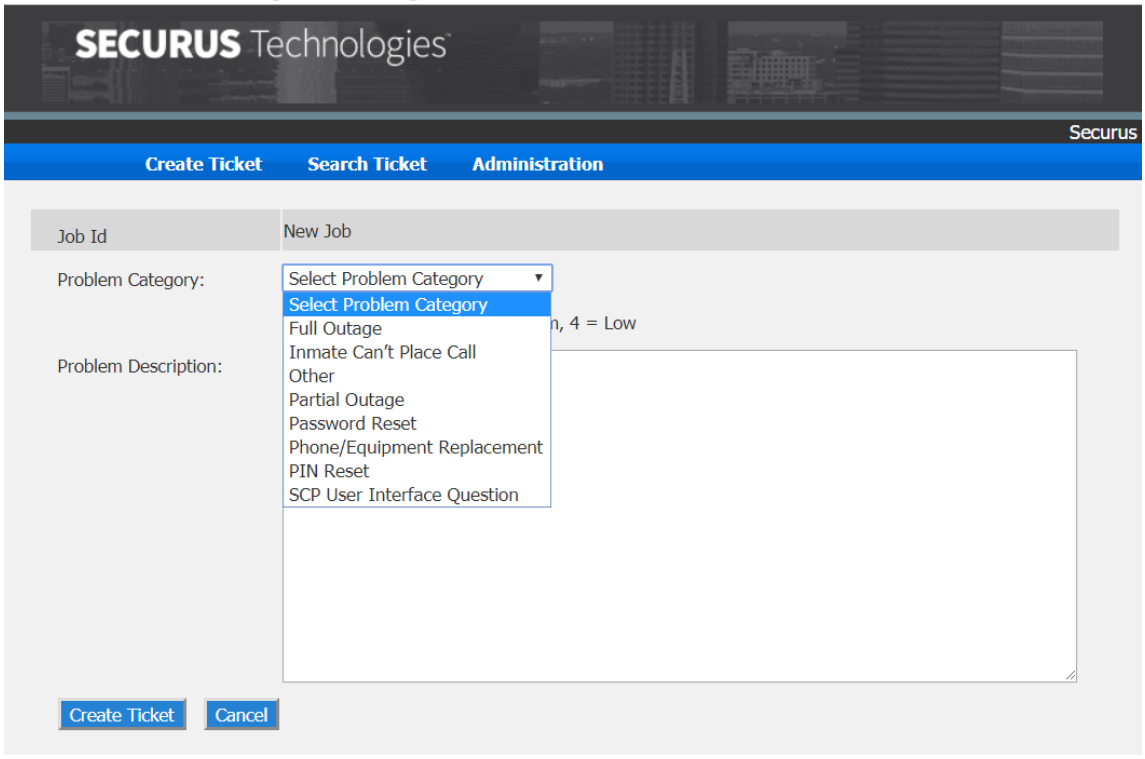
When a facility requires a service visit for any reason, including routine maintenance, a service ticket is opened and visible within the service request portal to track the event and allow for further analysis of any system issues and/or performance.

As with all service requests, those entered directly into the service request portal include information collected on the issue as gathered by the certified technician(s) to ensure our response is appropriate for the service event. Diagnosis of the event will determine whether the request or repair can be performed remotely or if onsite trouble-shooting assistance with our local field technician, working in conjunction with our Network Operations Center (NOC), is necessary. All service events, whether resolved remotely or via an onsite visit, are tracked and our customers can provide feedback on how we have performed and if we met their expectations. Further, the service event will be assessed to avoid repetitive service issues, which may indicate a system deficiency issue or fraudulent activity.

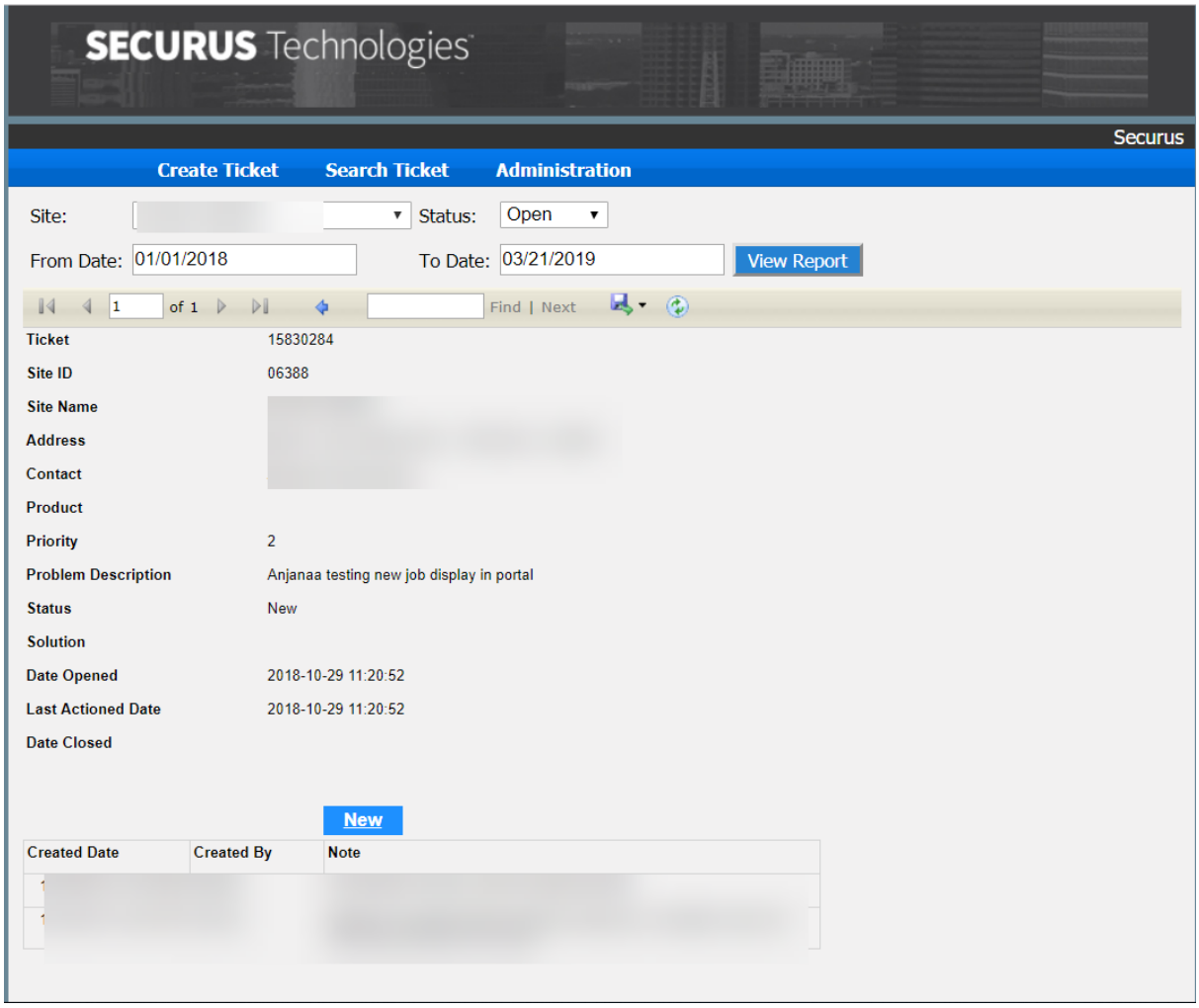
The service request ticketing system is used in various departments throughout Securus to provide a current view of any open items. The system automatically generates reports internally that are sent to management for service level reviews and customer status.

Through the Securus service request portal, CDOC staff can view, track, and open service tickets; the portal also offers CDOC the advantage of knowing the status of a resolution or viewing comments on any service request, which results in efficient and effective communication through this direct line of communication without needing to place a call.

Opening a New Service Ticket



Ticket Number with Detail



34. TRAINING BY OFFEROR

A. The Offeror will provide training to authorized CDOC personnel at the locations where the equipment is installed. Additional training will be provided to new authorized CDOC staff assigned during the Contract period, at no cost to the CDOC, at the respective CDOC facilities. Video conferencing and/or webinar are acceptable.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides product training for all NextGen Secure Communications Platform™ (NextGen SCP™) features in the agreement with the CDOC. Experienced Securus employees conduct all training through online instructor-led classes or on-site, one-on-one and classroom training sessions at no cost. We deliver standard training using both hands-on experiences with your data and using instructor demonstrations to ensure each trainee understands all NextGen SCP functions.

Securus training programs enable facility staff to use all features the first day of installation. Since our products are web-based, after a two or three-hour training session, most facility staff can easily maneuver through the system's features.

In addition to standard training, Securus will develop an online training experience to meet the unique needs of your staff and facility. We offer separate classes focused on different agency functions such as investigations, live call monitoring, and system administration. Securus offers online instructor-led courses available twice a month throughout the year for product upgrades, new facility staff, or general refreshers. *Securus' ongoing training ensures your staff always "stays on top" of current and newly released NextGen SCP features*.

NextGen SCP Training Course Modules

Securus is committed to providing your staff with training that will maximize the potential of the features implemented at your facility. Training courses are offered in a user-friendly, task-oriented format to teach your staff what they need to know to do their jobs. We present courses in separate modules based on the types of duties officers tend to perform using the NextGen SCP offender telephone system while focusing on the unique features of our applications.

The following table presents the standard NextGen SCP training course modules and associated learning objectives.

NextGen SCP Course Modules:
Offender Telephone System

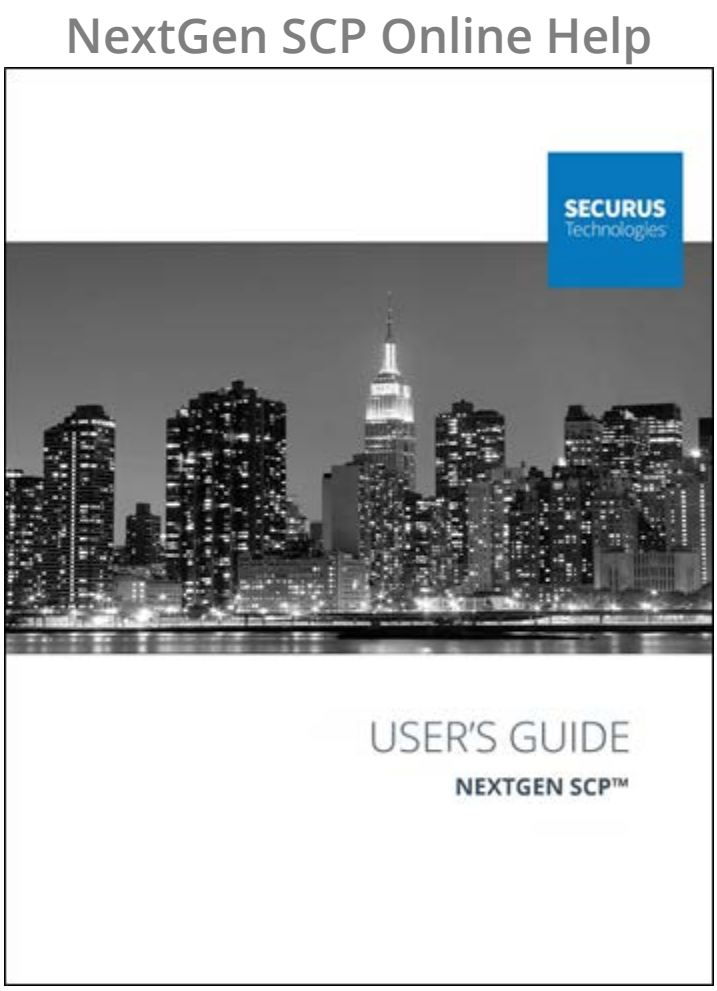
Course Module	Objective
Overview and Navigation	• Logging-in • Navigating through the features • Managing user password • Managing user profile • Manage system utility icons
Dashboard	• Review system announcements • Manage widgets
Monitor	• Monitor live calls • Forward Live Calls • Add Notes to Live Calls
Explore	• Review Offender Activity • Review Communication Records • Control Covert Alerts • Review System Logs • Review PAN Frequency
Investigate	• Open Investigator Pro • Open THREADS • Open ICER • Open WCS
Manage	• Offenders • Offender PAN • eMessaging
Administration	• Control Facility and Sites • Control Phone Numbers • Control Call Settings • Create Security Roles • Manage Users

NextGen SCP Online Help

Securus also provides online self-help available, at all times, from a convenient Help menu accessible through NextGen SCP. Trainees use this PDF document to find quick answers to their questions about NextGen SCP. Keyword searching offers immediate access to the information or users can follow the table of contents for a full learning experience. Step-by-step instructions are designed to help the user complete tasks.

Officers can print one topic or the entire help system if a full user manual is preferred. Securus continuously upgrades and enhances NextGen SCP, so we recommend only printing the section needed to ensure all printed material is current.

The following figure illustrates the NextGen SCP online PDF document.



B. Training manuals will be provided to authorized CDOC staff at all training meetings at no cost to the CDOC. All manuals will become the property of the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Training manuals will be provided as needed by mutual agreement. Many materials will be on-line, via web instruction, and in-person training. This will be provided at no cost to the DOC, and all manuals will become the property of the CDOC.

C. Informational pamphlets will be available for offenders' relatives to explain applicable features and functionalities of the kiosks when requested by the authorized CDOC staff, at no cost to the CDOC.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide informational materials for offenders' relatives to explain applicable features and functionalities of kiosks upon request at no cost to the CDOC.

D. Offeror provides in-depth training on tracking, researching, and investigating calls, videos, mail, email, messaging, and any other communication solution.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Training covers all these topics and trainers are available for follow-up sessions as required. All training is included in the proposal.

E. Offeror is expected to include proposed training materials with their proposal.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has included sample training documents in **Securus Attachment No. 6, Sample Training Documents.**

35. OFFEROR RESPONSE INSTRUCTIONS

A. Executive Summary

In no more than two (2) to five (5) pages, furnish a cover letter to introduce the firm and its qualifications. The Executive Summary should provide the reader with an overall understanding of the response and the Offeror's approach.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

A cover letter and executive summary are included in the ITN document, which is included in the submission.

B. Program Management Plan

Submit a program management plan demonstrating how the Offeror proposes to accomplish the statement of work requirements through the seamless integration of its diverse organizational elements, personnel, and subcontractors to ensure quality and continuity of operations throughout the contract lifecycle. In addition, demonstrate how the Offeror will apply new technologies and processes to improve efficiency. The program management plan, at a minimum, shall address the following:

i. An organizational chart(s) that shows the corporate structure and management reporting structure.

ii. Financial Capability

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has decades of experience in managing installations and projects in the corrections industry. This plan is described below.

- Organizational charts are included in S**ecurus Attachment No. 5, Complete Org Chart and Entities.**
- A two-year history of Securus' Audited Financial reports are included in the response as a separate file as required in the ITN instructions.
- A sample Implementation/Project Plan is included as **Securus Attachment No. 1, Project Plan.**

Securus has extensive experience installing and maintaining offender telecommunications systems and has developed installation and cut-over procedures that minimize disruptions and errors and maximize customer satisfaction. Securus has developed a preliminary implementation plan that includes all of the required components.

Implementation Plan

Securus has a proven track record of providing successful turnkey installations for mega-county, county, and city agencies, as well as large state department of corrections agencies. Over the last several years, our team has completed more than 2,800 quality installations of our calling service and has averaged a 4.6 (out of 5) customer satisfaction rating every year.

Recent customer testimonials include:

> "I could not be more pleased with the quality and professionalism of the SECURUS personnel associated with the installation of our inmate telephone system."
>
> *- Captain John Donegan – Suffolk County Jail, Riverhead, NY*

> "The Securus installation team is the most professional group of people that I have ever had the pleasure of working with on this type of project. Their attention to detail and dedication to customer satisfaction allowed them to complete a statewide, multi-location installation well under the projected completion date with virtually no unforeseen problems. I would love to work with them on another project."
>
> *-- Karl Prince, IT Manager, Louisiana DOC*

The Securus Project Team consistently demonstrates project management expertise that simply cannot be matched by any other service provider. We look forward to the opportunity to provide the CDOC with industry-leading project support and services.

Project Description

The CDOC implementation project includes a complete, turnkey installation of all equipment, facilities, and connectivity for offender telecommunications services.

Project Plan Overview

The project plan identifies the deployment of specific technologies under a phased-in schedule that delivers efficiencies where the CDOC needs efficiencies first. Securus proposes a preliminary implementation plan that transitions all offender telecommunications services within contractual terms. This includes complete, turn-key

installation of all hardware, software, and configurations for the offender telecommunications system.

The project begins with Securus representatives on-site at a designated CDOC location to kick-off our implementation plan within days of contract execution.

Degree of Involvement from CDOC

Securus makes every effort to limit the administrative burden that can occur during a transition of service providers. We have experience installing our system at more than 2,800 customer locations. This level of experience ensures that we do not waste any of your time.

At the beginning of the project, the Securus Project Team will meet with the CDOC team on site at a CDOC location. These well-organized meetings introduce project team members and review the project plan and timetables with the CDOC team in person to ensure a successful project kick-off.

Our project managers work with the CDOC team to coordinate equipment deliveries and facility access. When Securus technicians arrive on site, they may require escorts to the phone/terminal and equipment locations. The majority of project activity will occur during normal business hours. However, Securus can accommodate late-night/overnight cut-over activities. Some customers choose this method to eliminate service interruptions.

After each facility transitions to our NextGen Secure Communications Platform™ (NextGen SCP™), our project manager and field service technician review our quality checklists with the CDOC team.

The Securus project team hosts weekly stakeholder meetings with participation from the DCOC team.

At the beginning of the implementation project, the Securus project management team will work with the CDOC team to identify key stakeholders and primary points of contact. The team defines roles and responsibilities for the duration of the project.

The Securus project management team will establish regular meeting forums and communication protocols that accommodate the requirements of the CDOC team.

Throughout the project, our project management team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

In addition to the personal communication from our project managers, Securus can set-up automated email notifications for the CDOC team. The automated email

notifications the communication of updates and status changes for major milestones and other tasks.

Implementation Procedures

The project plan consists of:

- Project Initiation Phase
- Project Planning Phase
- Project Execution Phase
- Project Monitoring/Controlling Phase
- Project Closure Phase

Project Initiation Phase

Immediately after contract award, the Securus project management team hosts a meeting with the CDOC team to review project scope, critical success factors, and the implementation timeline. Site survey activities are coordinated to ensure project information matches the latest physical characteristics of each location.

Project Planning Phase

During the Project Planning Phase, the Securus project management team coordinates material and human resources required for the project. This phase includes the coordination of travel, facility access, deliveries, and customer training. Securus works directly with all interstate, intrastate, and local exchange carriers (LECs) to coordinate the installation of network services and equipment required for the project. The Securus project management team coordinates all activities and timelines with the CDOC team.

Project Execution Phase

During the Project Execution Phase, Securus technicians will travel to each location and complete pre-installation activities in preparation for the cut-over. The pre-installation activities include pre-wiring, hardware staging, and telecom test and turn-up activities that can be done in advance to reduce the time and complexity of the actual cut-over.

The Securus project management team coordinates cut-over activities with the CDOC team and the current service provider to ensure a seamless transition of service. The transition of service can be coordinated after hours or during offender lockdown to

limit service interruptions. If a service interruption is required, the activity will be coordinated with the CDOC team at least five business days in advance.

During the cut-over, the Securus team performs a thorough inspection of the installation and resolves any issues before finalizing the implementation. The installation technicians perform a walk-through with the CDOC team to review all installation documentation and checklists. The Securus project management team hosts a customer acceptance review meeting with the CEOC team after finalizing the cut-over at each location.

Onsite training and web-based training activities (if applicable) occur during this phase of the project.

Project Monitoring/Controlling Phase

During the Project Monitoring/Controlling Phase, the Securus project management team focuses on completing any outstanding action items. The Securus installation and site engineering team will conduct daily diagnostic checks and monitoring to ensure the installed equipment works and meets the requirements of CDOC.

The Securus project management team maintains frequent communication with the CDOC team through the resolution of all outstanding action items and final receipt of customer acceptance for the implementation project.

Project Closure Phase

During the Project Closure Phase, the Securus project management team ensures there are no outstanding action items or deliverables. Securus reviews the full implementation project with the CDOC team to obtain final acceptance.

The Securus project management team transitions support responsibilities to the Securus account management team for long-term, ongoing account support. The Securus project management team completes all internal updates and project closure activities.

Project Quality Management Plan

The implementation project plan includes quality control checkpoints at important stages throughout the project. The quality control checkpoints are essential elements of the Securus project that ensure consistent, high-quality implementations. The Securus installation support team uses a Six Sigma quality measurement technique that identifies and removes the causes of errors and minimizes variability in the installation process. Each installation project follows a defined sequence of steps with quantifiable targets. These targets can be financial or any other measure that is important to our

customers. The current process sigma is 4.12 (meaning less than five errors per 1,000 checks), with first-pass quality scores exceeding 90 percent.

Securus truly provides a level of quality assurance unmatched in our industry.

Quality Control Checkpoint 1: Customer Provisioning

Securus installation support technicians provision the system before any onsite installation activity. Provisioning prepares our system to support the CDOC offender calling or video traffic, and ensures the configuration of all necessary applications and calling features. After customer provisioning is complete, the installation technician submits a quality control review form to the engineer, project manager, and account manager for the CDOC project. Each of these Securus associates must review the customer provisioning "pre-cut" record, and provide verification and approval.

Quality Control Checkpoint 2: Customer Pre-Installation

While onsite, the Securus field service technicians will complete a checklist to ensure that the physical installation characteristics meet or exceed Securus' standards. A review of equipment inventory, equipment location, electrical, network, telecommunication, and telephone/terminal installation standards occurs at this checkpoint.

Quality Control Checkpoint 3: Equipment Testing / Functional Validation

At this stage of the project, the system is online, and test calls performed. This quality control checkpoint ensures that all system options are set up to meet the requirements of the CDOC. Technicians test call scenarios and phone labels, call durations, on/off times, administrative terminals, and verify other customer configurations.

Quality Control Checkpoint 4: Customer Acceptance

The final quality control checkpoint involves a review by the CDOC team. During this review, the Securus project management team provides copies of all quality control documents, equipment inventory records, and network diagrams. The Securus project management team hosts a review of these documents with the CDOC team. Resolution of any outstanding deliverables or service issues occurs before completing the Customer Acceptance checkpoint.

a. The Offeror must have adequate financial resources to perform the requirements of this contract or the ability to obtain them. The Offeror must provide a copy of its audited financial statements for the past two (2) years. If an audited financial statement is not available, provide the most recent revised, compiled or internally prepared

financial statement. Offerors that are newly formed entities must submit the financial statements of the "parent" company(ies), (if applicable).

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Two years of audited financial statements are provided and are included as a separate file as instructed in item (d) (iii) below.

b. Provide organizational information including years in business, organizational structure, parent organization and any affiliations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

T-Netix, Inc. began under the name Tele-Matic Corporation, incorporated under the laws of the State of Colorado on February 6, 1987. In 1992, the company acquired eight affiliated companies in the offender phone business as well as the offender phone business assets of two other companies. In 1993, T-Netix met the offender fraud control challenge and was the first company to introduce to the corrections marketplace the capability to detect a three-way call.

From its inception until July 1992, T-Netix was primarily engaged in designing, manufacturing, marketing, and servicing public payphones, including pay telephones for use in correctional facilities. In 1991, the company began to focus on providing specialized telecommunications services for the offender calling market as the result of US Justice Department mandates to prevent offenders from committing massive credit card fraud from prisons.

Securus Technologies, Inc. formerly Evercom Systems, Inc., was incorporated August 22, 1997 in the State of Delaware. Over the next several years after incorporation, the company acquired the assets of several other offender telephone service providers, all of which had been in the offender telephone service business between 5 to 12 years.

In 2004, Securus Technologies, Inc. (now known as Aventiv Technologies, LLC) was created as the parent company of Evercom Systems, Inc. (now known as Securus Technologies, LLC) and T-Netix, Inc. The Securus product line comes from hands-on teaming with correctional facilities. Our product offerings are a direct result of our commitment to technological excellence. The Securus goal of providing outstanding customer service to correctional institutions, offenders and friends and family members of offenders drives our commitment to service.

Today, Securus provides service to more than 3,470 correctional facilities nationwide, including locations operated by city, county, state, and federal authorities, juvenile detention centers, and private facilities.

A detailed organization chart showing ownership and entities is included as **Securus Attachment No. 5, Corporate Org Chart and Entities.**

Securus Technologies, LLC is a Limited Liability Corporation (LLC).

c. Financial statements submitted shall be a separate file to the proposal, and should be labeled as "Financial Documents".

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Two years of Audited Financial Statements are included in the response as instructed here.

d. Such financial documents are provided by Offeror to CDOC at no cost to CDOC

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

iii. Provide an affidavit stating that the proposed key personnel meet the requirements identified in the SOW and have the associated licensing, certification, and any other requirements necessary for the position. Resumes or similar documents are not required.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

All Securus personnel meet the requirements identified in the SOW and have required licensing, certifications, and other requirements for their roles in fulfilling the contract.

Proposed Project Team	
Name	**Qualifications/Responsibility**
Daniel Furrer, **Senior Account Executive**	Daniel has 6 years of communications experience with JPay and Securus. He will work alongside Michele Paige and the rest of the CO DOC Project Team to ensure a hundred percent customer satisfaction during the installation and throughout the duration of the contract. Daniel works with 13 DOCs around the country and brings substantial background into the DOC environment.
Steve Viefhaus, **Vice President, Sales**	Steve has more than 39 years of communications experience with Securus, MCI and Verizon. He will work with the CDOC project team to ensure the project is implemented on time and answer any questions the State may have.
Josh Conklin, **Sales Vice President**	Joshua (Josh) Conklin is Vice President of Sales at Securus Technologies, LLC with more than 13 years of communications experience. Josh will work with Steven and CDOC to ensure that the project is completed on time and

	above expectations, answering any key questions that may come up during installation. Before joining Securus, Mr. Conklin served as Senior Vice President and General Manager of California and Nevada for Integra Telecom, a privately owned, facilities-based, integrated communications carrier and equipment provider headquartered in Portland, Oregon.
Michele Paige, **Senior Account Manager**	Michele is a results-oriented manager with over 25 of experience working in the public and private sectors. Extensive experience in customer service, account management, sales, event planning, team building and public relations. Expert manager of people and resources, easily develop rapport with people of diverse backgrounds and experiences. She has served as account executive for the largest correctional facility accounts with more than 200,000 customers. Michele has effectively developed and implemented innovative tracking and customer satisfaction programs to meet customer's needs.
David Bensmihen, **Sales Engineer**	David has supported offender systems and correctional facility accounts for more than 10+ years. He will provide assistance throughout the installation.
Nestor Nunez, **Sr. Manager, Implementation Project Manager**	Nestor has experience managing multiple projects and delivering results on time and within budget. He will oversee the CDOC installation from initiation to completion and will be the first-line escalation during implementation.
Johnny Hagins, **Director, Operations**	Johnny has more than 23 years of experience in the telecommunications industry. His current management responsibilities include overseeing all managers, field technicians and field site administrators who service and maintain state DOCs, county jails, and other private prisons and jails in the Eastern Region of the United States.
Jonathan Jones **Regional Manager, Field Services**	Jonathan brings more than 20 years of progressive experience and accomplishments in technical and service delivery environments requiring strong leadership, IT/telecommunications, communication, and customer support skills. He is a strategic and proactive leader with a proven track record of managing people, resources, processes, and technologies to meet business objectives, customer goals, and revenue and profit goals

Bobby Folsom **Technical Support Manager**	Bobby has more than 19 years of experience within the Technical Support Department for Securus Technologies. He has held all the technical positions within the department and his current management responsibilities include overseeing technical support supervisors, technical support technicians and the top tier tech 3 escalation team who all work to service and maintain both state DOCs, county jails, and other law enforcement facilities across the United States.
Jerimy Thompson **Regional Manager, Field Services**	Jerimy has direct Supervision of Installs encompassing 17 States to include DOC Facilities and County Jails. He managers Day to Day functions and scheduling of all major installs in the Western Region. Jerimy works hand and hand with facilities to meet timeframes and schedules that fully benefit the customer.
David Brannan, **Manager, Field Services**	David has 16 years of experience in the Telecom Industry, including 10 years of this experience as a Field Operations Senior Manager. He is experienced in managing time-critical projects, delivery of our services across cross functional teams, and experience in managing high profile and large-scale deployments across the continental United States, Canada, Mexico and the U.S. Virgin Islands. David is proficient in Microsoft Word, Excel, Visio, and Wrike. I am also skilled in Project Management, RF Network Design, Structured Cabling design, Planning and deployment, as well as RF Network Deployment and Testing.
Tony Westbrook, **Field Service Technician**	Tony will serve as the lead technician for the planned installation at CDOC.
Chris Pair, **Field Service Technician**	Chris will serve as back up to the assigned onsite technician and provide additional support during implementation as needed.
Trevor Lipscomb, **Field Service Technician**	Trevor will serve as back up to the assigned onsite technician and provide additional support during implementation as needed
David McTee, **Instructor, Customer Training & Product Adoption**	David brings more than 35 years of professional training experience. He will provide CDOC staff with the knowledge and skills needed to efficiently administer the system.

STATE OF: Texas

COUNTY OF: Denton County

AFFIDAVIT

I, Russell Roberts, the Chief Growth Officer of Securus Technologies, LLC, fully authorized to contractually obligate Securus Technologies, and being duly sworn, affirm the following statement:

> The proposed key personnel meet the requirements identified in the SOW and have the associated licensing, certification, and any other requirements necessary for the positions for which they will service in fulfillment of the contract resulting from the Colorado Department of Corrections (CDOC) ITN CFNA #2022000005.

RR

Signature

April 7, 2022
Date

Russell Roberts
Printed Name

Chief Growth Officer
Title

Sworn to me this day of 7th, day of April 2022.

NOTARY PUBLIC Misty D Madore

Misty Dawn Madore
My Commission Expires
03/31/2024
ID No 132421299

iv. Provide examples of how the Offeror has applied new technology towards improvements and the outcome achieved. In addition, provide the Offeror's expectation for future improvements to improve efficiency.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is continually developing new applications and encourages employees to submit patent applications when development warrants it. We are proving a summary of how we have used technology to improve product, services, and efficiencies to improve the environment within the corrections community and to encourage offender relationships with family and friends to develop to improve their return to society.

INNOVATION/ONGOING IMPROVEMENT

At its core, Securus is a team of technology experts who are driven and inspired by innovative products and solutions. We're always at the forefront of corrections technology and are continuously looking for ways to leverage modernization to improve our offerings.

With a focus on delivering corrections technology solutions that fit the needs of our consumers, we're always integrating feedback from our clients. Our products undergo continuous improvements throughout the year. In fact, many of our products receive feature updates to improve performance and efficiency each month.

Beyond ongoing improvements, we focus on delivering solutions that solve the evolving business-critical needs of our clients and platform users. Here's a look at a few of our latest innovative products and services launched in 2022:

- **Securus Text Connect** –a new texting product that allows family and friends to initiate an SMS text conversation with their incarcerated loved one **–** Launched in Q1!
- **Media Subscriptions** – monthly game, music, and movie subscription services that provide incarcerated individuals with access to fresh, premium media content. Game subscription services are available now with music subscriptions slated for Q2 and movie subscriptions for Q3, 2022.

By leveraging our diverse catalog of correction-focused technology tools, we continue to support our mission: to provide top-quality solutions that help our facilities enforce policy, manage procedures, and ensure safety.

2022 ROADMAP

We're re-thinking corrections technology. And our approach to doing things differently isn't just shaped by the insights we get from our clients, but also by the evolution and advancements of the industry. Take a look at a few of the major technology enhancements we have planned for our products in 2022:

1st half, 2022

- **Securus Video Connect enhancements** – update the user experience, privacy and security settings.
- **Securus Text Connect** –a new texting product that allows family and friends to initiate an SMS text conversation with their incarcerated loved one.
- **Game subscriptions** – a monthly subscription that gives incarcerated gamers access to a catalog of new releases and classic game titles.
- **Music subscriptions** – a monthly subscription that gives incarcerated listeners access to millions of tracks with new music added daily.

2nd half, 2022

- **Variable-length subscriptions** –bundles that allow incarcerated individuals to purchase a pre-determined number of subscription months for one low cost – i.e: a 3-month bundle, a 6-month bundle, etc.
- **Movie subscriptions** – a monthly subscription that gives incarcerated individuals access to hundreds of movie titles including movies from all genres like action, comedy, animation, and more.
- **Premium eBooks** – a service that will expand the available catalog of eBooks and allow incarcerated readers to purchase their favorite titles.
- **Consolidating the Admin portal –** a streamlined, single sign-on for our clients
- **Word Alert 2.0** – a fully integrated and enhanced Word Alert product with improved features and functionalities
- **Betterment application** – a new application filled with content focused on education, self-improvement, re-entry success, and more.
- **Streaming radio** – offenders can stream their favorite local or national radio stations.
- **Unity Terminal SE** – a new terminal built to support all current and future Unity tablet features and applications.

v. Provide examples of success on projects of similar in size and scope within the last 5 years.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Texas Department of Criminal Justice
Name: Lynda Cobler
Title: Assistant Director, Customer Support Services
Telephone #: 936-437-1437
E-Mail Address: lynda.cobler@tdcj.texas.gov

Oklahoma Department of Corrections:
Name: Matthew Craig
Title: Administrator of Technology and Logistics Operations
Telephone #: 405-425-7166
E-Mail Address: Matthew.Craig@doc.ok.gov

Arkansas Department of Corrections:
Name: Rhonda Patterson
Title: CTO, DOC Shared Services
Telephone #: 870-850-8521
E-Mail Address: Rhonda.Patterson@Arkansas.gov

North Dakota Department of Corrections:
Name: Shaun Fode
Title: Director of Facility Operations
Telephone #: 701.328.6112
E-Mail Address: cobraun@nd.gov

vi. A description of how the Offeror's infrastructure, internal controls, and management strategies will ensure quality and continuity of operations in fulfilling the requirements of the contract.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus continually enhances quality to maximize customer satisfaction. We do this through a comprehensive approach that includes our culture, our employee selection process, measurements and feedback, system and process design, and internal controls.

Our Culture

At Securus, we believe a commitment to quality starts with culture. Securus has developed a culture of measurement and continuous improvement. Each Securus department measures and reports customer satisfaction and performance toward quality objectives. Internal teams review and analyze the results, and action items and initiatives are created to improve. Each quarter the company recognizes employees and work teams that have achieved outstanding results in the areas of teamwork, quality, innovation, and customer satisfaction.

Employee Selection

Having a quality-oriented culture is vital, but employees committed to our values and performing at the highest level is what sets us apart. Securus uses a formal process for employee selection that involves multiple departments and management levels. An in-house recruiter seeks out top candidates for open positions. Screenings ensure candidates match the requirements for positions and background checks ensure we only hire candidates with the highest integrity standards. Our formal processes ensure only the top candidates are selected.

Measurement and Feedback Systems

An important foundation of our quality focus is our measurement system. Securus uses a variety of quantitative and qualitative information gathering tools to solicit feedback from customers in our quality improvement process. These tools include:

- **Transactional Surveys** – We survey customers after key events (e.g. installations, adds, moves, changes, repairs) to gather information on performance. Respondents rate their experience through 21 questions. A low rating (a 1 or 2 on a 5 point scale) on any single question requires a management review, immediate contact with the customer, and an action plan for improvement.
- **Relationship Survey** – We survey our customers periodically to understand if we are meeting their expectations. This survey specifically evaluates the performance of our customer operations and account management teams. Again, we ask 21 questions, and a low rating requires a management review, immediate contact with the customer, and an action plan for improvement.
- **User Groups** – Securus periodically sponsors user groups inviting customers to discuss their ideas and future development of our products and platforms. Operational and security challenges customers brought to Securus are at the heart of many of our patented innovations.

These feedback mechanisms provide invaluable information and help Securus meet our customers' expectations.

System and Platform Design

We use a professional and formal approach to platform and process design that ensures quality software and functionality releases. Before release, all modifications to the platform undergo rigorous testing in a test environment.

Software Development

The Securus use of information technology (IT) best practices, industry standard quality measurement tools, and strict environmental controls ensure the highest system functionality and availability. The Securus development team uses the Waterfall Software Development Lifecycle (SDLC) to ensure high-quality deliverables. The feature/functionality enhancements process stages are:

- Analysis
- Design
- Development
- Quality Assurance
- Implementation
- Post Implementation Support

Each phase has specific deliverables and gates (controls) to ensure high quality and to minimize rework. Securus uses the following distinct system environments in conjunction with our SDLC:

- Development – Used by IT Development to create and unit test new enhancements
- Quality Assurance – Used by Quality Assurance Analysts to test and certify new enhancements and bug fixes
- Pre-Production – Used by Production Support to validate hot fixes for production, and for final validation and mock deployment of major functionality releases
- Production – Used by all Securus customers and accessible by only Securus Production Support and Tech Support

Each environment has access controls, and we use source code control systems to ensure the proper promotion of code and as a document repository.

Securus uses industry-standard HP Quality Center for defect tracking and follows a rigorous test cycle including:

- Verification of New Functionality – Ensures a feature is working as designed
- Load Testing – Determines the upper threshold or breaking point of the component or feature
- Performance Testing – Determines the expected user experience
- Regression Testing – Ensure all existing functionality still works as designed
- Exception Testing – Tests boundary conditions and unexpected usage scenarios

New releases typically create new functionality. Upon completion of the Quality Assurance stage, the code changes are packaged and deployed into our pre-production environment for the final end-to-end quality check, and to optimize the implementation. This effort enables Securus to minimize the maintenance window related to system changes.

Both IT and business stakeholders review and must approve all scheduled changes to production in two change control meetings to safeguard the stability of the production environment.

Upon implementation of new code into production, Securus Production Support and IT Development monitor changes closely to minimize the impact of any adverse or unexpected system behavior.

This attention to detail allows Securus to build feature functionality that leads the industry in quality and performance. For example, the Securus three-way call detection feature has been proven to be more accurate than the same feature offered by competitors. Independent testing by an outside research and testing company proves it. Similarly, our voice biometric feature leads the industry in accuracy.

The voice quality available on our call platform provides near perfect fidelity. Customers have used information heard through background conversations to prevent and solve crimes.

Our quality control does not end with our system design but continues all the way through site installation. Securus and each customer develop a defined quality checklist to install the system in a manner that meets their unique operating requirements. As described and included with our installation plan, Securus uses quality control checkpoints for each phase of an installation:

- Quality Control Checkpoint 1 – Provisioning: After customer provisioning is complete, Securus technicians submit a quality control review to the Engineer, Project Manager, and Account Manager for the project.

- Quality Control Checkpoint 2 – Pre-Installation: While on-site, Securus Field Service Technicians complete a checklist to ensure that the physical installation characteristics meet or exceed Securus standards.
- Quality Control Checkpoint 3 – Equipment Testing/Functional Validation: Technicians complete test call scenarios and phone labels, call durations, on/off times, administrative terminals, and verify other customer configurations.
- Quality Control Checkpoint 4 – Acceptance: The Securus Project Team provides copies of all quality control documents, equipment inventory records, and network diagrams. The Securus Project Team will host a review of these documents with CDOC.

These tools are used to verify that work is completed properly before moving to the next step in a process. Customers must indicate their satisfaction with a sign off moving to the next step in a process.

Internal Controls

Finally, Securus has developed the best internal controls in the industry to make sure we follow our processes and that our information is accurate and ensure its security. Securus access controls for all systems are internally audited for compliance with The Sarbanes–Oxley Act of 2002 (SOX), which set new or enhanced standards for all U.S. public company boards, management and public accounting firms. This internal audit ensures CDOC will get accurate and timely reporting and payments from Securus.

Securus also employs an internal audit team that constantly reviews and audits our systems and security procedures and verifies our performance compared to our standards.

vii. Offerors may submit a proposal for any service category section identified in the SOW, but must respond to each section in its entirety. Offeror's response must include the corresponding service category section number, item number, etc. (ie.13., Kiosks, A., Kiosk Types, i. Turnkey ii. Hardware Only Kiosk, etc.) inserting one blank page between each service category in their proposal. Offerors must acknowledge, respond or indicate no response on Sections 3 through 34 in a sequential order and in its entirety.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

viii. The following must be completed in its entirety and returned with Offeror's bid response.
a. Vendor Response Signature Page of ITN located on page 20.
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

I. VENDOR RESPONSE SIGNATURE PAGE
INVITATION TO NEGOTIATE
ITN #2022000005, "OffenderCommunication"

VENDORS: See the ITN "ADMINISTRATIVE INFORMATION" section for the ITN response deadline and other response submission information and requirements.

Vendors responding to this ITN must fill out this page in its entirety, sign and return with Vendor's response. This page must bear a physical or electronic signature, as electronic signature is defined in the "Uniform Electronic Transactions Act", section 24-71.3-102 (8), evincing an intent by the Vendor to be bound by its response. Failure to do so may disqualify the Vendor response.

The undersigned understands and agrees that misrepresentation made in this response and/or subsequent discussions or information presented to the State may be deemed sufficient cause for the refusal by the State to execute a contract as a result, and that that later discovery of any omission or misrepresentation made in the ITN response and/or subsequent discussions or information presented to the State may be grounds for the cancellation of an existing contract.

YES	NO	*Indicate if your company is SDVOSB or Resident Bidder below. Include supporting documentation with your response.*
	XX	Company is a Service-Disabled Veteran-Owned Small Business. Reference §24-103-905, CRS
	XX	Company is a Colorado resident Vendor. Reference §24-103-906, CRS

Legal Company Name	Securus Technologies, LLC
Doing Business As	Securus Technologies, LLC
FEIN	82-391792
Authorized Signature	RR
Printed Name	Russell Roberts
Title	Chief Growth Officer
Company Address	4000 International Parkway, Carrollton, TX 75007
City:	State: Zip:
Phone Number:	972-277-0300
Email address	Daniel.Furrer@securustechnologies.com
Contact for Clarifications:	Daniel Furrer
Title	Senior Account Executive

Phone	954-862-6900, x3009
Email Address	Daniel.Furrer@securustechnologies.com

b. OCS SOW Equipment/Software/Inventory & Rate Proposals - Offeror proposal must include the description of the market resources, methodology, and technology used to determine the proposed rates for the contract base period.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Attachment 3 – OCS SOW Equipment_Software_Inventory & Rate Proposal are completed and will be included in the zipped file with the complete submission.

c. Vendor Disclosure Statement

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

COLORADO
Department of Corrections

DIVISION OF CANTEEN SERVICES

TITLE: Offender Communication

Invitation to Negotiate (ITN)

ITN CFCA # 2022000005

ATTACHMENT 4

Vendor Disclosure Statement

Attachment 4
State of Colorado – Contract Management Information
Vendor Disclosure Statement
Colorado Revised Statues §24-102-206

Contract Performance Outside of the United States or Colorado

---

Prior to contracting, or as a requirement for the solicitation of any contract for services from the State of Colorado, a prospective vendor is required to disclose the following information in a statement of work.

Completing this Form

- To the extent the following information has **not previously been disclosed** in a statement of work, a prospective vendor shall complete this Vendor Disclosure Statement and return it to the contracting state agency or institution of higher education (IHE).
- This Disclosure Statement is not required for contracts under Medicare, the "Colorado Medical Assistance Act", Articles 4 to 6 of Title 25.5 C.R.S., the "Children Basic Health Plant Act", Article 8 of Title 25.5, C.R.S, or the "Colorado Indigent Care Program", Part I of Article 3 of Title 25.5 C.R.S.
- This Disclosure Statement is not required for Construction contract.

---

1. Solicitation Number: ITN #2022000_____
   State Agency Name: Colorado Department of Corrections

   Vendor Name: _____Securus Technologies, LLC_____

2. Where will the services under the contract, including any subcontracts, be performed? List all county(ies) and state(s).
   _Fremont County, CO; Crowley County, CO; Chaffee County, CO; Jefferson County, CO; Delta County, CO; Denver County, CO; Pueblo County, CO; Lincoln County, CO; Garfield County, CO; Logan County, CO; Las Animas County, CO; Bent County, CO; Denton County, TX._____

3. If it is anticipated that services under the contract or any subcontracts will be performed outside of the United States or the State of Colorado, explain why it is necessary or advantageous to go outside the Untied Stated or the State of Colorado to perform the contract or any subcontracts.
   __All services under the contract will be performed within the United States._____

Signature	April 7, 2022 *Date*
Russell Roberts *Printed Name*	Chief Growth Officer *Title*

d. W-9

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

A copy of Securus' W-9 Form is included in **Securus Attachment No. 9, W-9 Form**.

e. Colorado Secretary of State's Certificate of Good Standing

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus Technologies, LLC is registered to do business in the state of Colorado by the Secretary of State and a copy of the "Certificate of Fact of Good Standing" is provided in **Securus Attachment No. 3, CO SOS Certificate of Fact of Good Standing, and FCC Registration Form**.

f. Contract Performance Outside the United States or Colorado - Vendor Disclosure & Notification - Non-Construction

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Please refer to the **Vendor Disclosure Statement**, requirement number c, above.

ix. Accessibility

Provide a statement confirming the Offeror's intent and capability to comply with accessibility requirements in accordance with Section 508 of the U.S. Rehabilitation Act of 1973, as amended, and with the most current version of the Web Content Accessibility Guidelines (WCAG) available at https://www.w3.org/TR/WCAG21/.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus equipment will meet with all accessibility requirements in accordance with Section 508 of the U.S. Rehabilitation Act of 1973, as amended, and with the most current version of the Web Content Accessibility Guidelines (WCAG) available at https://www.w3.org/TR/WCAG21/.

x. Rate Adjustments

One (1) rate adjustment request must be made in writing no later than 60 days prior to the annual renewal date, and is subject to negotiation. The annual price adjustment request shall not exceed the amount specified in the U.S. Bureau of Labor Statistics Consumer Price Index (CPI-U) under the appropriate category and services, and in accordance with FCC Regulations.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus understands that rate adjustment requests must be made in writing no later than 60 days prior to the annual renewal date, and is subject to negotiation. Securus also understands that the annual price adjustment request shall not exceed the amount specified in the U.S. Bureau of Labor Statistics Consumer Price Index (CPI-U) under the appropriate category and services, and in accordance with FCC Regulations.

xi. Debarment and Suspension

Identify any required disclosures under paragraph IV.N of this ITN.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is not debarred or suspended for any purpose.

In Securus Attachment No. 2, we have provided a litigation and administrative action history as requested. Under a separate confidential file, included with the response, Securus has provided further relevant information.

xii. Conflicts of Interest/Ethics

Identify any potential or actual conflict of interest in accordance with paragraph IV.O of this ITN.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has no conflicts of interest or apparent conflicts of interest as defined in Section "P" of the ITN.

xiii. Offeror Proposal Assumptions

a. Offerors are expected to provide all proposal assumptions used in preparing their responses. Assumptions should include rational for all cost elements.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

b. It is imperative that Offerors submit supporting rational to explain the basis of their cost estimates. Provide assumptions used to establish proposed costs, including any escalation rates used (i.e. historical data, technical experience, market research, etc.) Offerors must also ensure that their subcontractors' costs are also adequately supported.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is the largest provider of offender communication services in the country. We are touching over half of the incarcerated population in the US every day which has provided us significant experience with pricing and cost for deploying the services contemplated in this RFP. In terms of cost to the DOC, this will be a zero cost contract to the State. Securus will be responsible for all of the infrastructure necessary to deploy the services outlined in this procurement, using available wiring infrastructure from previous service deployments. We will provide all phones, tablets, connectivity, security, and server infrastructure for all elements of this agreement at no cost to the State. The prices charged to the end user for services are at or below market rates for all services. Telecommunications services prices have been extensively reviewed by Federal and State regulatory agencies, and caps have been established for those services that are cost based. The rates proposed in this RFP are at or below the established caps established by those agencies. Non-Regulated services contemplated by this RFP are set at or below the average service prices for the other agencies we serve, and are at or below the average consumer prices for media services available in the commercial marketplace. These service prices are tested to be fair and competitive in the commercial marketplace for movies, music, books, and games through large service providers like Netflix, Spotify, and Apple. It is our goal to provide similar prices for these services for those who wish to subscribe to those they would see outside facility walls. It is our goal that no price point charged under this contract would every fail to stand up to the scrutiny of the public, and the best way to do that is to ensure that the products are as similar as possible in purchase model and price to the way we consume these services in the general public. We are offering all-in subscriptions AND individual purchase options, so every family member and offender can procure services the way THEY choose, to provide budget predictability. It is exactly this reasoning that has led us NOT to offer to sell our services on a per minute rate. Our goal is for the population to use these tablets as much as possible. We never want you to be embarrassed publicly by any single purchase of any service, and charging per minute can create unwanted outcomes. For example, charging per minute for premium books can be very expensive. A 500 page book can take 20+ hours to read, which totals $60 at $.05/min. That same book could be owned for $4.99. An easy way to explain this is to simply go to the screen time reports on one's phone. At two hours per day, which most of us struggle to stay below, that's 3,270 minutes per month or $186 dollars. Though those numbers may not represent the norm, it can absolutely happen and we never want you, or us, to be in a situation where we've taken advantage of someone due to the fact that we are their only option. We are always committed to lower prices. We offer free communication options. We will provide every offender access to a plethora of free content and will never require them to purchase anything to have that access. We are assuming responsibility to provide everything included in this offer

at our sole expense, and that prices to the end users will be at or below the prices contained herein, for the life of this contract.

c. A basis of estimate (BOE) is an organized set of data and narrative information that explains the logic, methodology, calculations, and assumptions the Offeror uses to define the tasks and determine the resources needed to accomplish the SOW.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has the services contemplated in this RFP installed today in thousands of correctional facilities across the US. As each installation is completed we update what we call the "Playbook", which is the standard that we use to establish our BOE. The "Playbook" is an internal document that contains the Project Management processes and procedures we use to ensure a smooth installation including but not limited to site survey process, BOM development, risk mitigation procedures, supply chain management, human capital assignment, testing and deployment, agency and offender training, ticket analysis and follow-up, and account management handoff. From the first kickoff meeting it is our intention to partner with the agency to deploy our "playbook" within the parameters outlined by CDOC process and procedure. The State of Colorado can be assured that the installation and deployment by Securus has been pressure tested at the largest DOCs' in the country, and that all lessons learned from these installations, and most importantly the talented associates who completed these installations, will be brought to bear to complete this project to the only standard that matters to us-complete and total satisfaction of the Colorado Department of Corrections. It is our sincere hope that the State will inquire to our most recent installations of these services and ask these questions not just of us, but of the clients who have recent experience with the outcomes generated by the use of this "playbook". We believe you'll find from those conversations extremely satisfied customers who are satisfied beyond their expectations or the requirements of their contract and RFP.

xiv. Modifications to State Contract

a. Confirm the Offerors agreement with the draft contract in Attachment 6.

b. If the Offeror would like to suggest modifications or add additional terms and conditions, identify those in this section of the response. However, the conditions of paragraph, section IV.J of this ITN will apply.

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus agrees with the draft contract included in the ITN package, labeled as Attachment 6.

CLOSING

Company Summary

Securus Serves	City, County, State and Federal Governmental Agencies
Providing	Civil and Criminal Justice Technology Solutions
For	Public Safety, Investigation, Corrections and Monitoring Professionals
With Products And Services That Provide	Emergency Response Incident Management Public Information Investigation Verification Trust Funding and more... Communication Information Management Offender Self-Service Monitoring Offender Entertainment
Name and Address	Securus Technologies 4000 International Parkway Carrollton, TX 75007
Family and Friends Website:	www.securustech.net
Agency Website:	www.securustechnologies.com
Management:	David Abel, President & CEO Geoff Boyd, CFO Josh Conklin, Sales Vice President Russell Roberts, Chief Growth Officer
Corporate Office Locations	Carrollton, TX; Southborough, MA; Miami, FL; Atlanta, GA
Other Brands Owned	JLG Technologies Satellite Tracking of People (STOP) JPay, LLC Guarded Exchange, Inc. AllPaid, Inc.

Headquartered in Carrollton, Texas, and serving over 3,400 law enforcement and corrections agencies and 1,200,000 offenders across North America, Securus Technologies is committed to serve and connect by providing emergency response, incident management, public information, investigation, verification, communication, information management, offender self-service, and monitoring products and services in order to make our world a safer place to live. Securus Technologies focuses on “Connecting what matters”. To learn more about our full suite of civil and criminal justice technology solutions, please visit www.securustechnologies.com.

SECURUS ATTACHMENTS

List of Securus Attachments

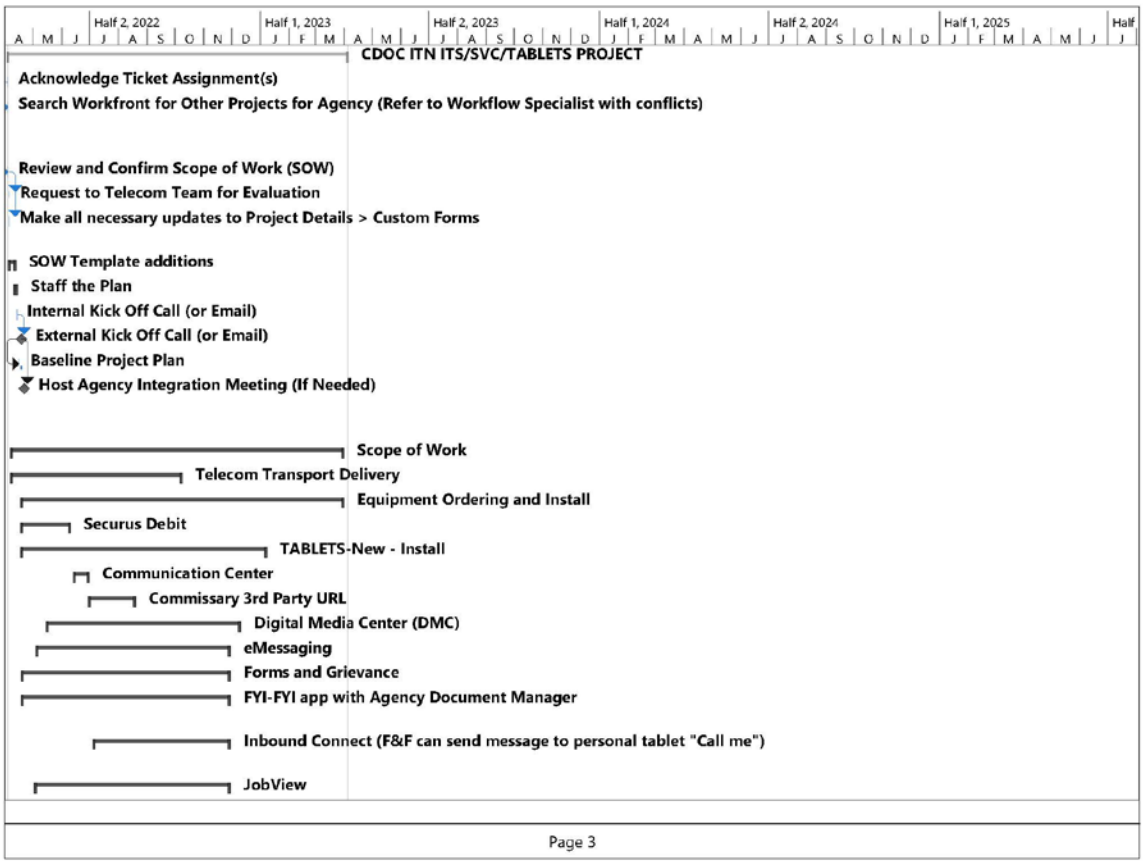
Securus Attachment No. 1	**Preliminary Project Plan**
Securus Attachment No. 2	**CO DOC Litigation History and Other Legal Proceedings**
Securus Attachment No. 3	**CO SOS Certificate of Fact of Good Standing, and FCC Registration Form**
Securus Attachment No. 4	**God Behind Bars Pando App**
Securus Attachment No. 5	**Corporate Org Chart and Entities**
Securus Attachment No. 6	**Sample Training Documents**
Securus Attachment No. 7	**Sample Quarterly Performance Report**
Securus Attachment No. 8	**XL Terminal Technical Specifications**
Securus Attachment No. 9	**W-9 Form**

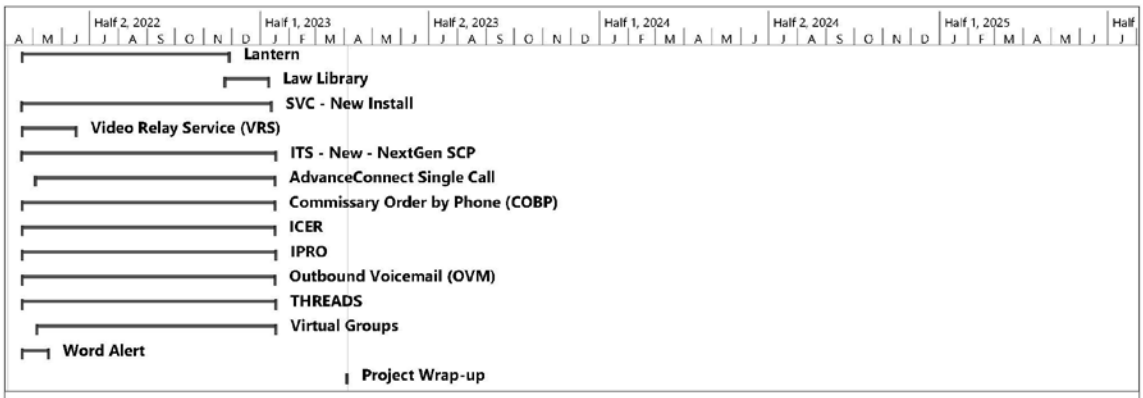
Securus Attachment No. 1:
Preliminary Project Plan

ID	Task Name	Duration	Start	Finish	Resource Names	Predecessors
0	**CDOC ITN ITS/SVC/TABLETS PROJECT**	**253 days**	**4/4/2022**	**4/4/2023**		
1	Acknowledge Ticket Assignment(s)	2 days	4/4/2022	4/5/2022	Project Manager (PM)[0%]	
2	Search Workfront for Other Projects for Agency (Refer to Workflow Specialist with conflicts)	2 days	4/4/2022	4/5/2022	Project Manager (PM)[0%]	1SS
3	Review and Confirm Scope of Work (SOW)	2 days	4/4/2022	4/5/2022	Project Manager (PM)[0%]	1SS
4	Request to Telecom Team for Evaluation	2 days	4/5/2022	4/7/2022	Project Manager (PM)[0%]	3
5	Make all necessary updates to Project Details > Custom Forms	1 day	4/5/2022	4/6/2022	Project Manager (PM)[0%]	3
6	**SOW Template additions**	**4 days**	**4/5/2022**	**4/11/2022**		
13	**Staff the Plan**	**2 days**	**4/11/2022**	**4/13/2022**		
18	Internal Kick Off Call (or Email)	1 day	4/13/2022	4/14/2022	Project Manager (PM)[0%]	12FS+3 days
19	External Kick Off Call (or Email)	1 day	4/15/2022	4/18/2022	Project Manager (PM)[0%]	18FS+1 day
20	Baseline Project Plan	1 day	4/15/2022	4/18/2022	Project Manager (PM)[0%]	19SS
21	Host Agency Integration Meeting (If Needed)	1 day	4/20/2022	4/21/2022	Project Manager (PM)[0%],Integration Coordinator (IC)[0%]	19FS+2 days
22	**Scope of Work**	**246 days**	**4/7/2022**	**3/30/2023**		
23	**Telecom Transport Delivery**	**128 days**	**4/7/2022**	**10/7/2022**		
75	**Equipment Ordering and Install**	**239 days**	**4/18/2022**	**3/30/2023**		
365	**Securus Debit**	**37 days**	**4/18/2022**	**6/9/2022**		
404	**TABLETS-New - Install**	**180 days**	**4/18/2022**	**1/6/2023**		
470	**Communication Center**	**11 days**	**6/14/2022**	**6/29/2022**		
474	**Commissary 3rd Party URL**	**34 days**	**6/30/2022**	**8/18/2022**		
504	**Digital Media Center (DMC)**	**144 days**	**5/16/2022**	**12/9/2022**		
537	**eMessaging**	**142 days**	**5/5/2022**	**11/28/2022**		
574	**Forms and Grievance**	**154 days**	**4/19/2022**	**11/28/2022**		
605	**FYI-FYI app with Agency Document Manager**	**154 days**	**4/19/2022**	**11/28/2022**		
636	**Inbound Connect (F&F can send message to personal tablet "Call me")**	**101 days**	**7/5/2022**	**11/28/2022**		**611FS+1 day**
664	**JobView**	**144 days**	**5/3/2022**	**11/28/2022**		

Page 1

ID	Task Name	Duration	Start	Finish	Resource Names	Predecessors
694	Lantern	154 days	4/19/2022	11/28/2022		
727	Law Library	27 days	11/23/2022	1/9/2023		446
757	SVC - New Install	184 days	4/18/2022	1/12/2023		
807	Video Relay Service (VRS)	41 days	4/19/2022	6/16/2022		
839	ITS - New - NextGen SCP	187 days	4/18/2022	1/17/2023		
893	AdvanceConnect Single Call	175 days	5/3/2022	1/16/2023		
919	Commissary Order by Phone (COBP)	185 days	4/19/2022	1/16/2023		
949	ICER	185 days	4/19/2022	1/16/2023		
978	IPRO	186 days	4/19/2022	1/17/2023		
1022	Outbound Voicemail (OVM)	185 days	4/19/2022	1/16/2023		
1049	THREADS	186 days	4/19/2022	1/17/2023		
1078	Virtual Groups	174 days	5/5/2022	1/17/2023		
1111	Word Alert	20 days	4/19/2022	5/17/2022		
1141	Project Wrap-up	1 day	4/3/2023	4/4/2023		


Half 2, 2022
Half 1, 2023
Half 2, 2023
Half 1, 2024
Half 2, 2024
Half 1, 2025
CDOC ITN ITS/SVC/TABLETS PROJECT
Acknowledge Ticket Assignment(s)
Search Workfront for Other Projects for Agency (Refer to Workflow Specialist with conflicts)
Review and Confirm Scope of Work (SOW)
Request to Telecom Team for Evaluation
Make all necessary updates to Project Details > Custom Forms
SOW Template additions
Staff the Plan
Internal Kick Off Call (or Email)
External Kick Off Call (or Email)
Baseline Project Plan
Host Agency Integration Meeting (If Needed)
Scope of Work
Telecom Transport Delivery
Equipment Ordering and Install
Securus Debit
TABLETS-New - Install
Communication Center
Commissary 3rd Party URL
Digital Media Center (DMC)
eMessaging
Forms and Grievance
FYI-FYI app with Agency Document Manager
Inbound Connect (F&F can send message to personal tablet "Call me")
JobView
Page 3


Half 2, 2022
Half 1, 2023
Half 2, 2023
Half 1, 2024
Half 2, 2024
Half 1, 2025
Half
A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O N D J F M A M J J
Lantern
Law Library
SVC - New Install
Video Relay Service (VRS)
ITS - New - NextGen SCP
AdvanceConnect Single Call
Commissary Order by Phone (COBP)
ICER
IPRO
Outbound Voicemail (OVM)
THREADS
Virtual Groups
Word Alert
Project Wrap-up

Page 4

Securus Attachment No. 2:

Litigation History and Other Legal Proceedings

7-YEAR HISTORY FOR LITIGATION, ADMINISTRATIVE, AND OTHER LEGAL MATTERS

LITIGATION MATTERS

Below please find the seven-year litigation history for Securus and its affiliates. We do not believe the outcome of any pending litigation will have a material impact on our financial condition or ability to perform under the proposed contract.

Open Matters - Securus

Case No. 1:00-cv-00293 (GK), In the United States District Court for the District of Columbia
Wright, et al. v. Corrections Corporation of America, et al.
Description: Putative class challenges constitutionality of exclusive contracts for phone service.
Status: Stayed

Case No. D101cv2016-02529, State of New Mexico, County of Santa Fe, First Judicial District Court
Juarez, et al. v. Securus Technologies, Inc., et al.
Description: Incarcerated individuals challenge call rates.
Status: Pending

Case No. 1884CV01360, Commonwealth of Massachusetts, Suffolk Superior Court, Trial Court Department
Pearson et al. v. Thomas M. Hodgson et al.
Description: Putative class alleges that commission payments violated Massachusetts law.
Status: Pending

Case No. 8:20-CV-1936, United States District Court for the District of Maryland
*Albert et al. v. Global Tel*Link Corp., et al.*
Description: Putative class alleges price-fixing among co-defendants and misrepresentation of costs..
Status: Pending

Case No. 429-2020-CV-00180, In the 6th Judicial Circuit Court of New Hampshire-District Division-Concord
Grant v. Securus Technologies et al.
Description: Incarcerated individual challenges call rates.
Status: Pending

Case No. 4:20-CV-00801-RK, United States District Court, Western District of Missouri, Western Division
Farmer v. Kansas City, Missouri, Board of Police Commissioners et al.
Description: Lawsuit filed by estate of person who committed suicide using phone cord.
Status: Pending

Case No. 21-1006, USDC, District of South Dakota, Northern Division
Kurtenbach v. Securus Technologies
Description: Incarcerated individual alleges unlawful call recording.
Status: Pending

Case No. 1:20-cv-09243-KPF, United States District Court, Southern District of New York

Reid v. The City of New York, et al.
Description: Incarcerated individual alleges unlawful call recording.
Status: Pending

Case No. 20CV368522, Superior Court of California, County of Santa Clara County
Mizerak v. State of California Department of Corrections and Rehabilitation, et al.
Description: Lawsuit alleging injuries sustained while wearing ankle monitor.
Status: Pending
Case No.: GS21cv6860, Montgomery County General Session Court, Tennessee

Houbbadi v. Securus Technologies Inc.
Description: Incarcerated individual alleges issues with his phone account.
Status: Pending

Case No. 3:22-cv-00101, United States District Court, Northern District of Ohio, Western Division
Andrews v. Securus Technologies, LLC, et al.
Description: Formerly incarcerated individual alleges disclosure of recorded calls.
Status: Pending

Closed Matters – Securus

Case No. 3:05-CV-0654-D, In the United States District Court for the Northern District of Texas
T-Netix, Inc. v. Value-Added Communications, Inc. v. Securus Technologies, Inc.
Description: Value-Added Communications, Inc. filed a Motion to Reopen Case to Present Application for Order to Show Cause regarding alleged violation of a Protective Order.
Status: Closed

Cause No. 25756, In the 12th Judicial District Court of Walker County, Texas
Lane, et al. v. State of Texas – Department of Criminal Justice, et al.
Description: Complaint regarding an alleged electrocution by an incarcerated individual.
Status: Settled

Case No. 4:13-cv-562, United States District Court, Eastern District of Texas, Sherman Division
Howlink Global LLC v. Securus Technologies, Inc.
Description: Complaint regarding an alleged patent violation.
Status: Dismissed

Case No. 1:14-CV-366-LY, In the United States District Court, Western District of Texas, Austin Division
Austin Lawyers Guild et al. v. Securus Technologies, Inc., et al.
Description: Class action lawsuit alleging Defendants recorded privileged communications.
Status: Settled

Case No. 3:14-cv-01656-L, In the United States District Court, Northern District of Texas
*Securus Technologies Inc. v Global Tel*Link Corporation et al.*
Description: Securus filed suit alleging that defendants published numerous false statements about Securus.
Status: Settled

Case No. 14CH6346, In the Chancery Court for Anderson County, Tennessee
Frank, v. Blossman Gas, Inc., et al.

Description: Declaratory judgment action seeking an opinion as to the enforceability of Securus contract.
Status: Dismissed

Case No. 3:14-cv-02681-K-BK, In the United States District Court for the Northern District of Texas
*Global Tel*Link Corporation, Inc. v Securus Technologies, Inc., et al.*
Description: Complaint alleging false advertising under the Lanham Act and common law defamation.
Status: Settled

Case No. SCC 554635, Connecticut Superior Court, Small Claims Session
Chicano v Securus Technologies, Inc.
Description: Small claims complaint alleging Defendant owed Plaintiff funds related to a prepaid account.
Status: Dismissed

Case No. 0:15-cv-00550, United States District Court, District of Minnesota
Smith et al. v. Securus Technologies, Inc.
Description: Class action regarding an alleged violation the Telephone Consumer Protection Act.
Status: Dismissed

Case No. 15-02259-43, In the 431st District Court, Denton County, Texas
Rice v. Denton County, Texas, et al.
Description: Complaint filed by an incarcerated individual regarding video visitation.
Status: Dismissed

Case No. 5-02363-431, In the 431st District Court, Denton County, Texas
Young et al. v. Securus Technologies Holdings, Inc.
Description: Class action alleging antitrust violations in relation to video visitations and "no in-person visits" policy in Denton County Correction Facilities.
Status: Dismissed

Case No. 015V02493, Superior Court of California, County of Los Angeles
Vafaee v. Securus Technologies, Inc.
Description: Small claims regarding an alleged violation of the Telephone Consumer Protection Act.
Status: Dismissed

Case No. 2:15-cv-03926, United States District Court, Central District of California
Vafaee et al. v. Securus Technologies, Inc.
Description: Class action lawsuit alleging violation of the Telephone Consumer Protection Act.
Status: Dismissed

Case No. SC15-007JP1, In the County Court at Law, Fannin County, Texas
Buholtz v. Securus Technologies, Inc.
Description: Small claims alleging Defendant owed Plaintiff a refund balance of approximately $30.00.
Status: Dismissed

Case No. DC-15-07853, In the 193rd Judicial District Court, Dallas County, Texas
Securus Technologies, Inc. et al. v. Continental Prison Systems, Inc.
Description: Complaint regarding non-performance to a specific contract
Status: Settled

Case No. 1:16-cv-02874-RLY-MJD, United States District Court for the Southern District of Indiana
Sloan v Securus Technologies, Inc.
Description: Complaint regarding alleged calls placed from an individual in a facility Securus serviced.
Status: Dismissed

Case No. 3:13-cv-03009-K, In the United States District Court for the Northern District of Texas, Dallas Division
*Securus Technologies, Inc. v. Global Tel*Link Corporation*
Description: Patent infringement filed by Securus against GTL.
Status: Dismissed

Case No. 3:14-cv-0829-N, In the United States District Court for the Northern District of Texas, Dallas Division
*Global Tel*Link Corporation v. Securus Technologies, Inc.*
Description: Patent infringement filed by GTL against Securus.
Status: Settled

Case No. 14-5258 TLB, In the United States District Court for the Western District of Arkansas
Susan Mojica v. Securus Technologies, Inc.
Description: Civil rights class action challenging the constitutionality of exclusive contracts for phone service.
Status: Settled

Case No. 20C011412CT244, In the United States District Court for the Northern District of Texas
*Securus Technologies Inc. v. Global Tel*Link Corporation*
Description: Patent infringement suit filed by Securus against GTL.
Status: Settled

Case No. 3:16-cv-01338-D, In the District Court, Dallas County, Texas
*Securus Technologies Inc. v. Global Tel*Link Corporation*
Description: Patent infringement suit filed by Securus against GTL.
Status: Settled

Case No. DC-16-05352, In the United States District Court for the Northern District of Texas, Dallas Division
*Securus Technologies, Inc. v. Global Tel*Link Corporation*
Description: Tortious interference claim against GTL for false statements concerning Securus.
Status: Settled

Case No. 3:16-cv-01283-JM-MDD, In the United States District Court, Southern District of California
Romero et al. v. Securus Technologies, Inc.
Description: Class action alleging that Securus improperly recorded attorney-client calls.
Status: Settled

Case No. 192575-1, In the Chancery Court for Knox County, Tennessee
Cotham v. Nicholas Jay Yeager et al.
Description: Plaintiffs alleged that Securus/Anderson County contract extension violated state law.
Status: Trial court granted Securus's judgment on the pleadings; upheld on appeal.

Case No. 2016-26291CAD1, In the County Court in and for Miami-Dade County, Florida
Evans, Jr. v. Ryan Shapiro et al.
Description: Plaintiff alleged delayed or inoperable downloads to his JP5 tablet.
Status: Dismissed

Case No. 16.3586 H, Commonwealth of Massachusetts Superior Court, Suffolk County
Hernandez v. Securus Technologies, Inc.
Description: Claim alleging unauthorized access to calls recordings.
Status: Dismissed

Case No. 4:16-cv-00947 SRB, United States District Court for the Western District of Missouri
Crane et al. v. CoreCivic et al.
Description: Class action (attorney plaintiffs) alleging improperly recorded attorney calls.
Status: Settled

Case No. TTDCV175007178S, Superior Court of Connecticut, Judicial District of Tolland and Rockville
*Taylor v. Global Tel*Link Corporation et al.*
Description: Claims concerning the provision of international calls.
Status: Summary judgment granted for Securus.

Case No. 5:17-cv-05008-TLB, In the United States District Court for the Western District of Arkansas
Brown et al. v. Securus Technologies, Inc.
Description: Class action alleging that Securus violated the Arkansas and Illinois deceptive trade practices acts.
Status: Two claims dismissed; consent judgment entered for the remaining claim.

Case No. A-005465-16, Superior Court of New Jersey Law Division – Mercer County
Securus Technologies, Inc. v. Christie, et al.
Description: Securus challenged a New Jersey rate cap law.
Status: Dismissed

Case No. 2017 CA 00243 B, Superior Court of the District of Columbia, Civil Division
Thompson v. Securus Technologies, Inc.
Description: *Pro se* plaintiff alleges that Securus attempted to circumvent fee rules on prepaid calling account.
Status: Securus motion for summary judgment granted.

Case No. DC-17-04974, 192nd Judicial District Court of Dallas County, Texas
Securus Technologies, Inc. v. Emerald Correctional Management, L.L.C. et al.
Description: Securus alleged fraudulent inducement, negligent misrepresentation, breach of contract, and unjust enrichment against defendant in connection with the parties' telephone service agreement.
Status: Settled

Case No. 2:17-cv-02320-JAR-JPO
Huff et al. v. CoreCivic, Inc., et al.
Description: Class action (incarcerated plaintiffs) alleging improperly recorded attorney calls.
Status: Settled

Case No. SCC 670853, Centralized Small Claims Court, Hartford, Connecticut
Case No. HHD-CV17-5045779-S, State of Connecticut Superior Court, Rockville, Connecticut
Salatto v. Securus Technologies et al.
Description: *Pro se* plaintiff alleged that Securus failed to credit money to his telephone account.
Status: Settled

Case No. HHDCV175049317S, Superior Court of Connecticut, Judicial District of Hartford at Hartford
Lewis v. Securus Technologies, Inc., et al.

Description: *Pro se* plaintiff alleged that Securus owed him $25.00 toward his calling account.
Status: Dismissed

Case No. HHDCV175049297S, Superior Court of Connecticut, Judicial District of Hartford at Hartford
Raffone v. Securus Technologies, Inc. et al.
Description: *Pro se* plaintiff alleged that Securus billed for time not used on his calling account.
Status: Dismissed

Case No. 2:17-cv-12545-AC-APP, In the United States District Court, Eastern District of Michigan, Detroit
Jones-Bey v. JPay, Inc., et al.
Description: *Pro se* plaintiff alleged deficient performance of a JP5mini tablet.
Status: Dismissed

Case No. UWY-CV18-5022662-S, State of Connecticut – Waterbury Superior Court
Sterling, et al. v. Securus Technologies, Inc., et al.
Description: *Pro se* plaintiffs alleged that calling rates violated the Connecticut Unfair Trade Practices Act.
Status: Dismissed

Case No.: 18203772-1, In the Superior Court of Washington for Spokane County
Lawson, Sr. v. JPay, et al.
Description: *Pro se* plaintiff asserted claims regarding tablet performance.
Status: Dismissed

Case No. 1:99-mc-09999, In the United States District Court for the District of Delaware
Inventergy LBS, LLC v. Securus Technologies, Inc.
Description: Patent infringement suit filed by Inventergy against Securus.
Status: Settled

Case No. HHD-CV-19-5057391-S, In the Superior Court, Judicial District of Hartford, at Hartford
Conquistador v. Securus Technologies, Inc.
Description: *Pro se* plaintiff alleged that Securus failed to properly refund an account balance.
Status: Dismissed

Case No.: 2018-042904, In the Circuit Court of the Eleventh Judicial Circuit, Miami-Dade County
Small v. JPay et al.
Description: Former employee alleged unpaid wages, discrimination, and violations of the Equal Pay Act.
Status: Settled

Case No. D101CV201900504, First Judicial District Court, Santa Fe County, New Mexico
Delgado v. Securus Technologies, Inc.
Description: *Pro se* plaintiff alleged failure to refund a debit account post release.
Status: Dismissed

Case No. 18cv2187, In the Eighteenth Judicial District Court, Sedgwick County, Kansas, Civil Department
Bunyard v. Easter, et al.
Description: *Pro se* plaintiff alleged that Securus failed to properly connect calls.
Status: Settled

Case No. 4:19-cv-00285-WS-HTC, United States District Court for the Northern District of Florida
Strange v. J-Pay et al.

Description: *Pro se* plaintiff alleged violations of his First, Fifth, and Fourteenth Amendment rights.
Status: Dismissed

Case No. 3:19-cv-43-GNS, United States District Court, Western District
Montgomery v. Securus Technologies, et al.
Description: *Pro se* plaintiff alleged that Securus records wrongfully accused him of a crime he did not commit.
Status: Dismissed

Case No. 2020L 000028, In the Circuit Court of the Twenty-Third Judicial Circuit, Kendall County, Illinois
Young v. Kendall County, Illinois, et al.
Description: Plaintiff alleged that she was injured by a Securus video visitation terminal.
Status: Settled

Case no. 20-223-JPG, In the United States District Court for the Southern District of Illinois
Henneberg v. Securus Correctional Services
Description: *Pro se* plaintiff alleged ineffective provision of services.
Status: Dismissed

No. 2020-CV-02371, In the South Central Judicial District, County of Burleigh, ND
Burke v. Securus Technologies et al.
Description: *Pro se* plaintiff alleged tablet defects and excessive money transfer fees.
Status: Dismissed

Case No.: 2021-02094, In the Superior Court of the District of Columbia
Fontanez v. Securus Technologies
Description: *Pro se* plaintiff alleges that his emails to an incarcerated individual were deleted and blocked.
Status: Dismissed

Case No. 1:17-cv-00073-ACL, United States District Court, Eastern District of Missouri, Southeastern Division
Cooper et al v. Hutcheson et al.
Description: Plaintiffs allege claims arising out of former sheriff Cory Hutcheson's misuse of Securus product.
Status: Settled

Case No. 1:20-cv-00295-JDL, In the United States District Court for the District of Maine
Pratt, et al. v. Securus Technologies, Inc.
Description: Putative class action alleging that Securus violated the federal and Maine wiretap acts.
Status: Dismissed

Case No.: 21-DC V-284005, In the District Court of Fort Bend County, Texas, 268th Judicial District
Konrad, et al. v. Rosilez, et al.
Description: Claims arising from a crime committed by an individual allegedly wearing ankle monitor.
Status: Dismissed

Case No.: 21-16617-CP, 50th Judicial Circuit Court of Chippewa County, Michigan
Taylor v. JPay, Inc., Securus Technologies, LLC, et al.
Description: *Pro se* plaintiff alleges issues with JPay tablet and services.
Status: Dismissed

Open Matters - Affiliates

Case No.: 2:21-cv-07401, United States District Court, Central District of California
Cain, et al. v. JPay, Inc., et al.
Description: Putative class asserts claims related to JPay's debit release card product.
Status: Pending

Case No.: 20-2-00-201-23, Superior Court of Washington, Mason County
Burton et al. v. JPay LLC
Description: Incarcerated individuals allege issues with JPay products and services.
Status: Pending
Case No.: 2018 CV 0470, Common Pleas Court of Richland County, Ohio
Graham v. JPay, et al.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 7:21-cv-05487-KMK, United States District Court, Southern District of New York
DuBarry, et al. v. JPay, Inc., et al.
Description: Incarcerated individuals allege claims relating to censorship of explicit material.
Status: Pending

Case No.: 4:21cv367-WS/MAF, United States District Court, Northern District of Florida
Peterka v. JPay LLC et al
Description: Incarcerated individual alleges claims relating to printing of JPay messages.
Status: Pending

Case No.: G-4801-CI-0202102067-000, Common Pleas Court of Lucas County, Ohio
Burfitt v. JPay, Inc. et al.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: G-4801-CI-0202102834-000, Common Pleas Court of Lucas County, Ohio
Griffin v. Joe Doe, CEO of JPay
Description: Incarcerated individual alleges issues related to accessory product.
Status: Pending

Case No.: 2021 CV 0556 R, Common Pleas Court of Richland County, Ohio
Watson v. JPay, Inc.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 2022CVI00089, Elyria Municipal Court, Ohio
Guy v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 2020 CV 0423, Court of Common Pleas, Richland County, Ohio
Johnson v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 2021CV0023, Court of Common Pleas, Richland County, Ohio

Keys v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

1.

Case No.: 2021CVI02077, Elyria Municipal Court, Ohio
Dawson v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 21-12-214-GC, 93rd District Court, County of Alger, MI
Brown v. JPay Inc.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 21-12-215-GC and Case No. 21-11-208-SC, 93rd District Court, County of Alger, MI
Boudreaux v. JPay Inc.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 21-12-216-GC, 93rd District Court, County of Alger, MI
Louis v. JPay Inc.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 21-12-217-GC, 93rd District Court, County of Alger, MI
Pickett v. JPay Inc.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 21-11-212-GC, 93rd District Court, County of Alger, MI
Hubbard-Bey v. JPay Inc.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 5:18-CV-03146-SAC, Butler County District Court, 13th Judicial District, Kansas
Blake v. JPay, et al.
Description: Incarcerated individual alleges claims relating to censorship of explicit material.
Status: Pending

Case No.: 21-SC-128, Wakulla County Court, FL
McSwain v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Docket No.: MER-L-424-18, In the Superior Court of New Jersey, Special Civil Part
A. Dixon v. JPay, Inc., et al.
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 680CL22000017-00, Lynchburg Circuit Court, Virginia

Perry v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 35-2021-SC-003738-A, County Court of Lake County, Florida
Johnson v. JPay
Description: Incarcerated individual alleges issues related to his JPay tablet.
Status: Pending

Case No.: 16-CV-20121-DPG, United States District Court for the Southern District of Florida
Kobel et al. v. JPay, Inc.
Description: Putative class asserts claims related to JPay's money transfer and money order products.
Status: Pending

Closed Matters - Affiliates

Case No.: 21-01354CA01, Circuit Court of the Eleventh Judicial Circuit, Miami-Dade County
Brown v. JPay, et al.
Description: Claims regarding FL DOC's handling of COVID19 and the confiscation of tablets.
Status: Dismissed

Case No.: 2020-CA-002169, In the County Court of Leon County, Florida
Hasanati v. JPay, et al.
Description: Claims regarding FL DOC's confiscation of tablets.
Status: Dismissed

Case No.: 2021CVI02030, Elyria Municipal Court, Ohio
Camacho v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Settled

Case No.: CV-01-2019461, Fourth Judicial District, Ada County, Idaho
O'Shea v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet and purchased content.
Status: Dismissed

Case No.: 2021CVI02671, Elyria Municipal Court, Ohio
Hlavsa v. JPay LLC
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Settled

Case No.: 19000068SCAXMX, County Court of the 3rd Judicial Circuit, Hamilton County, Florida
Lutz v. JPay
Description: Plaintiff filed a lawsuit claiming JPay overcharged plaintiff for a JP5 tablet.
Status: Dismissed

Case No.: 2021CVI01383, Elyria Municipal Court, Ohio
Capone v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 185CL21001099-00, Tazewell Circuit Court, VA
Foran, Sr. v. JPay, Inc.
Description: Plaintiff filed a complaint claiming issues with his JPay tablet and media services.
Status: Settled

Case No.: 2021CVI01878, Elyria Municipal Court, Ohio
Grodek v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet and content.
Status: Settled
Case No.: 2021CVI01013, Elyria Municipal Court, Ohio
Davis v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Settled

Case No.: 2020 35909 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Stuckey v. JPay
Description: Plaintiff filed a complaint claiming downloading issues with moves and games.
Status: Dismissed

Case No.: 2021CVI01053, Elyria Municipal Court, Ohio
Williams v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Settled

Case No.: 2020 34032 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Garrison v. JPay
Description: Plaintiff filed a complaint claiming his tablet is having issues downloading movies.
Status: Settled

Case No.: 2021CVI00478, Elyria Municipal Court, Ohio
McDermott v. JPay
Description: Plaintiff filed a complaint claiming his tablet is defective.
Status: Settled

Case No.: 2:18-cv-11086-SFC-PTM, United States District for the Eastern District of Michigan
Kensu v. JPay, Inc.
Description: Putative class action lawsuit alleging defects in JPay's products and services.
Status: Dismissed

Case No.: 21BFSC00401, Superior Court of California, County of Los Angeles
Moore v. JPay
Description: Plaintiff filed a complaint claiming a $70.00 money order she sent never posted.
Status: Settled

Case No.: 2021CVI01103, Elyria Municipal Court, Ohio
Williams v. JPay
Description: Plaintiff filed a complaint claiming tablet and downloading issues.
Status: Settled

Case No.: 2021CVI00501, Elyria Municipal Court, Ohio
Cloud v. JPay
Description: Plaintiff filed a complaint claiming he is not satisfied with JPay's services.
Status: Settled

Case No.: 2021CVI00362, Elyria Municipal Court, Ohio
Spitler v. JPay
Description: Plaintiff filed a complaint claiming he didn't receive products that he paid for.
Status: Settled

2.

Case No.: 2021CVI00448, Elyria Municipal Court, Ohio
White v. JPay
Status: Settled

Case No.: 2021CVI01052, Elyria Municipal Court, Ohio
Williams v. JPay
Description: Plaintiff filed a complaint claiming issues with his JP6 tablet.
Status: Settled

Case No.: 2021CVI00233, Elyria Municipal Court, Ohio
Taylor II v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2021CVI00227, Elyria Municipal Court, Ohio
Outlaw, Jr. v. JPay
Description: Plaintiff filed a complaint claiming JPay's products are defective.
Status: Settled

Case No.: 2021CVI00481, Elyria Municipal Court, Ohio
Grodek v. JPay
Description: Plaintiff filed a complaint claiming issues with his JP6 tablet.
Status: Settled

Case No.: 2020CVI02169, Elyria Municipal Court, Ohio
Prather v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2021CVI00447, Elyria Municipal Court, Ohio
McCrary v. JPay
Description: Plaintiff filed a complaint claiming his tablet is defective.
Status: Settled

Case No.: 2021CVI00361. Elyria Municipal Court, Ohio
David Spencer v. JPay
Description: Plaintiff filed a complaint claiming he didn't receive a product that he paid for.
Status: Settled

3.

Case No.: 2020 39737 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Kibwikia v. JPay
Description: Plaintiff filed a complaint regarding the FL DOC JP6 Tablet Loaner Program.
Status: Settled

Case No.: 2021CVI00496, Elyria Municipal Court, Ohio
Fuller v. JPay
Description: Plaintiff filed a complaint claiming issues with his JP6 tablet.
Status: Settled

Case No.: 2020-166499-GC, Muskegon County, 60th District Court, Michigan
Cardello Smith v. JPay, et al.
Status: Settled

Case No.: CV2021-002653, Superior Court of Arizona, Maricopa County
Rodriguez v. JPay, et al.
Description: Plaintiff claimed JPay's subcontractor caused vehicle accident while she was a passenger.
Status: JPay dismissed from suit

Case No.: 2021CVI00021, Elyria Municipal Court, Ohio
Konoff v. JPay
Description: Plaintiff filed a complaint claiming his tablet is defective.
Status: Settled

Case No.: 2020CVI02348, Elyria Municipal Court, Ohio
Lindeman v. JPay
Description: Plaintiff filed a complaint claiming his tablet is defective.
Status: Settled

Case No.: 2019-36570-COCI, Volusia County Circuit Court, 7th Judicial Circuit
Williams v. JPay
Description: Plaintiff filed a complaint alleging his tablet will not hold a charge and is unresponsive.
Status: Dismissed

Case No.: 2020CVI02324, Elyria Municipal Court, Ohio
Capone v. JPay
Description: Plaintiff filed a complaint claiming the battery on his tablet is defective.
Status: Settled

Case No.: CVI2000016, Lebanon Municipal Court, Ohio
Gerald v. JPay
Description: Plaintiff filed a complaint claiming the battery in his tablet is defective.
Status: Settled

Case No.: 2019 CV 0763, Common Pleas Court of Richland County, Ohio
Graham v. JPay, et al.
Description: Plaintiff filed a complaint against JPay, JAMS, and AAA regarding arbitration
Status: Dismissed

Case No.: 2020CVI 00262, Elyria Municipal Court, Ohio
Spitler v. JPay
Description: Plaintiff filed a complaint alleging he never received two money orders from his family.
Status: Settled

Case No.: 2020-SC-001195, In the County Court of Leon County, Florida
Scott, Jr. v. JPay, et al.
Description: Plaintiff filed a complaint arising out of JPay's replacement of Keefe Commissary as content provider
Status: Dismissed

Case No.: 20-8-175-SC, 93rd Judicial District, City of Munising, Michigan
Flint v. JPay
Description: Plaintiff filed a complaint claiming the battery on his tablet is swollen.
Status: Dismissed

Case No.: 20-1494-SC and Case No.: 21-33-GC, Montcalm County District Court, Michigan
Moffat v. JPay
Description: Plaintiff filed a small claims complaint claiming his tablet is defective.
Status: Settled

Docket No.: ESX-L-003029-20, Superior Court of NJ, Essex County, Law Division
Pantusco v. JPay
Description: Plaintiff filed a complaint claiming tablet issues and claiming JPay's Terms of Service violate his first amendment rights.
Status: Dismissed

Case No.: 2020-002018-CB, Muskegon County, 14th Circuit Court, Michigan
Cardello Smith v. JPay, et al.
Description: Plaintiff filed a complaint claiming he is having issues downloading games onto his tablet.
Status: Dismissed

Case No.: 2020CVI01234, Elyria Municipal Court, Ohio
Russ v. JPay
Description: Plaintiff filed a complaint alleging photographs have been deleted from his tablet.
Status: Settled

Case No.: 19-959-SC and Case No.: 19-1375-GC, Montcalm County District Court, Michigan
Lovelace v. JPay
Description: Plaintiff filed a complaint in the alleging his photos were removed from his account.
Status: Settled

Case No.: 2020CVI01915, Elyria Municipal Court, Ohio
Moore v. JPay
Description: Plaintiff filed a complaint claiming after he was released he sent his tablet to JPay's warehouse.
Status: Settled

Case No.: 2019 38524 COCI, Volusia County Circuit Court, 7th Judicial Circuit

Doerfler v. JPay
Description: Plaintiff filed a complaint alleging issues with his tablet.
Status: Dismissed

Case No.: 18-6884-CP, In the State of Michigan, Baraga County Circuit Court
Richards v. JPay
Description: *Pro se* plaintiff lawsuit alleging violation of state law.
Status: Dismissed

Case No.: 2020CVI 01108, Elyria Municipal Court, Ohio
Dawson v. JPay
Description: Plaintiff filed a complaint alleging issues with his tablet.
Status: Dismissed

Case No.: 2020 34567 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Baker v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Settled

Case No.: 2020 34428 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Robinson v. JPay
Description: Plaintiff filed a complaint claiming issues with this tablet.
Status: Settled

Case No.: 2020CVI 01020, Elyria Municipal Court, Ohio
Keyes v. JPay
Description: Plaintiff filed a complaint alleging he is having issues downloading media content.
Status: Settled

Case No.: 2020CVI 01070, Elyria Municipal Court, Ohio
White v. JPay
Description: Plaintiff filed a complaint alleging he is having issues with his tablet.
Status: Settled

Case No.: 2020CVI01124, Elyria Municipal Court, Ohio
Aleman v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Settled

Case No.: 2:19-cv-14137, United States District Court for the Southern District of Florida
Rodriguez, et al. v. JPay Inc., et al.
Description: Putative class action arising out of JPay's replacement of Keefe Commissary as provider.
Status: Dismissed

Case No.: 19-cv-20341, In the United States District Court of Florida for the Southern District
Jackson v. JPay, et al.
Description: Plaintiff filed a complaint over the alleged use of his name, which he claimed was a copyright.
Status: Dismissed

Case No.: 2020 34056 COCI, Volusia County Circuit Court, 7th Judicial Circuit

Thomas v. JPay
Description: Plaintiff filed a complaint claiming issues with his tablet.
Status: Dismissed

Case No.: 2020 34779 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Noe v. JPay
Description: Plaintiff filed a complaint claiming his tablet.
Status: Settled

Case No.: 20-201CC, Charlotte County Circuit Court, 20th Judicial Circuit
Lewis v. JPay
Description: Plaintiff filed a complaint claiming he was unable to take advantage of a tablet promotion.
Status: Settled

Case No.: 2020 31830 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Luzier III v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2020 31850 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Barbour v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2020 32773 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Acevedo v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2020 33907 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Francois v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019-SC-000784, In the County Court of Leon County, Florida
Peavy v. JPay, et al.
Description: Complaint arising out of JPay's replacement of Keefe Commissary as the content provider.
Status: Dismissed

Case No.: 2020 32771 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Lewis v. JPay
Description: Plaintiff filed a complaint claiming downloading issues with his tablet.
Status: Settled

Case No.: 2020 32772 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Tate v. JPay
Description: Plaintiff filed a complaint claiming downloading issues with his tablet.
Status: Settled

Case No.: 2020CVI00706, Elyria Municipal Court, Ohio

Quinones v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2020CVI00302, Elyria Municipal Court, Ohio
Moore v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2020CVI00801, Elyria Municipal Court, Ohio
Williams v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 77D01-1906-SC-000123, In the Superior Court of Sullivan County, State of Indiana
Griffith v. JPay, Inc., et al.
Description: Plaintiff filed a complaint claiming funds were deposited into wrong account.
Status: Settled

Case No.: 77D01-1906-SC-000137, Sullivan Superior Court, Indiana
Ashby v. JPay, et al.
Description: Plaintiff alleging he lost funds from his JPay media account when another provider took over.
Status: Settled

Case No.: 2020 30694 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Williams v. JPay
Description: Plaintiff filed a complaint alleging tablet issues.
Status: Settled

Case No.: 2020 31031 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Williams v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 82-CO-20-98, 10th District Court, Washington County, Minnesota
Thomas a/k/a Amen El, Pharaoh El-Forever v. JPay
Description: Plaintiff filed a complaint claiming issues with his media content.
Status: Settled

Case No.: 2019CVI03349, Elyria Municipal Court, Ohio
Stansell v. JPay
Description: Plaintiff filed a complaint claiming issues with this media content.
Status: Settled

Case No.: 18CV196495, In the Court of Common Pleas, Lorain County, OH
Goins, et al. v. JPay
Description: Plaintiffs filed a lawsuit alleging false advertisement and faulty equipment.
Status: Settled

Case No.: 2020CVI00037, Elyria Municipal Court, Ohio

Davis v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019CVI03543, Elyria Municipal Court, Ohio
Beaty v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 19CECL00797, Superior Court of California
Washington v. JPay
Description: Plaintiff filed a complaint claiming he was unable to utilize his tablet at facility.
Status: Settled

Case No. 2019-37129-COCI, Volusia County Circuit Court, 7th Judicial Circuit
Anthony v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Docket No.: MER-L-000282-18, In the Superior Court of New Jersey, Mercer County
Lasane v. JPay, Inc.
Description: *Pro se* plaintiff filed a lawsuit alleging breach of contract.
Status: Dismissed

Case No.: 2019 37381 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Spindler v. JPay
Description: Plaintiff then filed a complaint claiming tablet issues.
Status: Dismissed

Case No.: 2019CVI03368, Elyria Municipal Court, Ohio
Lindsey v. JPay
Description: Plaintiff filed a complaint claiming issues with his media content.
Status: Settled

Case No.: 2019 37563 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Wagner v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019 37951 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Timmons v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019CVI01582, In the Elyria Municipal Court, Lorain County, Ohio
Moore v. JPay, Inc.
Description: Plaintiff filed a complaint claiming issues with this tablet.
Status: Settled

Case No.: 2019-36362-COCI, Volusia County Circuit Court, 7th Judicial Circuit
Williams v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019 38169 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Tomlinson v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019CVI02938, Elyria Municipal Court, Ohio
Blaising v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019CVI03083, Elyria Municipal Court, Ohio
Pudder v. JPay
Description: Plaintiff filed a complaint claiming tablet issues
Status: Settled

Case No.: 2019 37128 COCI, Volusia County Circuit Court, 7th Judicial Circuit
Binz v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019-36919-COCI, Volusia County Circuit Court, 7th Judicial Circuit
Wells v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019CVI02764, Elyria Municipal Court, Ohio
Taylor v. JPay
Description: Plaintiff filed a complaint claiming issues with his media content.
Status: Settled

Case No.: 2019CVI02765, In the Elyria Municipal Court, Lorain County, Ohio
Bruhn v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 4:18-cv-00730, United States District Court for the Eastern District of Texas
Salim v. JPay Inc.
Description: Putative class action with claims regarding video visitation services.
Status: Dismissed

Case No.: 2:18-cv-00315-R-MRW, United States District Court Central District of California
Reyes, et al. v. JPay, Inc., et al.
Description: Putative class action arising out of alleged fees charged to plaintiffs on debit release cards.
Status: Dismissed

Case No.: 2019CVI01735, Elyria Municipal Court, Lorain County, Ohio
Johnson v. JPay, Inc.
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No. 2019-35666-COCI, Volusia County Circuit Court, 7th Judicial Circuit
Cieplensky v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 17-M41C-00594, In the Magistrate Court of Raleigh County, West Virginia
Umberger v. J Pay Inc.
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019 35508-COCI, In the Seventh Judicial Circuit – Volusia County
Kahane v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2019CVI01974, In the Elyria Municipal Court, Lorain County, Ohio
Davis v. JPay
Description: Plaintiff filed a complaint claiming issues with media content.
Status: Settled

Case No.: 08-2019-SC 174, In Burleigh County, North Dakota
Burke v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 181 C 3008, In the State of Michigan, Judicial District, Judicial Circuit
Hollister v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Dismissed

Case No.: 46D02 18 09 PL1563, In the Superior Court of Laporte County, State of Indiana
Justise Sr. v. JPay
Description: Plaintiff filed a complaint claiming issues with his media account.
Status: Settled

Case No.: 113-5-17-Wrsc, In the Superior Court of Windsor, Vermont
Weber v. JPay, Inc.
Description: Plaintiff filed a complaint claiming issues with the kiosk at his facility.
Status: Closed

Case No.: 2019 31772 COCI, In the Seventh Judicial Circuit – Volusia County
Kahane v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.

Status: Settled

Case No.: EMC 2018CVI01570, In the Elyria Municipal Court, Small Claims; Civil Division
Spitler v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 18SM-0133, In the Superior Court of the State of California in and for the County of Kings
Morales v. JPay
Description: Plaintiff filed a complaint claiming issues with this media account
Status: Settled

Case No.: 1812-SC-000278, In the Sullivan Circuit/Superior Courts, State of Indiana (Small Claims)
Forte v. JPay
Description: *Pro se* Plaintiff filed complaint claiming issues with his media account.
Status: Settled

Case No.: 77D01-1812-SC-000273, Sullivan Circuit, Superior Courts/Indiana Supreme Court
Wallace v. JPay
Description: Plaintiff filed a complaint claiming issues with his media account.
Status: Dismissed

Case No.: 46C01-1812-CT-2280, In the LaPorte Circuit Court, State of Indiana
Fortson v. JPay
Description: *Pro se* Plaintiff filed a complaint claiming issues with his media account.
Status: Settled

Case No.: 2018-027529-SP-05, In the County Court in and for Miami-Dade County, FL
Robertson v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Settled

Case No.: 2018CVI01173, In the Elyria Municipal Court of Lorain, Ohio (Small Claims)
Love v. JPay, Inc.
Description: Plaintiff filed a complaint claiming issues with his media content.
Status: Settled

Case No.: 15-2-01122-4, Superior Court of the State of Washington in and for the County of Thurston;
Kozol, et al. v. JPay, Inc.
Description: Plaintiffs filed a complaint claiming tablet issues.
Status: Dismissed

Case No.: 2016 CV 190310, In the Court of Common Pleas, Lorain County, Ohio
Spitler v. JPay, Inc.
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Dismissed

Case No.: 2014-032194-CA-01 and Case No.: 2013-006816-CA-01
11th Judicial Circuit, Miami-Dade County

10800 Biscayne Holdings, LLC v. JPay, Inc.
Description: Lawsuit regarding a premises that JPay rented.
Status: Settled

Case No.: 2017CVI01582,
Elliott Miller v. JPay, Inc.
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Dismissed

Case No.: 2017CVI02241, In the Elyria Municipal Court of Lorain, Ohio
Jones Sr., et al. v. JPay Services
Description: Plaintiff filed a complaint claiming false advertising.
Status: Settled

Case No.: 17CV001689, In the Superior Court of California, County of Monterey
Carr v. JPay, Inc., et al.
Description: Plaintiff filed a complaint regarding the alleged use of release cards at the California CDCR.
Status: Dismissed

Case No.: 18SMSC0163, Superior Court of California, County of Los Angeles
Zapata v. JPay Inc.
Description: Plaintiff filed a complaint regarding the alleged fees associated with a release card.
Status: Settled

Case No.: MER-L-000055 18, In the Superior Court of New Jersey, Mercer County Vicinage
Reid v. JPay, et al.
Description: *Pro se* plaintiff filed suit alleging breach of contract,.
Status: Dismissed

Case No.: 2:17-CV-10212-KM-SCM, In the United States District Court for the District of New Jersey
DeFazio v. JPay, Inc.
Description: *Pro se* putative class action lawsuit claiming consumer protection act violations.
Status: Settled

Case No.:2016-CV-0615, In the Court of Common Pleas Richland County, Ohio
Graham v. JPay
Description: *Pro se* plaintiff filed a complaint claiming breach of contract.
Status: Settled

Case No.: GV15046286-01, Virginia Beach General District Court
Edwards v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Dismissed

Case No. 118-12-16 Ossc, Vermont Superior Court, Small Claims
Witham v. JPay
Description: Plaintiff filed a complaint claiming tablet issues.
Status: Dismissed

Case No.: 2015CA-002050-000-00, In the Tenth Judicial Circuit, In and for Polk County, Florida

Chandler v. JPay Inc.
Description: Plaintiff filed a complaint claiming he was entitled to records under the Public Records Act.
Status: Dismissed

ADMINISTRATIVE PROCEEDINGS

In July 2014, the Alabama Public Service Commission (PSC) issued an extensive proposed order in Docket No. 15957 which specified new ICS provider rules. This order set inmate calling rate caps and other requirements regarding ancillary fees, pre-paid calling cards, billing options, and extensive reporting requirements. On December 9, 2014 the Alabama PSC issued a Final Order making the rules effective Jan. 8, 2015. On December 16, 2014 Securus filed in both the Alabama Supreme Court and in Montgomery County Circuit Court to Appeal and Stay the Alabama PSC Final Order. On Dec. 30, 2014 the Supreme Court "Granted" the Appeal and Stay. Since that time the Alabama PSC Final Order has remained "stayed" as to Securus. Securus continues to work with the Alabama PSC to settle both court cases. In August 2017 Securus and the Alabama PSC reached a mutual agreement. Both court cases have been withdrawn and dismissed.

On August 16, 2016, the SC Office of Regulatory Staff ("ORS") issued a Show Cause case, Docket No: 1997-444-C and 2004-336-C, requiring Securus to demonstrate that its intrastate rates do not exceed its authorized tariff rates. Securus provided multiple documents and responded to multiple data requests demonstrating the actual rates charged to customers do not exceed it authorized tariff rate caps. The SC PSC issued their proposed order dated 1/31/17 to dismiss the Show Cause Petition finding Securus has not charged rates in excess of our SC tariff. Based on the pricing and related information contained in Securus price list filed with both the PSC and ORS, the Commission finds there is sufficient detailed information to accurately determine what rates are paid by consumers. On January 31, 2017 the SC PSC approved the final order and closed the case.

In October 2017, Securus voluntarily entered into a Consent Decree with the Federal Communications Commission ("FCC") to expedite the FCC's approval of a pending transfer of control application and to minimize certain escalating transaction fees, and agreed to pay a civil penalty in connection therewith. Securus does not believe it committed any wrongdoing and the Consent Decree itself explicitly states that it "does not constitute and shall not be construed as either an adjudication on the merits or a factual or legal finding or determination regarding any compliance or noncompliance" with applicable law and that it "does not constitute an admission of liability" by Securus.

In April 2018, Securus was fined $50.00 by the Nevada Public Utilities Commission for an annual report filed late in May of 2017.

In October 2021, Securus subsidiary JPay LLC settled a matter with the Consumer Financial Protection Bureau relating to JPay-branded debit cards that incarcerated individuals in some states receive upon release. The CFPB principally objected to the limitations on how incarcerated individuals receive their funds.

Securus Attachment No. 3:

CO SOS Certificate of Fact of Good Standing, and FCC Registration Form

OFFICE OF THE SECRETARY OF STATE
OF THE STATE OF COLORADO

CERTIFICATE OF FACT OF GOOD STANDING

I, Jena Griswold, as the Secretary of State of the State of Colorado, hereby certify that, according to the records of this office,

Securus Technologies, LLC

is an entity formed or registered under the law of Delaware , has complied with all applicable requirements of this office, and is in good standing with this office. This entity has been assigned entity identification number 19971141098 .

This certificate reflects facts established or disclosed by documents delivered to this office on paper through 02/02/2022 that have been posted, and by documents delivered to this office electronically through 02/04/2022 @ 12:03:09 .

I have affixed hereto the Great Seal of the State of Colorado and duly generated, executed, and issued this official certificate at Denver, Colorado on 02/04/2022 @ 12:03:09 in accordance with applicable law. This certificate is assigned Confirmation Number 13770835 .

Jena Griswold

Secretary of State of the State of Colorado

**********End of Certificate**********

Notice: A certificate issued electronically from the Colorado Secretary of State's Web site is fully and immediately valid and effective. However, as an option, the issuance and validity of a certificate obtained electronically may be established by visiting the Validate a Certificate page of the Secretary of State's Web site, http://www.sos.state.co.us/biz/CertificateSearchCriteria.do entering the certificate's confirmation number displayed on the certificate, and following the instructions displayed. Confirming the issuance of a certificate is merely optional and is not necessary to the valid and effective issuance of a certificate. For more information, visit our Web site, http://www.sos.state.co.us/ click "Businesses, trademarks, trade names" and select "Frequently Asked Questions."

E-Filed

Colorado Secretary of State
Date and Time: 01/13/2020 12:31 PM
ID Number: 19971141098
Document number: 20201033652
Amount Paid: $10.00

Document must be filed electronically.
Paper documents are not accepted.
Fees & forms are subject to change.
For more information or to print copies
of filed documents, visit www.sos.state.co.us.

ABOVE SPACE FOR OFFICE USE ONLY

Statement of Change Changing the True Name

filed pursuant to §7-90-305.5, and if applicable, §7-90-804 of the Colorado Revised Statutes (C.R.S.)

1. For the entity, its ID number and assumed entity name are

ID number 19971141098
(Colorado Secretary of State ID number)

Assumed entity name

_____.

2. The true name is
Securus Technologies, Inc.
_____.

3. The document number of the filed document being changed is 19991020518.

4. The true name has changed.

5. The true name, as changed, is
Securus Technologies, LLC
_____.

6. The assumed entity name (if applicable) is

_____.

7. ☐ This document contains additional information as provided by law.

8. *(Caution: Leave blank if the document does not have a delayed effective date. Stating a delayed effective date has significant legal consequences. Read instructions before entering a date.)*

(If the following statement applies, adopt the statement by entering a date and, if applicable, time using the required format.)

The delayed effective date and, if applicable, time of this document is/are _____.
(mm/dd/yyyy hour:minute am/pm)

Notice:
Causing this document to be delivered to the secretary of state for filing shall constitute the affirmation or acknowledgment of each individual causing such delivery, under penalties of perjury, that the document is the individual's act and deed, or that the individual in good faith believes the document is the act and deed of the person on whose behalf the individual is causing the document to be delivered for filing, taken in conformity with the requirements of part 3 of article 90 of title 7, C.R.S., the constituent documents, and the organic statutes, and that the

individual in good faith believes the facts stated in the document are true and the document complies with the requirements of that Part, the constituent documents, and the organic statutes.

This perjury notice applies to each individual who causes this document to be delivered to the secretary of state, whether or not such individual is named in the document as one who has caused it to be delivered.

9. The true name and mailing address of the individual causing the document to be delivered for filing are

Lozich	Michael		
(Last)	(First)	(Middle)	(Suffix)

4000 International Parkway
(Street name and number or Post Office Box information)

Carrollton	TX	75007
(City)	(State)	(Postal/Zip Code)
(Province – if applicable)	United States	(Country – if not US)

(If the following statement applies, adopt the statement by marking the box and include an attachment.)

☐ This document contains the true name and mailing address of one or more additional individuals causing the document to be delivered for filing.

Disclaimer:
This form/cover sheet, and any related instructions, are not intended to provide legal, business or tax advice, and are furnished without representation or warranty. While this form/cover sheet is believed to satisfy minimum legal requirements as of its revision date, compliance with applicable law, as the same may be amended from time to time, remains the responsibility of the user of this form/cover sheet. Questions should be addressed to the user's legal, business or tax advisor(s).

Delaware

The First State

I, JEFFREY W. BULLOCK, SECRETARY OF STATE OF THE STATE OF DELAWARE, DO HEREBY CERTIFY THAT THE ATTACHED IS A TRUE AND CORRECT COPY OF THE CERTIFICATE OF CONVERSION OF A DELAWARE CORPORATION UNDER THE NAME OF "SECURUS TECHNOLOGIES, INC." TO A DELAWARE LIMITED LIABILITY COMPANY, CHANGING ITS NAME FROM "SECURUS TECHNOLOGIES, INC." TO "SECURUS TECHNOLOGIES, LLC", FILED IN THIS OFFICE ON THE SEVENTEENTH DAY OF DECEMBER, A.D. 2019, AT 11:35 O`CLOCK A.M.

AND I DO HEREBY FURTHER CERTIFY THAT THE EFFECTIVE DATE OF THE AFORESAID CERTIFICATE OF CONVERSION IS THE THIRTY-FIRST DAY OF DECEMBER, A.D. 2019 AT 11:59 O'CLOCK P.M.





2788631 8100V
SR# 20198685030

Authentication: 204239478
Date: 12-17-19

You may verify this certificate online at corp.delaware.gov/authver.shtml

STATE OF DELAWARE

CERTIFICATE OF CONVERSION

FROM A CORPORATION TO A

LIMITED LIABILITY COMPANY PURSUANT TO

SECTION 18-214 OF THE LIMITED LIABILITY COMPANY ACT

FIRST: The jurisdiction where the corporation first formed is Delaware.

SECOND: The jurisdiction immediately prior to filing this Certificate is Delaware.

THIRD: The date the corporation first formed is August 22, 1997.

FOURTH: The name of the Corporation immediately prior to filing this Certificate is SECURUS TECHNOLOGIES, INC.

FIFTH: The name of the Limited Liability Company as set forth in the Certificate of Formation is SECURUS TECHNOLOGIES, LLC.

SIXTH: This certificate of conversion is to become effective on December 31, 2019 at 11:59:59 P.M.

IN WITNESS WHEREOF, the undersigned has executed this Certificate of Conversion on the 13th day of December, 2019.

By: _____
Name: Justin Maroldi
Title: Assistant Secretary

DOC ID - 32805449.2

State of Delaware
Secretary of State
Division of Corporations
Delivered 11:35 AM 12/17/2019
FILED 11:35 AM 12/17/2019
SR 20198685030 - File Number 2788631

Delaware

The First State

I, JEFFREY W. BULLOCK, SECRETARY OF STATE OF THE STATE OF DELAWARE DO HEREBY CERTIFY THAT THE ATTACHED IS A TRUE AND CORRECT COPY OF THE CERTIFICATE OF FORMATION OF "SECURUS TECHNOLOGIES, LLC" FILED IN THIS OFFICE ON THE SEVENTEENTH DAY OF DECEMBER, A.D. 2019, AT 11:35 O`CLOCK A.M.

AND I DO HEREBY FURTHER CERTIFY THAT THE EFFECTIVE DATE OF THE AFORESAID CERTIFICATE OF FORMATION IS THE THIRTY-FIRST DAY OF DECEMBER, A.D. 2019 AT 11:59 O'CLOCK P.M.





2788631 8100V
SR# 20198685030

Authentication: 204239478
Date: 12-17-19

You may verify this certificate online at corp.delaware.gov/authver.shtml

CERTIFICATE OF FORMATION

OF

SECURUS TECHNOLOGIES, LLC

The undersigned, desiring to form a limited liability company (the "Company") pursuant to the Delaware Limited Liability Company Act, Title 6 Delaware Code, Chapter 18, does hereby certify as follows:

FIRST: The name of the limited liability company is Securus Technologies, LLC.

SECOND: The address of the registered office of the limited liability company in the State of Delaware is c/o Corporation Trust Center, 1209 Orange Street, Wilmington, Delaware, 19801. The name of its registered agent at such address is The Corporation Trust Company.

THIRD: This Certificate of Formation is to become effective on December 31, 2019 at 11:59:59 P.M.

IN WITNESS WHEREOF, the undersigned has executed this Certificate of Formation on the 13th day of December, 2019.

By: _____
Name: Justin Maroldi
Title: Assistant Secretary

DOC ID - 32805449.2

State of Delaware
Secretary of State
Division of Corporations
Delivered 11:35 AM 12/17/2019
FILED 11:35 AM 12/17/2019
SR 20198685030 - File Number 2788631



FCC Registration

Search Public Information

Return to FCC Registration Home

Displaying Records 1 (of 1)

FRN	Registrant	Contact	Address	City	State	Zip	Country	RegDate
0006222319	Securus Technologies, LLC	Conde, Debbie	4000 International Parkway	Carrollton	TX	75007	United States	01/23/2002

REFINE SEARCH

Customer Service			
Frequently Asked Questions	Forms Requiring an FRN	Privacy Statement	FCC Home Page
FRN Help Line: 877-480-3201 (Mon.-Fri. 8 a.m.-6 p.m. ET).			
The FRN Help desk has a dedicated staff of customer service representatives standing by to answer your questions or concerns. You can also submit a help request at https://www.fcc.gov/wireless/available-support-services.			

Securus Attachment No. 4:

God Behind Bars Pando App

Pando App Overview

Pando is a revolutionary application from God Behind Bars that makes it possible for incarcerated individuals to engage their spirituality and improve mental health in a new way.

God Behind Bars and Securus partnered to have the Pando application designed specifically for use in the correctional environment, allowing us to deliver high quality content while maintaining necessary security.

Incarcerated individuals are able to specify their current spiritual/mental health needs for the application to recommend relevant messages, sermons, and other content automatically. The Pando application allows incarcerated individuals to access high-quality, uplifting faith-based content using their Securus Tablet.

What Does Pando Provide?

Pando provides 24-hour access to some of the best faith-based and leadership content in the world. God Behind Bars created the application for incarcerated individuals to still be able to stay connected and improve their lives. Through the content itself, incarcerated individuals can learn, grow and experience real life change.



The Pando application can simultaneously improve an incarcerated individual's spiritual journey and mental health through quality teaching, engaging experiences and virtual connection to high quality self-betterment content.

Pando Features

The Pando application provides an enriching and engaging experience that allows incarcerated individuals to receive critical spiritual growth, mental health, and self-betterment content.

High-Quality Streaming Videos

Utilizing Securus Tablets and network, Pando delivers a "Netflix-like" experience for streaming faith-based content in corrections. Incarcerated individuals can scroll & swipe through series of content based on their identified needs and interests.

Videos Include Topics Such As:

- Sermons
- Leadership Videos
- Topical Studies
- Prayer and Meditation
- Self-Help and Self-Betterment Material



Access to the Bible

The Pando app has multiple versions of the bible available within the application with additional tools that make navigation easy.

Prayer Wall

A unique feature of the Pando application is that it allows the ability for incarcerated individuals to submit prayer requests or share wins with others. Users of the application are able to indicate that they are praying for the individual who submitted the prayer.

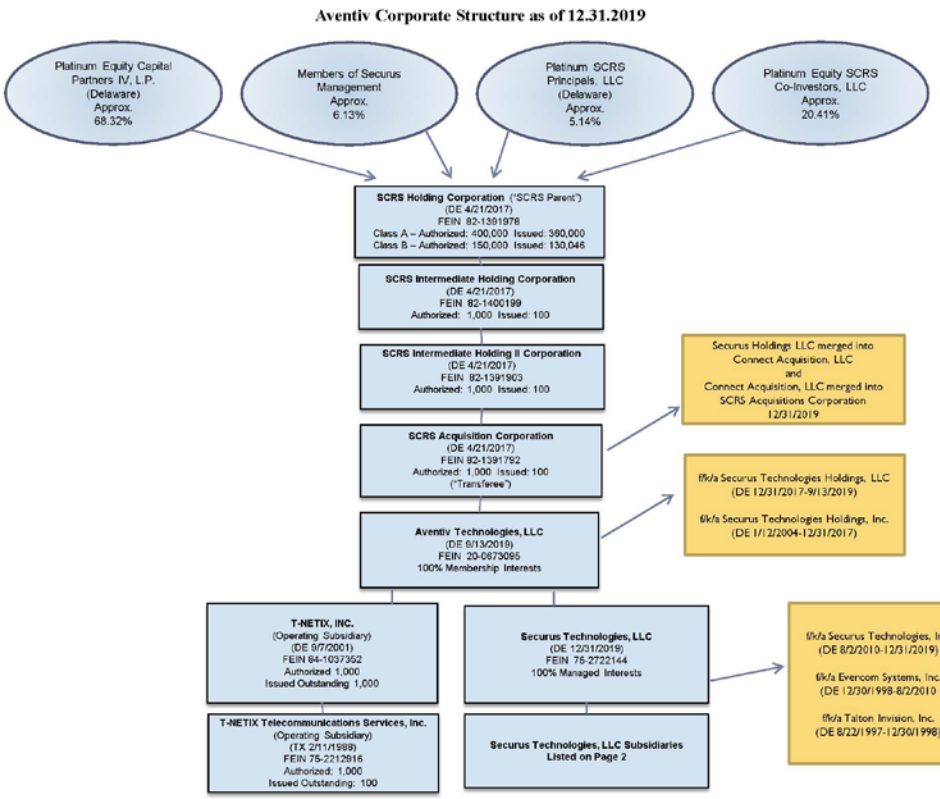
Pando utilizes a prayer auto-generation feature that creates the prayer on behalf of the incarcerated individual so they cannot pass messages or input inappropriate text. Prayers do not include names or identifying information.

Track Goals and Progress

The Pando application allows user accounts to track their progress in the app based on goals set by God Behind Bars. Incarcerated individuals can work towards earning bronze to platinum status by completing goals that include praying for others, submitting prayers and watching videos.

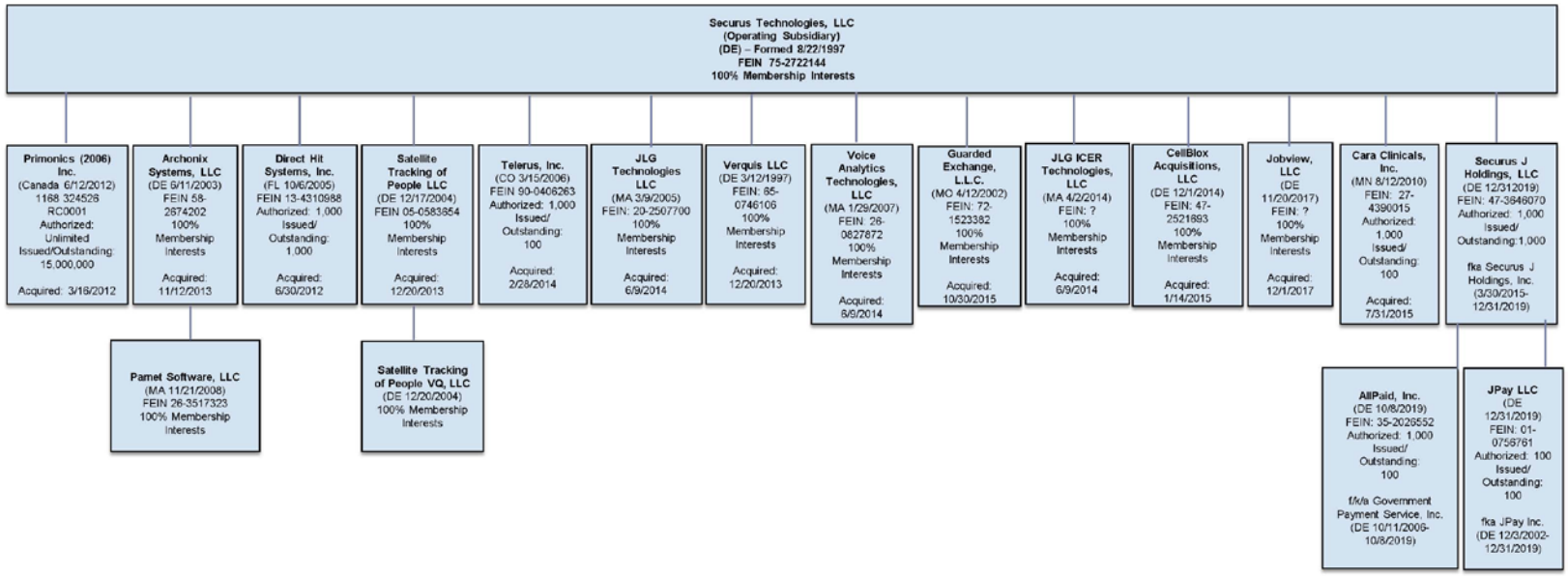
© Securus Technologies, Inc.

Securus Attachment No. 5:
Corporate Org Chart and Entities



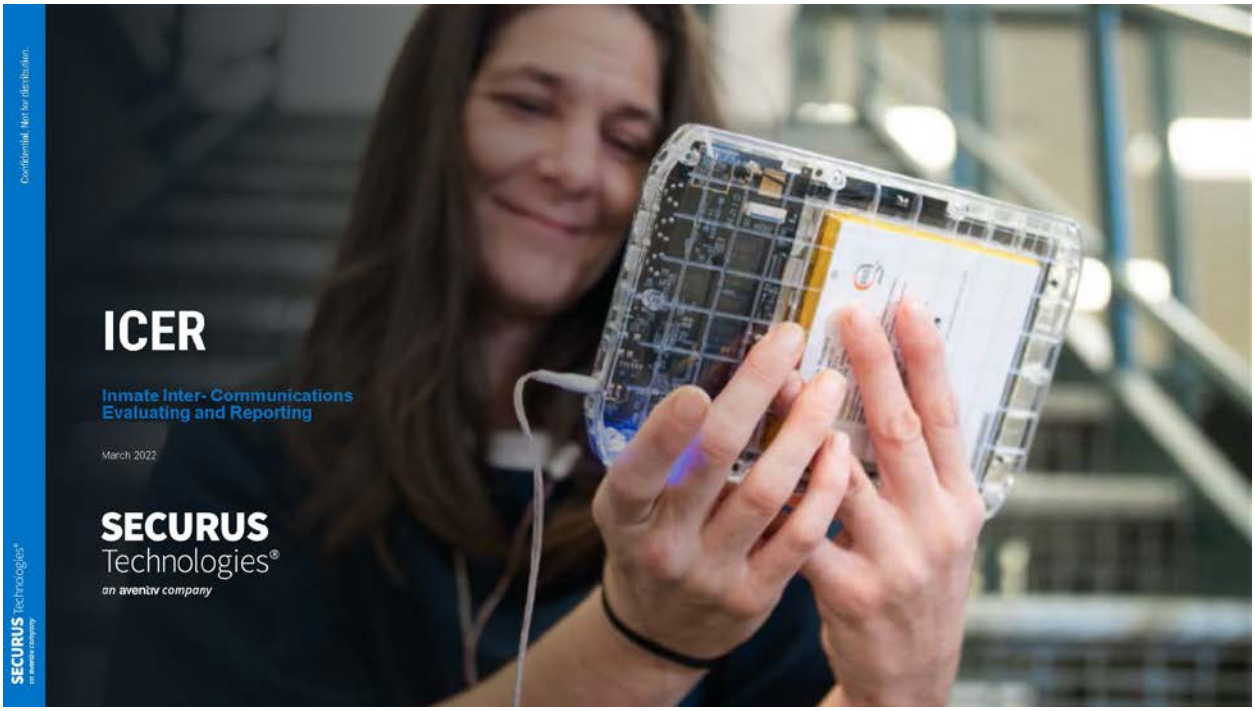
Securus – Corporate Structure – 1

Aventiv Corporate Structure as 12.31.2019



SECURUS Technologies

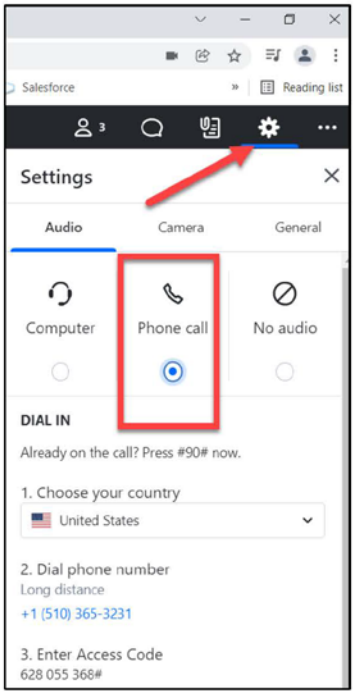
Securus Attachment No. 6:
Sample Training Documents


Confidential. Not for distribution.
ICER
Inmate Inter- Communications Evaluating and Reporting
March 2022
SECURUS Technologies®
an aventiv company
SECURUS Technologies®

Audio

PLEASE DIAL
Phone Number: 510-365-3332
ACCESS CODE: 403-361-180

If you cannot hear me, please dial in using these numbers



INTRODUCTION

David McTee
dmctee@securustechnologies.com
972-277-0364

Instructor
Customer Training and Product Adoption

Classroom Etiquette
Ask questions when you have them.




Confidential. Not for distribution.
SECURUS Technologies
Technical Support
FACILITY
technicalsupport@securustech.net
Friends and Family
Phone 800-844-6591
Phone – Spanish 866-561-6718
Customer_service@correctionalbillingservices.com
Web Access and Chat - www.securustech.net
SECURUS Technologies | 4

What is iCER?



Proactively monitors all inmate phone communications providing you with automatic alerts of inmate-to-inmate communications that might otherwise have gone undetected.

ICER ACCESS **LINK**

https://icer.icerconsortium.org/sign_in/



INCREDIBLY **EASY TO DO**



Confidential | Not for distribution.

SECURUS Technologies®
an Aventiv company

HOW ARE CALLS **IDENTIFIED?**

ICER looks for calls that overlap or occur simultaneously and listens for Call



Analyzes Using:
Voice Matching Technology



Reports Events:
Incident Details

iCER Event Report
Event Identified on : Apr 06, 2015
02:09 pm (EDT)

Inmate	London Daniels	James Jones
Agency	Securus DOC	Securus DOC
Site	Securus TX	Securus GA
Inmate ID	3648	3484
Called Number	12673241602	17188022256
Station Name	87	88
Call ID	7645333659	7645369156
Call Start Time	Apr 05, 2015 02:14 pm (EDT)	Apr 05, 2015 05:36 pm (EDT)
Time into Recording (H:M:S)	01m:33s (153 sec)	01m:29s (89 sec)
Duration of Event (H:M:S)	03m:38s (218 sec)	03m:38s (218 sec)

CALL SIGNATURE TECHNOLOGY

The Administrator would then access **SCP** to listen to the call.



The Administrator can also use **Investigator PRO** to listen to the call.



- Multiple features for investigators
- Attach notes to specific areas of a call
- Identify 3-way and Inmate-to-inmate calls

NGSCP IPRO

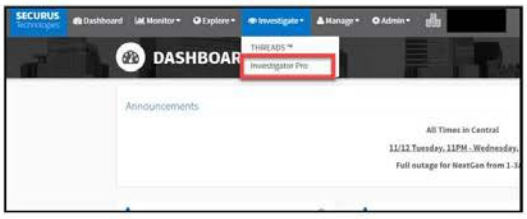
Access and Navigation

Accessing IPRO

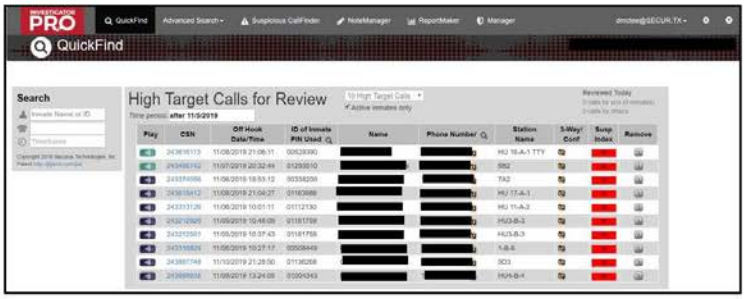
1. Log in to **NGSCP**



2. The NGSCP main screen displays. Click the **INVESTIGATE** dropdown and select **Investigator Pro**



The Main Screen



Menu Bar

The menu bar consists of the following:

QuickFind

Clicking the QUICKFIND tab will return you to the IPRO main screen.

ADVANCED SEARCHES

Advanced Searches offers three ways to search for calls:

1. Voice Search – allows a user to search for all calls where an incarcerated individual's voice print was identified – regardless of the PIN number used.
2. Call Finder – provides a wide variety of methods to search for calls.
3. MyCall Review – allows a user to search for all calls they have listened to

SUSPICIOUS CALL FINDER

The Suspicious Call Finder will point you in the direction of identified suspicious calls. Can find all of the suspicious calls here – where incarcerated individual voices differ from the PIN used, or where 3-way calls are likely to have been made.

NOTE MANAGER

The Note Manager is used to filter all the various types of notes that you can attach to each call.

REPORT MAKER

A user can setup different types of reports to expose patterns of ITS abuse and more.

MANAGER

The Command Staff can view the productivity of the investigators.

SETTINGS

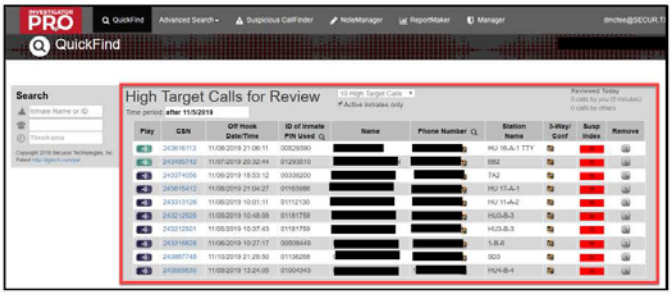
Assigning rights and roles to staff.

SEARCH



QuickFind provides instant access to all call activity detected in the system based on searches using any combination of Name/ID, telephone number and date range. It can also provide leads to telephone calls of interest.

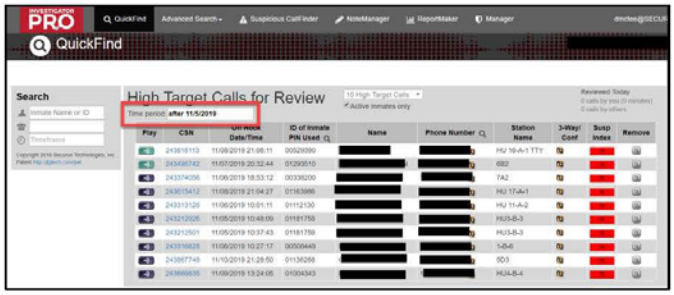
High Target Calls for Review



The High Target Calls for Review is the largest part of the home screen. It is here that IPRO displays calls that have been identified as being suspicious in nature either by identifying PIN Theft, 3-way calls, or Inmate-to-Inmate calls. Each of these calls will display on this home page.

Time Period

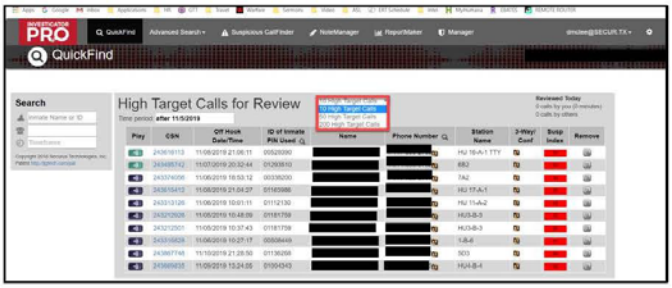
The Time Period is defaulted to 7 days in the past. Calls identified there are displayed. You can modify the time period by placing your cursor in the date field.



Performing this action displays a dialog box where the user can modify the date(s) to display on the home page.

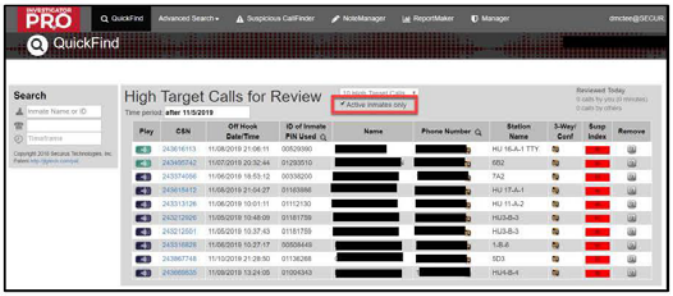


Modify Number of Calls Displayed



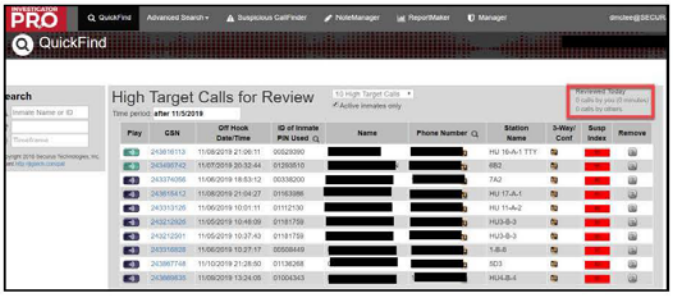
The default number of calls to display is 10. By clicking the drop-down arrow, the user can change that number to either 50, or 200.

Active Inmates



The system, by default, displays Active Inmates on the home screen. If the user's agency deactivates an Incarcerated individual's account upon release and they need to review that person's calls the user can deselect this checkbox and display not only active, but inactive incarcerated individuals at the same time.

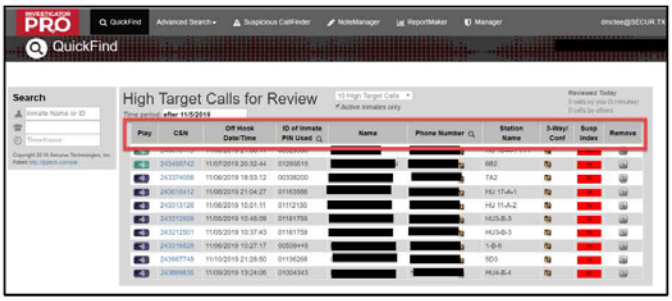
Review Today



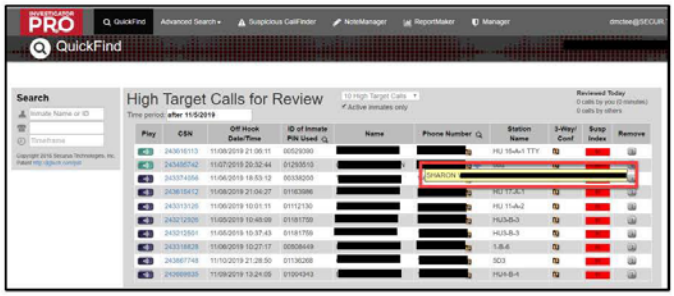
The Reviewed Today section displays how many calls the user has reviewed to as well as the number of calls others have reviewed.

Column Headings

The column headings provide a method of analyzing and identifying the individual calls that have been displayed.



- **Play**
  - Can left click on the speaker and hear the call
- **CSN** – Call Sequence Number
  - Call Sequence Number
  - Each call gets an auto-assigned number when placed
  - Can click the number to activate the Suspicious Call Finder
- **Off Hook Date/Time**
  - The time and date the call was placed
- **ID of Inmate PIN Used**
  - The Account Number and PIN Number of the incarcerated individual who's PIN Number is being used.
- **Name**
  - The name of the Incarcerated individual the PIN belongs to
- **Phone number**
  - The number being called
  - If you hover over the number, you can view the Billing Name and Address (BNA)



- **Station Name**
  - The phone in the facility the Incarcerated individual used to make the call

- **3-Way**
  - If either a 3-way call or an Inmate-to-Inmate call was placed, you would see an identifying icon based on the type of call
  - 3-way -  - Would see a yellow dot identifying it as a 3-way call where an Incarcerated individual called an outside party who in turn called a 3rd party and combined the calls
  - Inmate-to-Inmate -  - An incarcerated individual initiated a call to an outside 3rd party while an Incarcerated individual at another facility also initiated a call to the same party who merged the calls.
- **Susp Index**
  - Hovering on this shows the Incarcerated individual that may actually be placing the call
  - The number in the red box shows the percentage of certainty in ID the caller
    - Starting at 80% the index starts turning Orange
    - As the number goes up it gets brighter and brighter until the high 80's
    - Never goes over 95%
- **Remove**
  - If find that the 3-way call shouldn't be there of the incarcerated individual is innocent in relation to a 3-way, you can remove the call from the list.

NGSCP IPRO

Notes and Categories

A typical call is approximately 10-15 minutes. The incarcerated individual knows that their calls are being monitored and typically will not say anything incriminating in the first part of the call – that may happen later. The Note/Category feature in IPRO provides the Investigator a way to highlight a clip of the call and add a note relating to the importance of that clip. Additionally, the note can be categorized to allow for ease of search and grouping of like calls.

You can have as many notes on a call as desired.

Add a Note

Make sure that Skip Pauses are deselected and Speed controls are normal.

A. Add the Note and Categories

1. Navigate to the portion of the call with actionable intelligence.
2. **LEFT CLICK** your mouse and drag over the segment of the call you want to annotate.

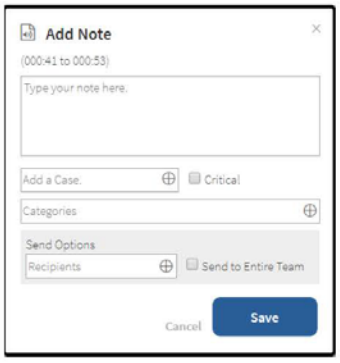


3. Click the **Add Clip Note** link.

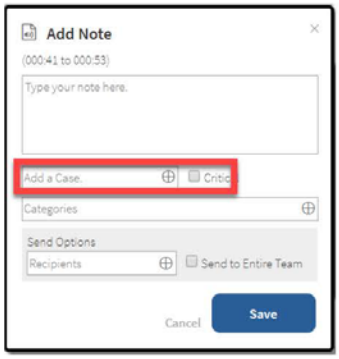


   a. Note you can also simply **Save the Clip as a .mp3 File**.

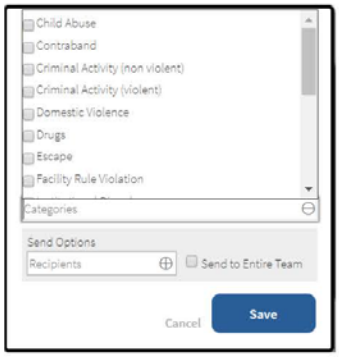
4. The **Add Note** dialog box displays. The cursor is in the free text field. Enter any note or comment relative to the call segment.



5. If desired, you can **Add a Case** number to the note for search and tracking functionality.

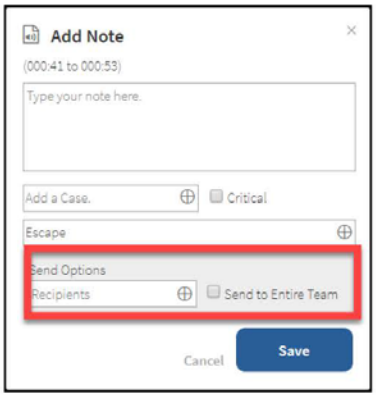


6. Click the **Categories** button to categorize the call segment. Click the desired category or categories that best describe the content of the call segment.

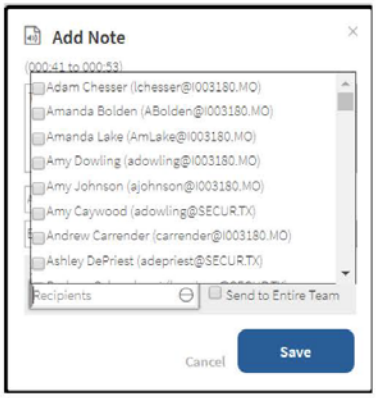


B. Send the Note to other Investigators

1. Click the **Send options** box. Here, you can pick specific personnel or the entire team to send a note to.



2. To send it to a specific Investigator, click in the **Recipients** box and select the person(s) to send the note to. NOTE: this is NOT an email, the recipient will see the note the next time they access IPRO.



3. Click **Save.**

NOTE: Once a note is sent, it is now a permanent part of the call and cannot be deleted or modified. The investigator(s) who receive the note can annotate it as the investigation progresses, but it cannot be deleted.

C. Delete an Unsent Note

1. An unsent note can be deleted if done so within 24 hours of creation.
2. Click the note icon on the call bar.



3. An edit menu displays. Click **Delete**.



4. A confirmation screen displays. Click **Delete**.



5. The note is deleted.

IPRO User Guide:



IPRO USER GUIDE 5.3.pdf

Securus Attachment No. 7:

Sample Quarterly Performance Report


A Securus Technologies Company
Colorado DOC – Money, Mail, Release Card Services
Quarterly Review
December 16, 2021

AGENDA

- Introductions
- Product Overview
- Focus on Improvements
- Questions/Comments/Concerns


INTRODUCTIONS

Michele Paige
Senior Account Manager
Securus Technologies, Inc.

Amy Hewitt
Vice President
DOC Account Management
Securus Technologies, Inc.

Armando (Eddie) Valeriano
Director, DOC Account Management
Securus Technologies, Inc.

Delorus Rose
Regional Client Manager
Securus Technologies, Inc.

Tonya Whitney
Inmate Bank/Cashier Manager
CTCF Business Office
Colorado Department of Corrections

Glenna Phillips
Accountant I, Cashier's Office
Colorado Department of Corrections

Kristina Ireland
CCi Canteen Services/Canteen Manager
Colorado Correctional Industries

A Securus Technologies Company


PRODUCT OVERVIEW

A Securus Technologies Company

Money Transfers | January 2021 to November 2021





Money Transfers		
Date	Transfers	Amount Transferred
Jan-21	14,641	$1,200,106.97
Feb-21	14,009	$1,174,263.64
Mar-21	19,154	$1,883,284.22
Apr-21	16,192	$1,583,508.18
May-21	13,758	$1,294,146.55
Jun-21	14,198	$1,340,711.73
Jul-21	15,168	$1,421,761.22
Aug-21	15,434	$1,400,513.51
Sep-21	14,607	$1,323,774.89
Oct-21	15,135	$1,391,779.72
Nov-21	14,147	$1,458,166.25
Grand Total	166,443	$11,639,480.02

A Securus Technologies Company

Release Cards| January 2021 to November 2021





Release Cards		
Month	**# Cards**	**Activation Totals**
Jan-21	545	$84,384.59
Feb-21	547	$101,972.96
Mar-21	519	$112,731.32
Apr-21	614	$218,905.11
May-21	497	$208,927.96
Jun-21	436	$151,605.39
Jul-21	466	$130,208.54
Aug-21	460	$129,279.64
Sep-21	556	$159,720.86
Oct-21	442	$138,432.58
Nov-21	445	$145,692.25
Banking Total	**5527**	**$1,581,861.20**

Mail| January 2021 to November 2021

Month	Mail			
	Customer Snap 'n Send	Customer Emails	Total Customer Mail	Prepaid Email Replies
Jan-21	41,293	28,224	69,517	25
Feb-21	38,159	26,396	64,555	25
Mar-21	49,685	30,420	80,105	20
Apr-21	52,871	30,811	83,682	28
May-21	55,745	30,050	85,795	24
Jun-21	56,560	30,608	87,168	14
Jul-21	64,454	31,483	95,937	25
Aug-21	65,566	33,382	98,948	24
Sep-21	60,706	31,530	92,236	26
Oct-21	62,923	30,344	93,267	32
Nov-21	65,071	36,967	102,038	35
Totals	613,033	340,215	953,248	278




FOCUS ON IMPROVEMENTS

Money Transfer

Q1 & Q2 2022

- Improvements to JPay.com (User Experience)
- AWS Platform Creation (Minimizes downtime)
- Money Transfer Batch Processing Improvement (Frequency/Monitoring)
- Legacy Kiosk
  - Camera Capabilities (Contract dependent)
  - Receipt Paper Override (Prevents downtime)
  - Cash Velocity (AWL Prevention)
- Cash Operations – Pick-up Notification system (Prevents downtime, cost efficiency)

Q3 2022

- New Money Kiosk Platform (NextGen Kiosk)
  - Improved KYC
    - ID Scanner
    - Camera Enabled
    - EMV Credit/Debit
  - Cash Aggregation for compliance

Mail

We will be launching a new mail product in 2022; Securus text connect will be available in Q1 for mass deployment.

Release Cards

- Release Cards for previously incarcerated and work release programs.
- Previously incarcerated individuals receive remaining trust account and gate money (if applicable) on their card at the time of release. Cards are available immediately for purchases and ATM withdrawals.
- Work release individuals still incarcerated use the card for daily expenses while out of the facility.
- Paper check available at anytime for remaining balance on the card 24/7/365 Product Support (IVR and Live Operator).
- Cardholder web portal (manage account) Upgrade to a personalized card at anytime (fees apply).
- 16 Department of Corrections and Agencies use our release card services in the USA (2021).
- Approximately 150,000 cards issued per year.
- Integrated within the JPay (Facility) web portal as a stand-alone product.
- A key product and service offering as part of our overall JPay Correctional Services and Payments.
- Product includes API integrations (if required) with Jail Management System.
- Cardholder fee reduction: One cardholder fee: $3.00 inactivity fee after 90 days - all other transactions are $0.00 (free) for the cardholder.
- Integration with Securus (Debit) for remaining funds in media and phone accounts.

Securus Attachment No. 8:
XL Terminal Technical Specifications

Video Visitation Terminal

Video visitation terminals shall be configured to meet the County's requirements.

The Securus Video Visitation terminal is a correctional-facility grade, tamper-proof steel enclosure. The hardware is wall mounted unit equipped with a built-in shatter resistant touch screen, a high-resolution video camera with integrated lighting, and tamper-proof, heavy molded plastic handset with an armor-reinforced cord for audio communication, and surge protection.

The proposed SVV terminals include, at a minimum, the following:



- A detention grade hardened steel enclosure
- One detention grade audio handset per terminal for the inmate, and two detention grade audio handsets per terminal for the public
- A shatter resistant LCD monitor with integrated camera
- Enclosures which prevent spills from entering
- Terminals that do not have any openings exposed to the user, including all wiring and ventilation holes
- Terminals without any external hinges
- Terminals are powered by 110 VAC, low voltage DC, or IEEE802.3at (PoE Plus).
- Rounded tops and corners
- Terminals with built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes and/or disables during all other functions
- Terminals that use standards based videoconferencing CODEC
- Terminals with multiple mounting methods: wall, table, pedastal or cart. All mounting options usestandard industry or better methods
- Options for powering the units on and off

Technical Specifications

• Light and ruggedized vandal-proof terminals (hardened steel): Best balance between weight and resistance
• Sealed: Dust and Liquids Resistant, spill-proof (accidental or deliberate).
• Assembly elements are hidden: No screws or hinges can be removed and used to manufacture

weapons. No doors/compartments that can be opened in the front or on the sides of the unit.
• Rounded edges that reduce the risks of accidental or intentional injuries.
• Abrasion and chemical resistant; the unit can be cleaned using commercial cleaning agents.
• Humidity and corrosion resistant
• Built-in LCD 15" with hardened shatter resistant touch screen
• HD camera, autofocus, (720p @ 30 fps)
• Sphone XL PoE has movable camera with a 2MP (1600x1200) resolution
• Optional hands free terminal with built-in HD video camera, Pan-Tilt-Zoom, 10x optical zoom, 4x digital zoom, 30fps
• Built-in LED lighting system
• Power ON LED indicator
• Magnetically activated pushbutton for on/off power
• Built-in heat sink mounted to the back for heat dissipation
• Built-in protection device against voltage variations
• Vandal-proof handset. Armored cable
• Standard non-proprietary computer components
• All electrical components comply with UL, CE and/or CSA
•System maintenance via wireless keyboard (Infra Red Access)
• Mother board: Micro/Mini ATX
• Intel Quad Core 2 GHz processor
• Memory: DDR3; RAM 4,096 MB (4 GB)
• Solid State (SSD) Hard drives to reducing moving components and potential failure points.• Network: Ethernet RJ-45 (CAT5/6)
• Power Options:
    AC: 110V 2 amps
    Low voltage DC: 24 V 8.33 amps
    Power over Ethernet: IEEE802.3at (PoE Plus).

Terminal Type	Height	Width	Depth	Weight
sPhone XL Single Handset	20.5	20	6	43
sPhone XL Dual Handset	20.5	23	6	44.6
sPhone XL Hands Free	23	17.375	6	49
sPhone XL Hands Free w/ PTZ camera	29.75	17.375	6	54.8
sPhone XL Single Handset PoE	20.5	20	4.25	38.6
sPhone XL Dual Handset PoE	20.5	23	4.25	40.2

- Manufactured according to ISO 9001:2008
- FCC Part 15 class A compliant
- sPhone XL PoE is CE compliant
- Touch Screen is UL-60950 and CSA 22.2 No. 60950 ball drop test compliant

Touchscreen meets IEC: 60529
• Touchscreen meets IP: 544
• Touchscreen meets NEMA: Type 12
• AC power Supply Meets Electrical Standard: CSA: 22.2• MTBF: 80,000 hours approx.

Securus Attachment No. 9:

W-9 Form

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give Form to the requester. Do not send to the IRS.

Print or type. See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

SCRS Acquisition Corporation

2 Business name/disregarded entity name, if different from above

Securus Technologies, LLC

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☑ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

4000 International Parkway

Requester's name and address (optional)

6 City, state, and ZIP code

Carrollton, TX 75007

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–			–				

or

Employer identification number

8	2	–	1	3	9	1	7	9	2

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ Mary Clear Date ▶ 12/09/2020

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

Cat. No. 10231X Form **W-9** (Rev. 10-2018)