DALLAS COUNTY

REQUEST FOR PROPOSAL FOR INMATE
PHONE, VIDEO VISITATION SERVICE AND INMATE
MULTI-FUNCTION KIOSK PROVIDER
RFP No. 2019-064-6828

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

An RFP Solution Prepared for:
Dallas County, Texas
Inmate Phone, Video Visitation Service and Multi-Function Kiosk Provider
RFP No. 2019-064-6828
October 21, 2019 at 2 PM

Presented to:
Abri-Gayle Sterlacci
Dallas County Purchasing Department
900 Jackson Street
Suite 680
Dallas, TX 75202
214.653.7763

Presented by:
Robert E. Pickens
Chief Executive Officer
Securus Technologies, Inc.
4000 International Parkway
Carrollton, Texas
75007

TABLE OF CONTENTS

A| COMPANY PROFILE

A. *COMPANY PROFILE*. **(20 Points) The following details of the Respondent's qualifications and experience to perform the services sought through this Request for Proposals shall be provided in narrative form and in sufficient detail that the County is able to judge IPS complexity and relevance. Specifically,**

> **Business/Corporate Experience**

1) **Provide a description of Respondent's corporate purpose and approach as it pertains to inmate telephone services or other services similar to those sought in this Request for Proposals.**

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

Our corporate purpose is to connect what matters.

Securus... Connecting What Matters.

Experience Matters.

Securus has been serving our correctional institutions for more than 30 years. For the last three decades, corrections industry constituents—facilities, inmates, and the family and friends of inmates—have relied on Securus Technologies and our predecessor organizations for communication solutions designed to fulfill their specialized needs.

1500+ DFW employees

470+ employees residing in Dallas County

We lead the way in inmate communications and investigative software. We have more than 190 patents issued and 100 patents pending. 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.

A new provider will need 6 to 12 months to be fully operational, creating inevitable lapses in service as well as potentially causing confusion and increasing costs for friends and family members. **By selecting Securus, the desired low-cost per minute rate that the County seeks can be implemented immediately.**

Securus has been proudly serving Dallas County for the last five years. Through our partnership with the County, we understand the internal operating procedures and corrections priorities of the jail and its administrators. Our knowledge and understanding of your facilities ensures accurate and efficient system maintenance.

> Securus will activate the phone application on the multi-function kiosks immediately to accommodate the increased phone usage from the reduced per-minute call cost.

As your partner, we have accomplished a lot in our tenure and are well positioned to add additional products and services to further improve the efficiencies of the jail and the opportunities for self-improvement for the inmates.

Over the next 5 years, as inmate needs evolve, we will work to provide solutions to meet those needs.

Some of our recent additions and accomplishments include:

- Developed custom applications, exclusively for Dallas County, to streamline the grievance process
- Increased wireless capacity when needed to match facility demand and growth
- Created custom reports for Dallas County to meet Jail Standard Grievance deadlines
- Increased video visit storage time from 30 days to 90 days
- Installed eight mobile kiosks for use in West Tower
- Installed six additional multi-function kiosks for use in Law Libraries
- Created training and refresher training videos for Parkland to assist with new hires and new assignments.
- Provide informational content and materials for inmates. See an example below:
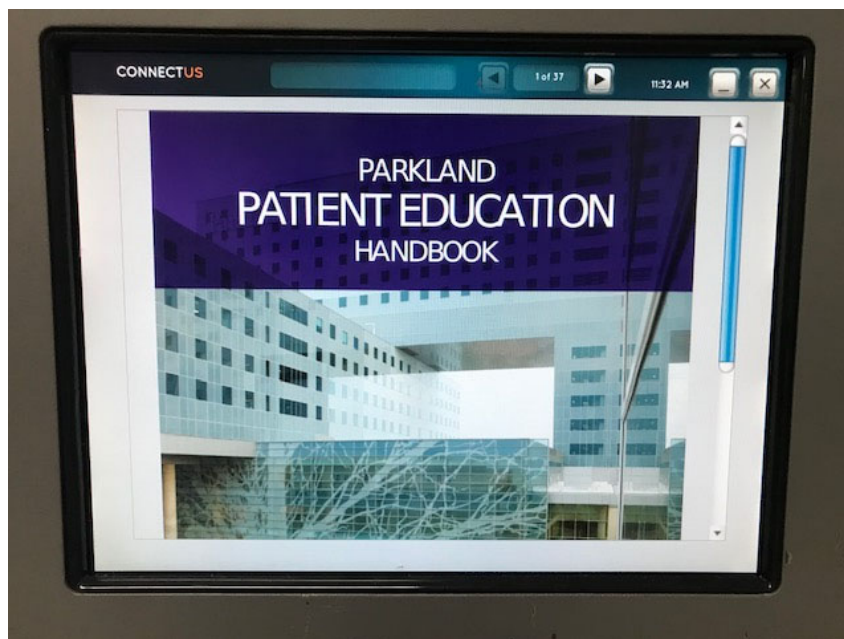
- Provided Data Analytics for Investigative Intelligence with our patented THREADS platform, Call Pattern Analysis and Covert Alert software
- Provided Monitoring & Investigative assistance regarding:
  - Escapes
  - Drug Activity
  - Human Trafficking
  - Threats towards Attorneys/officers
  - Staff misconduct
  - Hits on possible victims

And with another five years, we can accomplish even more!

Community Support Matters.

Inmates who stay connected with friends and family members are more likely to pursue opportunities for self-improvement and early release.

For a majority of inmates in America, imprisonment is not permanent. **Securus understands the importance of helping inmates stay connected with their communities outside of the jail environment.** As a result, Securus offers technology that benefits inmates as well as correctional facilities.

Securus is proud to be a member of the **North Texas Crime Commission** and **Texas Sheriff's Association**. In addition, we have a robust history of contributions to local charities through our employer-matched **United Way** contributions.

Safety Matters.

Public safety is best protected by reducing recidivism and successfully reintegrating inmates into mainstream society. As an inmate communications provider, Securus provides technology to **help inmates with education, literacy, job searches, legal research,** and, if desired, religious materials. Inmates who pursue self-improvement are inmates unlikely to return to criminal activity after release.

Tablets, we have learned, are particularly valuable to inmates. And Securus is unique among inmate communication providers in providing **FREE COMMUNITY TABLETS TO ALL INMATES** (with a low rental fee of *$5 a month* if the inmate chooses a personal tablet).

Inmates Matter.

To Securus, inmates are not just numbers. They are people who deserve the chance to be productive members of society. Our communication tools (such as our multi-function kiosks and **free community tablets**) give inmates opportunities to stay connected with loved ones and to improve their lives in preparation for their eventual release from incarceration.

The **SecureView Tablet** provides opportunities for incarcerated individuals to stay connected with their family, friends and the outside world as well as prepare for reentry into the community. In addition to email communications and media offerings, this digital tool allows offenders to work on personal rehabilitation with applications such as JobView, education, mental health and law library.

Please see a recent inmate graduate from a college program below. You can learn more about his story at https://securustechnologies.tech/ronnie/.

Access to these self-help applications is permitted free of charge to the incarcerated individual.

Jobview allows the incarcerated to create an action plan for reentry, and some even use it to find job opportunities for their family and friends. In the last 12 months, Jobview had an average of more than 135,000 monthly users, which is 31% higher than a year ago, and an average of 915,819 monthly jobs searches—up 74% from the previous year. **In August 2019, 930,259 job searches conducted, which is the largest number of job searches in a single month to date.**

Sample JobView Usage Report

Job Views By Job Category

Dallas County Jail TX-ConnectUs

June 2019

Category	monthly	YTD
Other	7,734	57,764
Transportation - Logistics	7,462	54,143
Construction - Trades	6,965	50,579
Restaurant - Food Service	5,708	30,406
Manufacturing - Operations	2,278	20,557
Janitorial - Housekeeping	1,702	11,767
Customer Service - Call Center	1,603	8,614
Retail	1,294	6,775
Sales	982	5,539
Healthcare - Medical	827	5,672
Automotive - Mechanic	822	9,069

JobView in Corrections News

Job Search: Offenders Gain a Jump on Employment

Studies have repeatedly shown that employment lowers the risk of rearrest for released individuals. One 2015 study from the Manhattan Institute revealed that "enhanced job-readiness training and job-search assistance helped reduce recidivism among non-violent ex-offenders by one-third, with rearrests dropping from 52% to 35%."

The tablet not only helps offenders stay connected to family and friends via email and media offerings, it allows offenders to work on personal rehabilitation with applications such as JobView, education, mental health and law library. Access to these self-help applications is permitted free of charge.

JobView allows the incarcerated to create an action plan for reentry, and some even use it to find job opportunities for their family and friends. Use of the app is up, the company reports. In the last 12 months, it had an average of 135,000-plus monthly users, which is 31% higher than a year ago, as well as an average of 915,819 monthly jobs searches, up 74% from the previous year. In August 930,259 job searches were conducted, which is the largest amount of job searches in a single month since its corrections launch in 2009.

The job search tool is now used in 30 states, assisting offenders in learning about types of available jobs and their requirements so they can gain skills while incarcerated and get a jump on securing a job soon after release.

VISIT US AT WWW.CORRECTIONSFORUM.NET

What We Do

Connecting What Matters®

Securus provides leading edge civil and criminal justice technology solutions that improve public safety and modernize the incarceration experience. Thousands of public safety, criminal justice, and corrections agencies rely on Securus for secure, simple and powerful technology solutions, which are always accessible and easy to use.

Securus is more than an inmate telephone provider. In addition, our offer to Dallas County:

1. **Communications Services** – phone, video, and messaging all are essential in allowing incarcerated individuals to maintain relationships with their loved ones. Past studies have shown a strong direct link between having a support network to return to and success after being released.
2. **Education and Job Training** – not only does a returning citizen need a support network, he or she needs access to employment to be successful. Securus is excited about the opportunities that technology can create for inmates in this area.
3. **Entertainment and Motivation** – many of our media services help an incarcerated individual cope in the correctional environment. This helps reduce the stress level for all and helps to channel behavior appropriately.
4. **Providing a Voice to the Incarcerated** – our grievance, sick call, assault reporting, and commissary ordering applications make sure the incarcerated individual's voice is heard and listened to!

Who We Are

Our Presence

Securus has the resources to install and operate large prison facility telecommunications systems. **Four of the top five mega county facilities in the United States have chosen Securus as their provider.** We serve multiple DOCs and other very large facilities that house thousands of inmates, including Arkansas DOC; Louisiana DOC; New Mexico DOC; Missouri DOC; Illinois DOC; Kentucky DOC; Pennsylvania DOC; Connecticut DOC; New York City DOC; Boston, Massachusetts; Denver, Colorado; Dallas, Texas; Seattle, Washington; and Portland, Oregon. We are uniquely equipped to handle any inmate population, and community population.
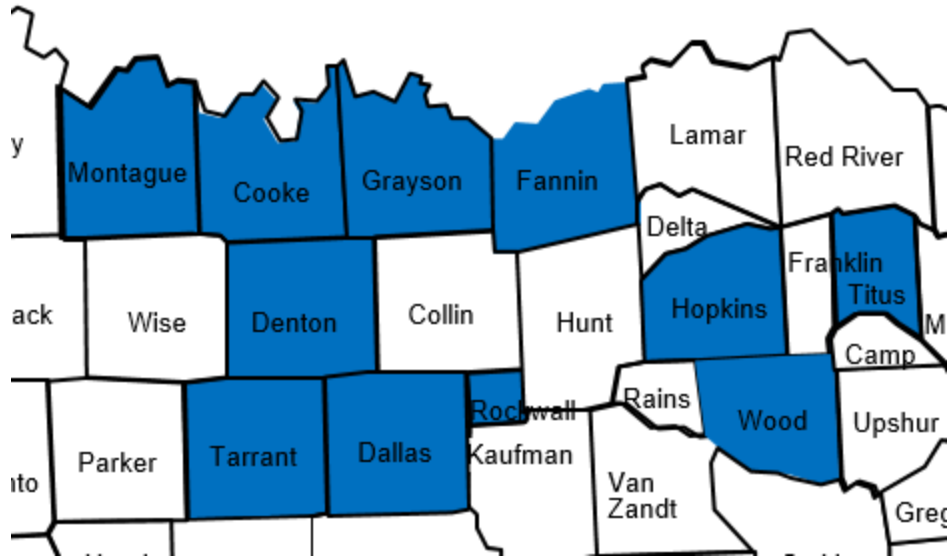
Locations served by Securus Technologies

Securus employs more than 1500 DFW-area residents—nearly 500 of whom live in Dallas county. We are a local company with national reach.

What We Offer Dallas County

Ten thousand free prepaid calling cards every year for staff distribution to indigent inmates.

Unlimited free calls in Intake and Booking area.

With your renewal, we will be **adding advanced technology enabling inmates to improve inmate lives during their stay, low cost to communicate with loved ones and the least impact on facility staff.** Securus has the **qualifications, experience, and community support** required to continue to provide the County with the most reliable, powerful, and efficient inmate communication solution available, both today and for years to come.

Over the past five years, Securus has partnered with and supported Dallas County with communication solutions that illustrate our commitment to the County and its inmates. We have added and enhanced our services at no cost to grow with the needs of the County.

For your consideration, we have included thorough detail outlining the functionality, technical compliance and our approach to performing at the highest level throughout the term of our partnership and beyond. Securus' inmate telephones, inmate kiosks and tablets are the strongest and most reliable units available and are designed specifically for the prison environment. **With our headquarters located only a few miles away and the dedicated on site staff in this offer we can assure you the service and support will be unmatched**.

Securus in the News

Recently there has been increased public discussion and media coverage about the economics and services offered by communications providers in jails and prisons, including Securus. We would like to address some of the commentary specifically directed towards Securus.

Securus understands the importance of accessible and secure communications between incarcerated individuals and their loved ones, which is why we have always been committed to following the directives of every state and county we serve in determining the best and most affordable methods of deploying and funding our services. Once each agency selects a funding option, we then work with them to offer the most affordable services possible while still covering the technology and monitoring needed to prevent misuse of communications tools and protect public safety.

All of these decisions are made with the full knowledge and sign-off of our agency partners. Securus works intimately with correctional partners to determine the costs and fees absorbed by the ultimate end users. Securus takes a neutral stance on the funding model chosen by any agency or community– our services and products function regardless of who pays.

The same is true of commissions. In the last few years Securus has made significant changes to the way we operate to make our services more affordable to incarcerated people and their families, including our willingness to bid on no-commission, cost-neutral plans, like Dallas County is currently seeking. In fact, we are committed to offering every agency a 0% commission option.   Securus was the first corrections telephone provider to negotiate and implement a taxpayer model for corrections telephone services in New York City. In fact, if any facility desires a change in rates or commissions, Securus will readily negotiate those changes.

Securus recognizes that each community has unique budgetary and technology needs, and we're proud to offer multiple rate options, numerous communication vehicles and a full suite of ancillary and investigative products to meet those distinctive needs. Ultimately, the balance between costs and services must be made by the agencies as demonstrated by the vendor selection criteria set in RFPs -- of which rates are only one consideration. Not only do we cover the expenses of maintaining our infrastructure and hardware, we also invest hundreds of millions of dollars in technological developments to enhance the quality of our communication services as well as constantly innovating our investigative tools that protect the incarcerated population, correctional officers and the general public, and to increase efficiencies in the correctional environment. In spite of those investments, we've been able to lower call rates by an average of 30% over the past three years.

Securus invests hundreds of millions of dollars in technological developments to enhance the quality of communication inmates' experience, to provide investigative tools that protect the incarcerated population, correctional officers and the general public, and to increase efficiencies in the correctional environment.

Securus wants to support and maintain familial and community connections for incarcerated individuals. We recognize the importance of contact with much needed support systems and we are committed to providing programs that reduce recidivism, such as no-cost education for the incarcerated.   And we welcome the opportunity to be a part of this process through low communication costs and increased contact between incarcerated individuals and their social support systems.

2)   Provide the Respondent's business plan and administrative structure. Describe the Respondent's organizational structure, depicting clear lines of authority.

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

Securus' business plan is to meet the following goals:

1.   Continue to work with local, regional and national entities and organizations that serve and/or are impacted by the corrections industry.

2.   Through meaningful engagement, understand the needs of all stakeholders in the jail environment: staff, inmates, friend and family, and the general public.

3.   Partner with minority-owned and/or small business entities to help the local economic communities around the facilities we serve.

4.   Continue to lead the way in developing technological solutions for industry stakeholders.

5.   Work with facilities, county officials, and advocates to understand the ever-changing and ever-evolving goals and priorities of correctional facilities around the United States.

6.   Help facilities combat crime through effective monitoring and investigation tools.

7.   Promote the safety of inmates, staff members and the general public through technological innovation and customized communication services.

8.   Use our technology to facilitate important connections between inmates sand their social support system.

9.   Support efforts to break the revolving door of probation and parole by offering meaningful opportunities for inmate self-improvement and self-enrichment

We meet these goals through our continued membership in corrections and public safety organizations, our participation in summits and conferences, the ongoing training and education of our staff, and through discussions and plans developed in concert with facilities and community organizations.

Specific examples of our execution of our business plan include membership in organizations like:

- North Texas Crime Commission
- Texas Sheriff's Association
- Association of Women Executives in Corrections
- National Sheriff's Association
- American Jail Association
- American Corrections Association

We also support (through donations and volunteering) organizations like the United Way, Feed My Starving Children, Keeping Families Connected, the Securus Foundation and the Women's Prison Association.

Finally, we are leading the way in fighting human trafficking with our **Guarded Exchange** data analytics and **preventing the introduction of harmful contraband with services like eMessaging and Digital Mail.**

Administrative Structure

Led by our experienced Senior Executive team outline below, Securus believes that we must provide world-class service to our three customers—the County, the inmates, and the Community.

Consistent with this belief is the ongoing, proactive development of our Texas-based Technical Support Center (TSC) for our law enforcement customers and Carrollton-based Securus Friends and Family Call Center (SFFCC) for support of the friends and family of inmates.

Company Management

Effective January 1, 2018, Mr. Robert E. ("Bob") Pickens became Securus' Chief Executive Officer. Previously, Mr. Pickens served in the positions of President, Chief Operating Officer, and Vice President of Marketing of Securus. He held these same positions at Eschelon Telecom, Inc., a Minneapolis, Minnesota telecommunications company where he and Mr. Richard A. ("Rick") Smith, the prior CEO of Securus, worked together for nine years before joining Securus in 2008. Mr. Pickens leads a team of highly talented group of executives who possess more than 210 years of combined telecommunications and/or inmate telecommunications experience. Mr. Smith continues to support Securus in the role of Senior Advisor to Securus' Board of Directors.

The company organization chart is on the following page.
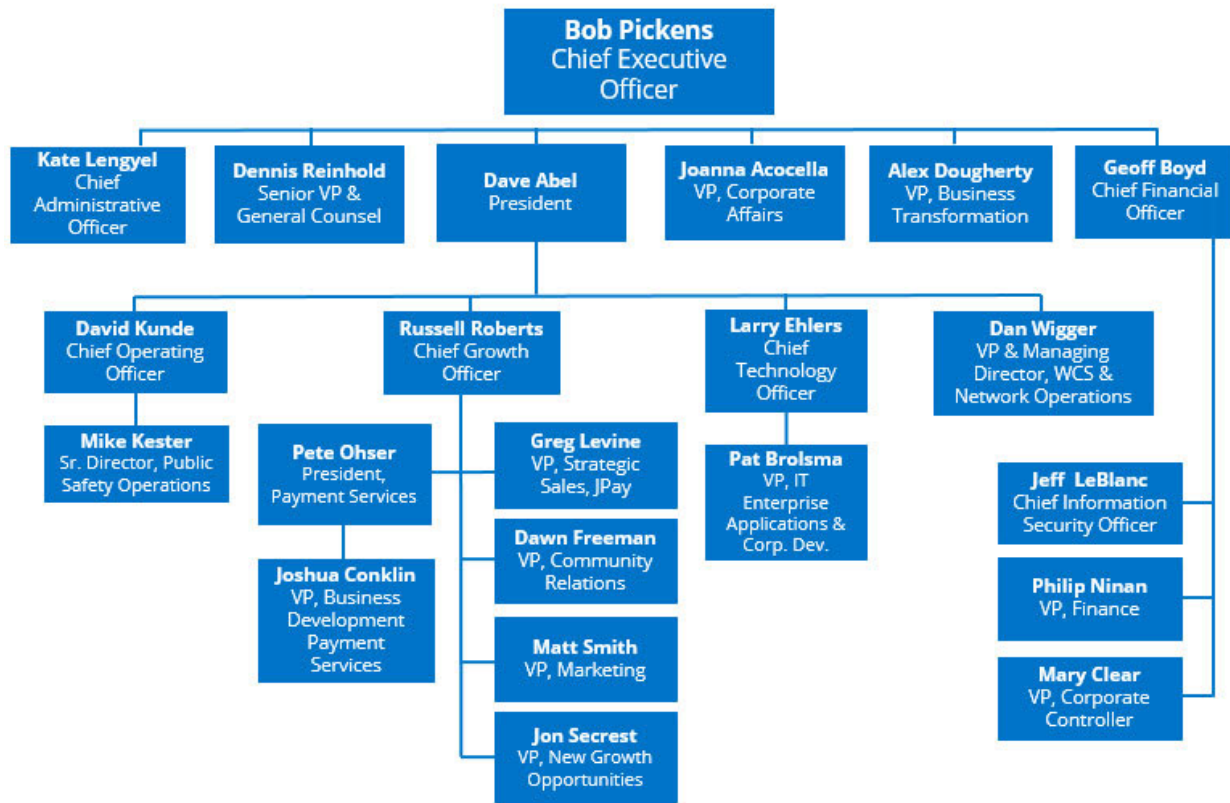
Securus' executive management team and biographies are below.

Robert E. Pickens, Chief Executive Officer

Robert (Bob) Pickens is the Chief Executive Officer of Securus Technologies, Inc. with more than 22 years of communications experience. He has responsibility for all corporate and field operating areas. Before joining Securus in September 2008, Mr. Pickens held multiple executive positions—including Chief Operating Officer—at Eschelon Telecom, Inc., a publicly traded (NASDAQ Exchange) $350 million revenue, 1,500 associate competitive local exchange carrier located in Minneapolis,

> CEO Bob Pickens was honored with a Gold Stevie® award for Executive of the Year at the 2018 International Business Awards

Minnesota. Mr. Pickens holds a Bachelor of Science degree in Business Administration from the University of Minnesota's Carlson School of Management.

Dave Abel, President

Dave Abel is the President of Securus Technologies, Inc. He has more than 27 years of public and private sector technology experience, with a concentration in criminal justice, law enforcement, national security and intelligence. Mr. Abel started a successful automation and artificial intelligence business, was an executive in the US and overseas with IBM, and was a partner at PricewaterhouseCoopers. At IBM, he was the General Manager of the US Public Sector with service revenue over $2 billion and a team of more

than 4,000 employees and contractors. Mr. Abel has a Bachelor's of Science in Business as a graduate of the McIntire School of Commerce at the University of Virginia.

Russell Roberts, Chief Growth Officer

Russell Roberts is Chief Growth Officer. He oversees Sales, Product Management, Customer Training, Marketing Strategies, and RFP teams. In this role, Mr. Roberts has the responsibility of Product Engagement and Marketing Strategies for all Securus Products.

Joshua E. Conklin, Vice President, Business Development, Payment Services

Joshua (Josh) Conklin is Vice President, Business Development, Payment Services at Securus Technologies, Inc. with more than 13 years of communications experience. 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.

David A. Kunde, Chief Operating Officer

David (Dave) Kunde has been on the executive team since August 2011. Mr. Kunde has overseen the deployment of numerous operational practices that have resulted in significant uptime improvements across all platforms at Securus. He has been a growth leader for our Video Visitation, IVR, and Wireless Containment lines of business. Mr. Kunde has more than 30 years of telecommunications industry experience and 20+ years working with members of the Securus executive team. Mr. Kunde has senior-level experience in building and managing national VOIP networks and has developed and launched highly successful services such as IPTV television during his career.

3) **Identify no less than five (5) or more than ten (10) current and/or past (within five (5) years) contracts of at least half the size of the Dallas County operations for the provision of services similar to those identified in this RFP that fully demonstrate/illustrate that the Respondent has the experience and ability to completely and timely perform all services contemplated by this RFP. This information should include the number of inmate phones covered by the contract and must reflect at a minimum 450 phones or more to constitute qualification.**

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

Please see nine contracts listed below.

Customer #1

Facility Name	Travis County
Facility Location	3614 Bill Price Road, Del Valle TX 78617
Services Provided	Secure Call Platform, Inmate phones, Securus Video Visitation, Law Library, JobView, AIS (Automated Information Services), IPRO, Threads, ICER, Tablets
Number of Phones	500+
ADP	2,500

Customer #2

Facility Name	Gwinnett County, Georgia
Facility Location	2900 University Pkwy, Lawrenceville, GA 30043
Services Provided	Secure Call Platform, Securus Video Visitation, Threads, Prepaid Calling Cards, AIS (Automated Information Services), Investigator Pro – Continuous Voice Identification, National Cell Phone Forensics, Guarded Exchange Monitoring, ICER, JobView
Number of Phones	364
ADP	2,175

Customer #3

Facility Name	Fulton County, Georgia
Facility Location	185 Central Ave SW, Atlanta, GA 30303
Services Provided	Secure Call Platform, Securus Video Visitation, Threads, Inmate Debit, AIS (Automated Information Services), Investigator Pro –

	Continuous Voice Identification, National Cell Phone Forensics, Guarded Exchange Monitoring, ICER, JobView, Law Library
Number of Phones	394
ADP	2,800

Customer #4

Facility Name	San Diego County, CA
Facility Location	446 Alta Road, San Diego, CA 92158
Services Provided	Secure Call Platform, Securus Video Visitation, Investigator Pro, ICER, Threads
Number of Phones	830
ADP	7,642

Customer #5

Facility Name	Denver County, CO
Facility Location	490 W Colfax Ave, Denver, CO 80204
Services Provided	Secure Call Platform, Inmate Phones, Securus Video Visitation,
Number of Phones	153
ADP	2,200

Customer #6

Facility Name	Riverside County
Facility Location	1627 s. Hargrave St, Banning CA 92220
Services Provided	Secure Call Platform, Inmate Phones, ICER, Investigator Pro
Number of Phones	425
ADP	3800

Customer #7

Facility Name	Broward County, FL
Facility Location	555 SE 1st AVE, Ft. Lauderdale, FL 33301

Services Provided	Secure Call Platform, Inmate Phones, AIS Automated Information Services, Securus Video Visitation, ICER, Investigator Pro
Number of Phones	654
ADP	4,500

Customer #8

Facility Name	Georgia Department of Corrections
Facility Location	300 Patrol Road, Forsyth, Georgia 31029
Services Provided	Secure Call Platform, Inmate Phones, Investigator Pro, ICER, THREADS, GEX Call Monitoring, GEX Forensic LAB, Wireless Containment Services, Drone Detection, JPay Tablets, JPay Kiosks
Number of Phones	951
ADP	2215+

Customer #9

Facility Name	Tarrant County
Facility Location	100 N. Lamar Street, Fort Worth, TX 76196
Services Provided	Secure Call Platform, Inmate phones, Voice Biometrics
Number of Phones	376
ADP	4,100

Customer #10

Facility Name	Arkansas Department of Corrections
Facility Location	2403 E. Harding, Pine Bluff, AR 71601
Services Provided	Secure Call Platform, Inmate Phones, IPRO, ICER, THREADS, Video Visitation, Tablets
Number of Phones	900
ADP	17,000+

4) **Provide a narrative summary of contract performance in the above-identified contracts, including any major adverse findings.**

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

1.   Travis County has been a customer for over 15 years. Over the years, they have installed more and more of Securus products and services. We have an excellent working relationship with Travis.

2.   Gwinnett County Sheriff's Office has been a customer since 2013. Gwinnett has installed many Securus products and services including extensive investigative products. The investigative products are especially effective as we have a strong amount of customers in Georgia including the DOC. Using Threads and other tools the agencies are able to share information on inmates collaborating between agencies. We have an excellent partnership with Gwinnett County

3.   Fulton County Sheriff's Office has been a customer since 2012 and has installed most of the Securus' products and services. Fulton utilizes investigative tools, as well as many products serving the Friends/Family as well as inmates. AIS allows inmates to dial their PIN and retrieve information regarding charges, bail etc. JobView allows inmates to view jobs available if they are being released soon or for other family members. We have a great relationship with Fulton County.

4.   San Diego has been a customer since 2012. Along with Inmate Phones, Sn Diego is utilizing Securus Video Visitation and several of investigative products including Investigator Pro to identify every inmate on every call. We have a great relationship with San Diego County.

5.   The City and County of Denver have been a customer since 2013 and have recently expanded their services with Securus for another 5 years. It is with leading technology, great customer support, and a true understanding of the specific needs for the community of Denver, why Securus maintains a good partnership with the city and county.

6.   Securus has maintained a good partnership with Riverside County over that last 5 years and has provided technology that is helping to supplement important investigations. In the next coming years, we anticipate to add on more leading technology to help with inmate programs.

7.   Broward County has been a partner with Securus since 2002. During this time they have added Video Visitation, AIS, THREADS Data Analytics, and Investigator PRO among other solutions. Broward is the second largest agency in Florida and Securus partnered with BSO to build an offsite visitation center in 2016. We have an excellent relationship with Broward County.

8.   Georgia DOC has a heavy focus on investigations and security. The DOC relies on our voice identification technology and cell forensic labs to assist in investigations. They use our Wireless Communication services to disable contraband cell phones in their prisons. They also use our drone detection software to eliminate contraband from being

dropped in the yards and we monitor approximately 5% of the inmate phone calls and report suspicious activity to the investigators. We have a great partnership with the George DOC.

9.   Tarrant County has been a Securus customer since 1996. During this partnership, we have provided excellent service maintaining the inmate phones. Since they do not currently record inmate calls we do not have investigative technology enabled at this time. We have an excellent relationship with Tarrant County.

10.   Arkansas DOC has implemented Securus Video Visitation to ensure family and friends are able to visit from anywhere at convenient times and staff does not have to escort for every visit. Tablets are available for inmates to provide a positive and productive stay as well as a safety tool for the staff. Threads, IPRO and ICER are utilized to assist investigators with the latest investigative technology for safety in their prisons.

5)   Provide the name and current telephone number and address for the specified contract manager for each identified contract.

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

Customer #1

Facility Name	Travis County, Texas
Facility Address	3614 Bill Price Road, Del Valle TX 78617
Contact Name	Lt. Laura Town
Contact Phone Number	512-854-5351

Customer #2

Facility Name	Gwinnett County, Georgia
Facility Address	2900 University Pkwy, Lawrenceville, GA 30043
Contact Name	Silvia Black, IT Director
Contact Phone Number	770-822-3839

Customer #3

Facility Name	Fulton County, Georgia
Facility Address	185 Central Ave SW, Atlanta, GA 30303
Contact Name	Colonel Mark Adger
Contact Phone Number	404-613-2065

Customer #4

Facility Name	San Diego County
Facility Address	446 Alta Road, San Diego, CA 92158
Contact Name	Captain Alan Kneeshaw
Contact Phone Number	619-615-2501

Customer #5

Facility Name	Denver County CO
Facility Address	490 W Colfax Ave, Denver, CO 80204
Contact Name	Diane Muscianisi, Director of Technology Unit
Contact Phone Number	720-865-4108

Customer #6

Facility Name	Riverside County
Facility Address	1627 s. Hargrave St, Banning CA 92220
Contact Name	Rosa Lazenby, Inmate Services Manager
Contact Phone Number	951-922-7313

Customer #7

Facility Name	Broward County, FL
Facility Address	555 SE 1st AVE, Ft. Lauderdale, FL 33301
Contact Name	Kathleen Casey Kathleen_casey@sheriff.org
Contact Phone Number	Office # (954) 831-0225

Customer #8

Facility Name	Georgia Department of Corrections
Facility Address	300 Patrol Road, Forsyth, Georgia 31029
Contact Name	Tammy Sexton
Contact Phone Number	478-992-6327

Customer #9

Facility Name	Tarrant County Corrections Center
Facility Address	100 N. Lamar St., Fort Worth, TX 76196
Contact Name	Executive Chief Randy Cundiff
Contact Phone Number	817-805-3914

Customer #10

Facility Name	Arkansas Department of Corrections
Facility Address	2403 E. Harding, Pine Bluff, AR 71601
Contact Name	Rhonda Patterson
Contact Phone Number	870-850-8521

6)   **Provide a summary of any exemplary or qualitative findings, recommendations, or other validations, demonstrating operational experience. (i.e., specialized accreditations, grant awards, etc.).**

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

Securus is an accredited BBB company with an A+ rating. "Accredited" means the BBB has determined that Securus meets the BBB's strict accreditation standards, which include a commitment to make a good faith effort to resolve any consumer complaints. BBB accreditation also means the BBB monitors Securus for continued compliance and for support of BBB services to the public. Securus' A+ rating is based on information BBB has obtained about Securus, including complaints received from the public. It is the highest out of 13 possible BBB ratings and represents the BBB's opinion of how Securus interacts with our customers.

Giving Back

Correctional Officer Memorial Fund

Securus supports the communities we serve. Our team members across the country improve the places they live by participating in multiple philanthropic organizations and giving countless volunteer hours each year. As a company, Securus demonstrates our commitment to the community through two significant initiatives.

Securus founded and fully funds a nationwide correctional officer memorial fund. This fund provides financial assistance to the families of corrections officers who have fallen in the line of duty at any Securus customer facility.

The company provides one year's salary as a token of gratitude, honoring the sacrifice corrections officers make protecting the communities they serve.

Community Betterment

Nationally, Securus is aligned with Dallas County and values good corporate citizenship, affirmative action, and environmental preservation policies. Securus has conducted annual giving campaigns for the United Way since 2008. We earned recognition for the New Campaign of the Year in 2008, the Largest Increased Campaign in 2009, and in 2015 and again in 2016, achieved a number of record United Way contribution levels, including:
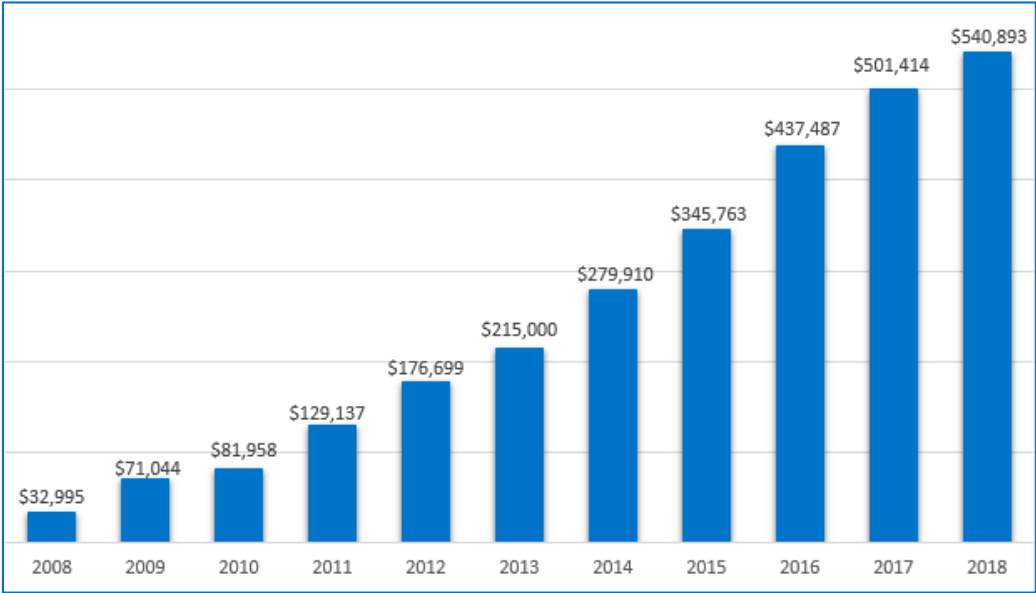
Securus was recently awarded the Silver Award for Corporate Social Responsibility Program of the Year at the 2017 Golden Bridge Awards.

We take our social and corporate responsibility seriously and this award demonstrates our commitment to improving the lives of those in our communities.

- Highest level of annual Securus Associates contributions
- Greatest number of Leadership Givers ($1,000 per year or more)
- Greatest percent increase above annual goal
- Greatest number of Associates giving

Securus has partnered with the United Way for 10 years and has contributed more than $2.275 million to this well-respected charity. Securus' record-breaking campaign growth is a testament to the shared commitment of the company's leadership and associates to making our communities a better place to live, work and raise families.

Employees designated their donations to 250 of their favorite United Way Agencies and local initiatives across the country. More than 96 percent of the management team contributed in 2017 with 291 associates giving at the United Way Leadership Level. This was 16 percent higher than last year's Leadership participation level.

Securus' charitable giving campaign harnesses its people, expertise, and partnerships to create a positive impact in the communities we serve. Securus employees are encouraged to tap into their passions and support the charities of their choice. In 2017, associates supported dozens of charitable organizations across the country, from donating to United Way to helping hurricane ravaged communities to donating to local toy drives. Year after year, Securus associates continue to donate in record numbers.

Associate Charitable Contributions

Year	Amount
2008	$32,995
2009	$71,044
2010	$81,958
2011	$129,137
2012	$176,699
2013	$215,000
2014	$279,910
2015	$345,763
2016	$437,487
2017	$501,414
2018	$540,893

Award Winning Customer Service

Securus prides itself on the quality of its customer service and in 2018 was the recipient of multiple Gold Stevie Awards for Sales and Customer Service, following on similar successes in 2017. The Gold Stevie Awards is considered the world's top honors in business recognizing excellence in customer service, contact centers, business development, and sales professionals.

Stevie Awards Securus received in 2018

- **Gold**—Customer Service Complaints Team of the Year (Corporate Escalations)
- **Silver**—Customer Service Professional of the Year (Customer Service Manager)
- **Bronze**—Front-Line Customer Service Team (Video Visitation Team)

In 2018, Securus, its executives, and leading salespeople received nine awards from the SVUS Awards®. The coveted annual CEO World Awards, Customer Sales and Services Awards, and Women in Business & the Professionals World Awards program encompasses the world's best in leadership, innovation, organizational performance, new products and services, and milestones from major industries across the world.

CEO World Awards (Gold) received in 2018:

- **CEO Achievement of the Year**—Robert Pickens, CEO
- **Executive of the Year**—Director of Support Services

Customer Sales and Service Awards (Gold) received in 2018:

- **Customer Service Professional of the Year**—Client Manager
- **Champion of the Year**—Manager of Technical Support
- **Most Valuable Professional of the Year**—Manager of Support Services

Women in Business & the Professions World Awards received in 2018:

- **Female Employee of the Year (Gold)** —Field Service Technician
- **Maverick of the Year (Gold)**—Field Services Manager
- **Female Executive of the Year (Bronze)**—Sr. Director Technical Support & Client Management
- **Female Professional of the Year (Bronze)**—Customer Service Supervisor

Patents

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 innovation.

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 140 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.

7) **Provide information indicating whether the Respondent intends to provide 100% of services directly or intends to utilize subcontractors and if so, provide identification of all subcontractors delivering service delivery. Include a statement indicating the percentage of work to be completed by the Respondent and each subcontractor as measured by percentage of the total contract.**

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

Securus is capable of performing 100 percent of the required work without any support from subcontractors. However, to support the local community and the values of Dallas County, we are committed to using a SBE-certified subcontractor to perform onsite technical services when possible.

> **Business/Corporate Entity Details (include the following information on Respondent and each subcontractor (if subcontracting is indicated);**

1)   Date established

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

Securus Technologies, Inc., f/k/a Evercom Systems, Inc., was incorporated in the state of Delaware on August 22, 1997.

2)   Ownership (public company, partnership, subsidiary, etc.)

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

Securus is a private corporation.

3)   Primary type of Business

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

Securus provides communication and investigative services to more than 3,450 public safety, law enforcement and correctional institutions nationwide, including 14 state departments of corrections. We connect 380 million inmate calls every year, serve more than 1.2 million inmates every year and maintain an A+ BBB rating.

4)   Total number of employees

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

Securus employs 1589 employees—nearly 500 of whom live in Dallas County.

5)   Indication of type of business (i.e. corporation, sole proprietorship, partnership). If the respondent is a corporation, indicate the date and state of incorporation. State the length of time the respondent has been in the inmate phone business.

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

Securus Technologies, Inc. f/k/a Evercom Systems, Inc., was incorporated in the state of Delaware on August 22, 1997. Over the next several years after incorporation, the company acquired the assets of several other inmate telephone service providers, all of which had been in the inmate telephone service business between 5 to 12 years. Securus has been operating under its current name since August 2, 2010.

Securus Technologies, Inc. ("Securus") has served the corrections industry for more than 30 years.

6) **Provide list of all officers of the firm indicating the percentages of ownership of each officer and the name of the Board of Directors, if applicable.**

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

Please see our Officers and Board of Directors identified on the following page. Please note that we consider this information proprietary and confidential, and respectfully request that the information not be disclosed to third parties.

Securus Technologies, Inc.
Officers and Board of Directors

Officers	Title	Address
Robert E. Pickens	Chief Executive Officer	4000 International Parkway, Carrollton, Texas 75007
Richard A. Smith	Senior Advisor – Board of Directors	4000 International Parkway, Carrollton, Texas 75007
Geoffrey Boyd	Chief Financial Officer	4000 International Parkway, Carrollton, Texas 75007
Dennis J. Reinhold	Senior Vice President, General Counsel and Secretary	4000 International Parkway, Carrollton, Texas 75007

Directors	Address
Eva M. Kalawski	Platinum Equity 360 North Crescent Drive South Building, Beverly Hills, CA 90210
Mary Ann Sigler	Platinum Equity 360 North Crescent Drive South Building, Beverly Hills, CA 90210

Securus ownership information is provided on a chart on the following page. This information is proprietary and confidential and we respectfully request that it not be shared with third parties.
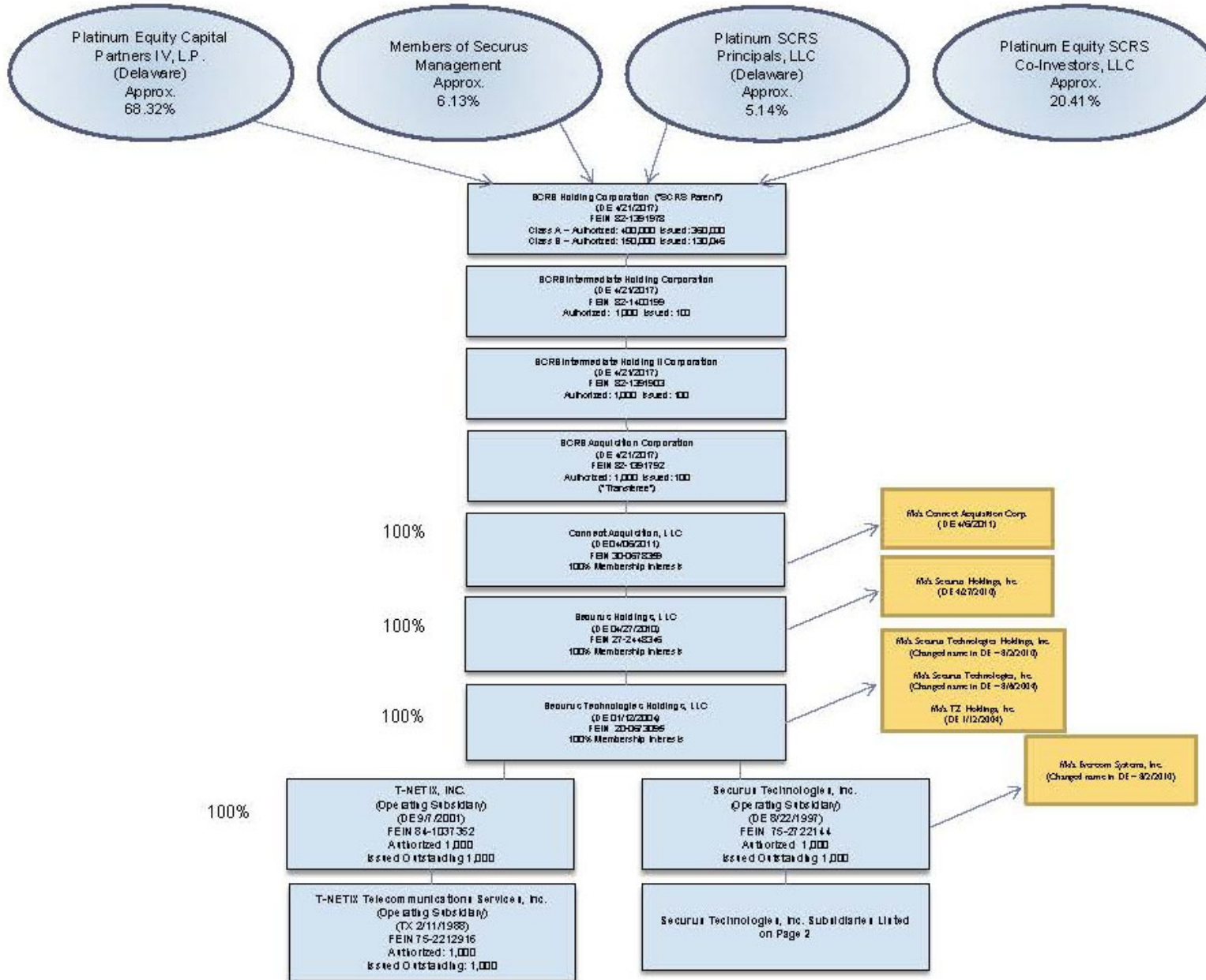
7) **Provide the Federal tax identification number or social security number, as applicable to the legal entity that will be performing as the Primary Contractor under any resulting Contract.**

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

Securus' tax ID number is 75-2722144.

➢ **Organizational Chart**

1) **Respondent shall provide an organization chart outlining the hierarchy of key contract personnel assigned under this RFP.**

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

We have provided our organizational chart of key assigned personnel below.
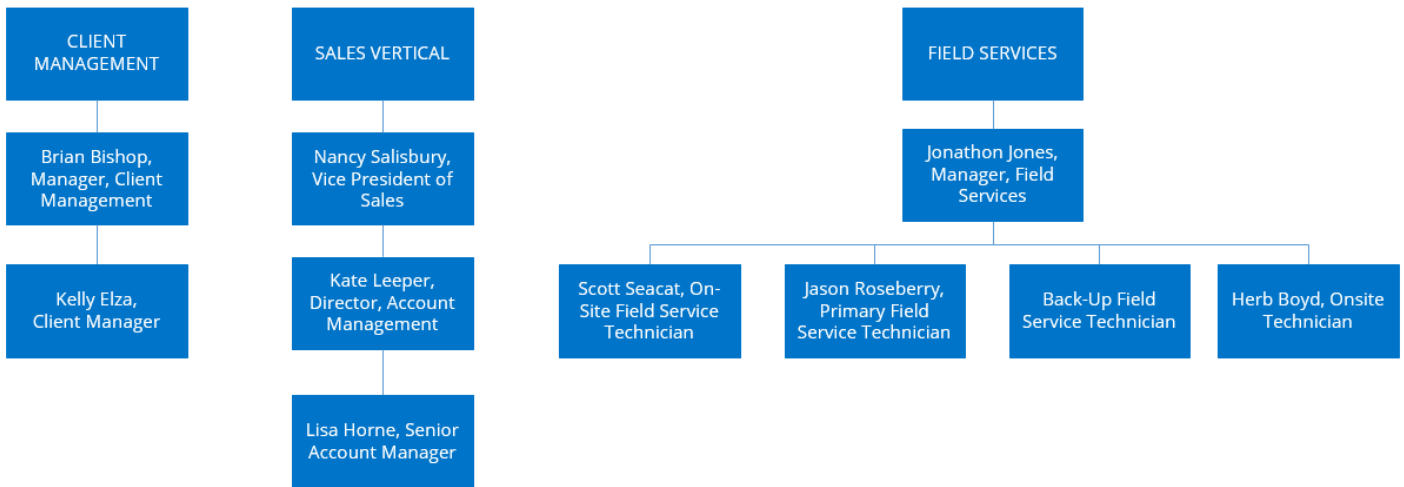
2) **Provide biographies or curriculum vitae and qualifications of the IPS System Administrator to be assigned to the contract. Such information shall demonstrate the required experience in provision of telephone services in a correctional or law enforcement environment. In addition, provide general job descriptions outlining the duties and responsibilities of the Field Repair/Site Technician and Service Representatives to be utilized to perform service tasks. Job descriptions should include specific job functions and minimum qualifications of the identified position(s).**

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

> Most of our field service technicians are located less than 30 miles from the Dallas County Jail.

The Securus Field Services organization is one of the largest in the inmate phone system industry. Our team consists of approximately 150 Field Service Technicians (FSTs) located throughout the United States. Our field services team installs and maintains inmate phone systems for approximately 2,600 facilities and a million inmates in 47 states. **The Securus Field Operations Director manages three Regional Service Managers who possess more than 60 years of combined field service experience.**

The local Securus service and account management team will provide support 24 hours per day, seven days per week, and 365 days per year (24x7x365).

Jonathon Jones, Field Service Manager

Jonathon has more than twenty years of project and field service management experience and has been with Securus for the last 5 years. He is responsible for making sure that field technicians achieve their goal of maintaining and fixing equipment in a timely and professional manner.

For your facilities, Jonathon will:

- Conduct remote visits via phone bimonthly. Based on information obtained from call, a trouble ticket may be opened
- Work with the account team quarterly to evaluate contract progress with the County
- Provide the facility with applicable site information that assists them based on the account profile
- Monitor ticket traffic
- Resolve escalation issues, as needed.

Each field service manager possesses the skills required to perform the duties of the field service technician and can provide additional or backup support as needed.

Field Service and Onsite Technicians

Dallas County will be assigned several on-site technicians and administrators.

Your onsite technicians will work with offsite field service technicians (FSTs) to ensure optimal performance of your inmate communication systems at all times. Our FSTs are required to follow a structured technical and management escalation process if they are unable to isolate the problem within four hours. Our integrated support model keeps our centralized technical support team engaged through problem resolution. FSTs and the technical support team have direct access to product and development engineers, enabling them to expedite repairs and minimize customer downtime.

Securus' Field Services Technicians receive:

- training on all of the Securus equipment and products

- training on Securus platforms at our training labs in Carrollton, Texas.

- annual training on OSHA requirements, ESD, and safety in correction facilities.

Securus field service technicians maintain a working level of spare parts for minor repairs consisting of telephone sets, handsets, dials, and replacement circuit boards, either on-site or in their truck. If a technician does not have a required part, Securus will drop-ship the item to the site. Securus will ship counter-to-counter on the same day in critical situations.

Scott Seacat, Onsite Administrator

Scott Seacat will be assigned to Dallas County as an onsite administrative technician. He is an Air Force veteran with a degree in applied electrical engineering. Scott has been with Securus since 2014, but his experience with inmate phone services goes back to 1995.

Herb Boyd, Onsite Administrator

Herb Boyd is employed by Shawntech, a **certified SBE**, and assigned to Dallas County on behalf of Securus.

Jason Roseberry, Onsite Administrator

All the personnel listed are essential to ensuring that Dallas County receives first class service. Your Account Manager, Lisa Horne, will oversee the entire Securus team working with Dallas County, including Kelly Elza, your assigned client manager, and your on-site service technicians. **It is our desire that your Client Manager and assigned Field Service Technicians become virtual members of the County's team to ensure your inmate communications system is running at peak performance levels.**

We will keep our commitments to Dallas County and be flexible to best meet your needs, and as an extension, the community's needs, throughout our relationship.

Please see the job descriptions for the On-Site Administrator and Three (3) On-site Technicians on the following pages.

Job Description
On-Site Administrator for Grievance and Tablet Support

Summary	The position of On-Site Administrator is established to provide quality and timely customer service to various audiences associated with correctional facilities, Securus personnel, and partners. They are to provide administrative services of inmate calling accounts and systems. Service Administrators ensure data integrity and proper system functionality of inmate calling system. Service Administrators assist Technical Support in the maintenance of computer hardware, software, and telephony equipment by providing troubleshooting results to appropriate parties.
Responsibilities	**Duties and Essential Job Functions** • Follow the direction of the County contact on daily required needs • Primary representative between on-site facility personal, Securus management and personnel • Maintain a high level of ongoing effective communication with management to assure quality customer service is being provided to all customers and issues are being resolved in a timely manner • Dress neatly and wear proper attire based upon the surroundings and the facility guidelines • Report to work and remain on-site as scheduled • Follow-up with the facility to insure all systems are operational and work is completed thoroughly and accurately • Administration of IPIN data entry, blocks and unblocks, debit & prepaid transactions, investigations of Inmate and Facility complaints, processing of internal documents, and generate reports as requested • Keeping accurate logs and documentation conveying messages and information in writing and/or via e-mail • Advise Management and open Heat tracking ticket for all facility service affecting issues • Maintain effective operation of Inmate Calling system components including hardware, software, and telephony equipment **Accountabilities** • Customer service levels are measured through individual metrics and customer satisfaction survey results. • Demonstrates proficient understanding of the customer's service needs and works to improve the operation of their facility with regard to the Inmate Calling System. • Is courteous, friendly and professional in attitude and appearance. • Arrives on time and works the agreed upon schedule. • Accurate and timely reporting of timesheet and expenses. • Timely responses to requests from Management and customers via phone, pager, or e-mail, etc. • Makes the customer feel good about doing business with Securus. • Communicates effectively and timely with customers and Securus personnel.

	• Adhere to Field Service Operations Service Administrator Administrative
Qualifications	• High school diploma or GED, minimum
	• Self-starting, able to pass an extensive criminal background check
	• Ability to adjust to the correctional facility environment and guidelines
	• Excellent ability at multi-tasking, setting priorities and tracking issues concurrently
	• Have no family incarcerated in any local correctional facility
	• Strong communications skills, written and verbal, for working with customers, dispatchers, technical support specialists, field technicians and management
	• Microsoft Operating System experience including, but not limited to Outlook, Excel, & Word
	• Enthusiastic approach to customer service
	• Must exhibit all of the company's cultural attributes
	• Prior experience in a telecommunications environment
	• Basic Telephony concepts

Job Description
Field Service Technician

Summary	The position of Field Service Technician is established to install, maintain, repair telecommunications, associated computer, networking and electronic equipment and wiring per specifications and operational procedures.
Duties	• Install, maintain, repair telecommunications, associated computer, networking, electronic equipment, and wiring per specifications and operational procedures at correctional facilities. • Gather, update, record, and maintain data and/or statistics. • Communicates with dispatchers to receive work assignments and provides dispatchers with ticket closing information. • Interfaces with multiple departments and/or organizations for problem solutions. • Maintains company vehicle ensuring the following items are current & operational: routine maintenance, inspection sticker, registration sticker & repairs. • Troubleshoots situations where standard procedures have failed in isolating or resolving problems. • May be required to assist in consulting, giving technical support to or training client personnel on Securus products & services. • Maintains inventory of equipment and tools.
Other Functions and Responsibilities	• Determine when to negotiate alternatives, when to escalate a problem or when to ask for assistance in dealing with the various problems reported. • Perform site surveys for new accounts, moves, additions, changes and upgrades. • Work under general supervision • Collect and maintain coin phones. • Perform other duties as assigned.
Accountabilities	Maintain and submit the following as needed: weekly timesheets, service ticket closing information, equipment & tool (truck stock) inventory, preventative maintenance checklists, site surveys and physical site equipment audits.
Qualifications	• High school diploma or GED • Self-starting, able to self-train on telephony based product line • Excellent ability at multi-tasking, setting priorities and tracking issues concurrently • Strong communications skills, written and verbal, for working with customers, dispatchers, technical support specialists, other field technicians and management • Experience working with Windows operating systems

	• Telephony and/or computer hardware experience, Including but not limited to: pulling cable (Cat3 & Cat5), terminations (110, 66, Krone, RJ11 & RJ45) up to 100 pair cables and troubleshooting wiring / T1 / CO dial tone problems and computer repairs (drive, card, board, memory replacements and troubleshooting of hardware as well as OS problems).
Preferred	Microsoft Certifications (A+, N+, MCSE etc…), Cisco Certifications (CCNA etc…), Electronics / Electrical Certification or Degree, PBX & Key System Certifications, 5 years or more of related experience. Previous experience working in law enforcement, correctional environment, customer service skills
Physical Requirements/ Work Environment	While performing the duties of this job, the employee is regularly required to sit and use hands to finger, handle, or feel objects, tools, or controls. The employee frequently is required to talk or stoop, kneel, crouch, or crawl. The employee must regularly lift and/or move up to 50 pounds. Specific vision abilities required by this job include close vision, color vision, peripheral vision, depth perception, and the ability to adjust focus. The noise level in the work environment is usually moderate. The physical demands and work environment described here are representative of those that must be met by an employee to successfully perform the essential functions of the job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

> **Financial Capability**

1) **Provide the most recently issued audited financial statement (or if un-audited, reviewed in accordance with standards issued by the American Institute of Certified Public Accountants.) All statements shall include the following information:**

   a) **Auditor's Report**
   b) **Balance Sheet**
   c) **Statement of Income**
   d) **Statement of Retained Earnings**
   e) **Statement of Cash Flow**
   f) **Notes to financial statement**
   g) **Any written management letter issued by the Auditor to the Respondent's management, its Board of Directors, or the Audit Committee, or, if no management letter was written, a letter from the Auditor, stating that there was no management letter written and that there were no material weaknesses in internal control or other reportable conditions.**

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

Please see our 2018 Audited Financial Report included as **Exhibit A.**

2) ~~If the year end of the most recent completed audit (or review) is earlier than nine (9) months prior to the issuance date of this RFP, then the most recent unaudited financial statement (consisting of items b, c, d, e and f above) shall also be provided by the respondent in addition to the audited statement required in Section 3.3.1.1. The unaudited financial data will be averaged with the recent fiscal year audited (or reviewed) financial statement data, in evaluating financial capability. Unaudited financial statements shall have been completed within the last six months prior to the release of the RFP and shall be certified as accurate by the signature of the respondent's CEO or CFO.~~ **Deleted per Addenda #3.**

3) **If relying on financial documentation of a parent corporation, the Respondent shall provide an original signed letter of commitment from the parent corporation's executive who is legally authorized to bind that parent corporation, certifying that the parent corporation is 100% financially responsible for respondent's performance of the contract.**

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

Securus is not relying on the financial documentation of a parent corporation.

4) **If the respondent is a sole proprietor or non-corporate entity, bidder shall provide financial documentation that is sufficient for an independent CPA to evaluate financial capability including applicable bank and credit statements, income tax returns and other documents NOTE: The County acknowledges that privately held corporations and other business entities are not required by law to have audited financial statements. In the event the respondent is a privately held corporation or other business entity whose financial statements ARE audited, such audited statements shall be provided. If the privately held corporation or other business entity does not have audited financial statements, then unaudited statements or other financial documentation sufficient to provide the same information as is generally contained in an audited statement, and as required below, shall be provided. The County also acknowledges that a respondent may be a wholly-owned subsidiary of another corporation or exist in other business relationships where financial data is consolidated. Financial documentation is requested to assist the Department in determining whether the respondent has the financial capability of performing the contract to be issued pursuant to this RFP. The respondent MUST provide financial documentation sufficient to demonstrate such capability including wherever possible, financial information specific to the bidder itself. All documentation provided should be of the type and detail regularly relied upon by the certified public accounting industry in making a determination or statement of financial capability.**

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

Securus is not a sole proprietorship or a non-corporate entity.

5) **The Respondent should have a Dun & Bradstreet credit-worthiness summary indicating scores of between 1 and 3, or low to moderate, on all categories rated in regard to creditworthiness. The respondent shall provide the name for the entity that will be performing as the contractor. If the respondent is relying upon the creditworthiness of a parent corporation, to qualify under this criterion, the respondent shall also provide the name for the parent corporation. If relying on the Dun & Bradstreet rating of a parent corporation, the respondent shall provide an original signed letter of commitment from the parent corporation's executive that is legally authorized to bind that parent corporation, certifying that the parent corporation is 100% financially responsible for respondent's performance of the contract.**

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

Please see our most recent Dun & Bradstreet report included as **Exhibit B.**

➢ **References**

1) **The Respondent shall furnish a minimum of five (5) business/corporate references to support Respondent's stated Business/Corporate Experience. In order to qualify as relevant current experience, services described by corporate references shall be ongoing or have been completed within the sixty (60) months preceding the issue date of this RFP. Reference(s) shall identify the type of services provided by the Respondent, dates of service provision, the firm/agency name of the entity, for which the services were provided, and the current telephone number and address of the reference. Reference(s) shall include a paragraph describing services similar in magnitude and scope to those requested in the RFP (i.e., ~~900~~ 450 or more phones). The County reserves the right to contact reference sources not listed in the response.**

Note: All references shall be furnished in writing and submitted with the bid packet under the section marked "References".

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

Securus is pleased to offer the following references for Dallas County's review.

Reference #1

Type of Service	Secure Call Platform, Inmate phones, Video Visitation, Connectus, AIS Automated Information Services, Investigator PRO, THREADS, ICER, Tablets
Dates of Service	2002 – present
Firm/Agency Name	Travis County, TX
Number of Phones	500+
Contact Name	Lt. Laura Town
Contact Address	3614 Bill Price Road, Del Valle Texas 78617
Contact Phone Number	512-854-5351
Description of Scope	Travis County has been a customer for over 15 years. Over the years, they have installed more and more of Securus products and services. Travis has installed Investigator Pro, Threads and ICER to assist with investigations and security at the jail. Video visitation allows Family and Friends to visit from anywhere to keep in touch with loved ones. AIS provides the loved ones and inmates a way to self-serve information at any time whether they need to know facility information, charges, and much more. We have an excellent working relationship with Travis

Reference #2

Type of Service	Secure Call Platform, Securus Video Visitation, Investigator Pro, ICER, Threads
Dates of Service	2012 – present
Firm/Agency Name	San Diego County, CA
Number of Phones	830
Contact Name	Captain Alan Kneeshaw
Contact Address	446 Alta Road, San Diego, CA 92158
Contact Phone Number	619-615-2501
Description of Scope	San Diego has been a customer since 2012. Along with Inmate Phones, Sn Diego is utilizing Securus Video Visitation and several of investigative products including Investigator Pro to identify every inmate on every call. We have a great relationship with San Diego County

Reference #3

Type of Service	Secure Call Platform, Inmate Phones, AIS Automated Information Services, Securus Video Visitation, ICER, Investigator Pro
Dates of Service	2003 – present
Firm/Agency Name	Broward County, Florida
Number of Phones	654
Contact Name	Kathleen Casey Kathleen_casey@sheriff.org
Contact Address	555 SE 1st AVE, Ft. Lauderdale, FL 33301
Contact Phone Number	Office # (954) 831-0225
Description of Scope	Broward County has been a Securus customer since 2003 and has an average ADP of approximately 4,500 inmates and 654 phones. Securus provides our Secure Call Platform, Automated Information services, Investigator Pro, PINs, and Video Visitation. Securus has worked closely with the BSO for over sixteen years developing specialized installation methods for unique facility needs and providing a unique exterior wall conduit that was approved by the American Jail Association.

Reference #4

Type of Service	Secure Call Platform, Inmate Phones, IPRO, ICER, THREADS, Video Visitation, Tablets.
Dates of Service	2015 – Present
Firm/Agency Name	Arkansas Department of Corrections
Number of Phones	900+
Contact Name	Rhonda Patterson
Contact Address	2403 E. Harding, Pine Bluff, AR 71601
Contact Phone Number	870-850-8521
Description of Scope	Arkansas DOC has implemented Securus Video Visitation to ensure family and friends are able to visit from anywhere at convenient times and staff does not have to escort for every visit. Tablets are available for inmates to provide a positive and productive stay as well as a safety tool for the staff. Threads, IPRO and ICER are utilized to assist investigators with the latest investigative technology for safety in their prisions.

Reference #5

Type of Service	SCP, Inmate Phones, Investigator Pro, ICER, THREADS, GEX Call Monitoring, GEX Forensic LAB, Wireless Containment Services, Drone Detection, JPay Tablets, JPay Kiosks
Dates of Service	2017 - Present
Firm/Agency Name	Georgia Department of Corrections
Number of Phones	2,215+
Contact Name	Tammy Sexton
Contact Address	300 Patrol Road, Forsyth, Georgia 31029
Contact Phone Number	478-992-6327
Description of Scope	Georgia DOC has a heavy focus on investigations and security. The DOC relies on our voice identification technology and cell forensic labs to assist in investigations. They use our Wireless Communication services to disable contraband cell phones in their prisons. They also use our drone detection software to eliminate contraband from being dropped in the yards and we monitor approximately 5% of the inmate phone calls and report suspicious activity to the investigators. We have a great partnership with the George DOC

➢ **Contact for Contract Administration**

> **1)** **The Respondent shall designate one person authorized to conduct Contract administration and function as the Contractor's Representative under the Contract resulting from this RFP and supply the following information;**
> **NAME:**
> **TITLE:**
> **COMPANY NAME:**
> **ADDRESS:**
> **TELEPHONE NUMBER:**
> **FAX NUMBER:**
> **E-MAIL ADDRESS:**

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

Nancy Salisbury, Sales Vice President, will conduct contract administration/negotiations for the contract resulting from this RFP.

Name:	Nancy Salisbury
Title:	Sales Vice President
Company Name:	Securus Technologies, Inc.
Address:	4000 International Parkway, Carrollton, TX 75007
Telephone:	972-277-0596
Fax:	972-277-0699
Email:	nsalisbury@securustechnologies.com

Robert E. Pickens, Chief Executive Officer, will sign the contract on behalf of Securus.

Name:	Robert E. Pickens
Title:	Chief Executive Officer
Company Name:	Securus Technologies, Inc.
Address:	4000 International Parkway, Carrollton, TX 75007
Telephone:	972-277-0386
Fax:	972.277-0699
Email:	bpickens@securustechnologies.com

B | SYSTEM FUNCTIONALITY, TECHNICAL COMPLIANCE AND APPROACH

B.   SYSTEM FUNCTIONALITY, TECHNICAL COMPLIANCE AND APPROACH (30 points).

Such materials should be organized in the following format:

Inmate Phone Service (IPS) as contemplated in this RFP includes the service, system design, infrastructure and network, equipment, installation, training, operation and ongoing repairs and maintenance of the system and IPS components which best meet Dallas County's desired service levels set forth in the Statement of Services Sought.
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Please see our detailed responses to the Statement of Need/Services sought below.

STATEMENT OF NEED/SERVICES SOUGHT

Inmate Phone Service (IPS) (Control system, Inmate Telephones and Public Telephones), Video Visitation System (VVS) (Control System, Inmate Video Visitation Terminals, Public Terminals, Remote Video Visitation Software and Applications) and Inmate Multi-Function Kiosk (Control System, Software and Applications) as contemplated in this Request for Proposal (RFP) includes the service, system design, equipment, software, installation, training, operation and ongoing repairs and maintenance of the system and its components which shall be provided at no cost to Dallas County. The Hosted Video Visitation Solution proposed for Dallas County must meet or exceed the technical requirements outlined in this Section of the RFP. The Hosted Video Visitation Solution proposed to meet these technical requirements must be provided for all Dallas County facilities at no cost to Dallas County including system installation, training, operation and maintenance of the system and its components. The service to be negotiated through this RFP shall meet any minimum requirements set forth in Section 2, Statement of Services Sought and shall include, but not be limited to provision of the following:
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide Inmate Phone Service (IPS) (Control system, Inmate Telephones and Public Telephones), Video Visitation System (VVS) (Control System, Inmate Video Visitation Terminals, Public Terminals, Remote Video Visitation Software and Applications) and Inmate Multi-Function Kiosk (Control System, Software and Applications) as contemplated in this Request for Proposal (RFP), which includes the service, system design, equipment, software, installation, training, operation and ongoing repairs and maintenance of the system and its components that shall be provided at no cost to Dallas County. The Hosted Video Visitation Solution proposed for Dallas County will meet or exceed the technical requirements outlined in this Section of the RFP. The Hosted Video Visitation Solution proposed to meet these technical requirements will be provided for all Dallas County facilities at no cost to Dallas County including system installation, training, operation and maintenance of the system and its components. The service to be negotiated through this RFP shall meet all minimum requirements set forth in Section 2, Statement of Services Sought.

- **a comprehensive Inmate Phone Service that will allow for collect and prepaid (to include debit) calls for, intralata, interlata, intrastate, interstate and international calls and local telephone exchange service.**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

NextGen SCP is a comprehensive Inmate Phone Service that will allow for collect and prepaid (to include debit) calls for, intralata, interlata, intrastate, interstate and international calls and local telephone exchange service.

- **a technology system, which includes, but is not limited to system infrastructure, network, database, servers, new call processors, digital and analog communications circuits telecommunications capabilities, monitoring, and other required system functionality as specified in Section 2 of this RFP to support the inmate and pay phone telephone service;**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is offering a technology system, which includes, but is not limited to system infrastructure, network, database, servers, new call processors, digital and analog communications circuits telecommunications capabilities, monitoring, and other required system functionality as specified in Section 2 of this RFP to support the inmate and pay phone telephone service.

- **installation of new/refurbished to like new telephone instruments (equipment) at all identified facilities including the required number of instruments and any required station cabling as determined necessary;**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will install new/refurbished to like new telephone instruments (equipment) at all identified facilities including the required number of instruments and any required station cabling as determined necessary.

- **maintenance of visitation phones and Kiosks**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Our Securus video visitation devices are multi-function kiosks equipped with our **ConnectUs** suite of applications. Securus will maintain and support all video visitation phone kiosks. Please see the chart below for more details.

ConnectUS™ Applications

ConnectUS™ Application	Description
Inmate Telephone Application **Benefits** • Security • Controlled Access • Minimal Disruption • Easy User Experience • Multi-purpose device allows more capabilities with less hardware	Inmates can speak to loved ones using our Securus Call Platform (SCP). SCP delivers the latest in inmate calling technology with improved call quality, more effective investigative tools, and greater flexibility and scalability for future growth. New technologies are applied immediately through quarterly upgrades provided at no cost. Inmates can place calls with the same ConnectUs™ terminal they use to conduct a video visitation or submit a grievance. All communications are 100 percent monitored and completely secure.
Video Visitation Application **Benefits** • Security • Controlled Access • Minimal Disruption • Easy User Experience • Multi-purpose device allows more capabilities with less hardware	Nothing beats the ability to "see" a loved one, and Securus Video Visitation makes that and much more possible. While a friend or family member visits from the comfort of their home or office, an inmate visits from their pod, eliminating the need to move the inmate inside the facility. SVV is a fully web-based visitation system that allows family, friends, attorneys, and public defenders to schedule and participate in video visitation sessions with an inmate – from any computer connected to the Internet. Integration phone calling and video visitation onto a common platform maximizes facility revenue and improves investigative capabilities.
Inmate Request Form Application* **Benefits** • Allow any number of forms made available electronically • Define custom routing of forms to the correct person • Enables two-way communication so inmates to receive an electronic response • Documents and archives all communication	Valuable time is lost every day when officers have to process inmate requests manually. Worse yet, every request must be hand written and there is no easy way to maintain accurate records. This creates unnecessary liability for your facility and leaves inmates believing their requests have been ignored. Inmates can electronically create and track requests through ConnectUs™ and staff can easily review, respond, and process requests. Requests and responses are tracked and saved for future reference. Two-way communication with inmates could not be easier.

Grievance Application

Benefits

- Create multiple inmate forms with individualized routing processes
- Configure the Grievance Application to process multiple types of forms and custom routing based on the type of form submitted
- Require responses from jail staff to validate that the response was received
- Eliminate manual administration/paper-handling of grievance forms

INMATE FORMS

Grievance administration is often one of the most complicated and manually laborious processes in a correctional facility. Certain inmate rights must be honored, facilities must respond within strict timelines, and all actions must be properly documented. Failure to do so comes with large penalties and fines and creates legal liability.

The Grievance Application is a form submission and routing tool that allows inmates to submit grievances electronically. Correctional staff can then electronically prioritize, route, and respond to the submissions.

Inmate Handbook Application

Benefits

- Reduces/Eliminates printing/distribution costs
- Reduces staff workload distributing and replacing handbooks
- Provides instant, electronic updates to documents

INMATE HANDBOOK

A digital version of your inmate handbook can be accessed through The Inmate Handbook application on ConnectUs™. Inmates can access information without printing or distributing a single piece of paper. Digital versions of other important documents can be available on ConnectUs™ in addition to the Inmate Handbook.

Video Education Application

Benefits

- Communicate information to all inmates, even those unable to read
- Provides a form of communication that is often easier to comprehend, ensuring your message is understood
- Provides educational videos without staff involvement

PREA

ConnectUs™ provides the ability to upload any MP4 video. Everything from a video version of your inmate handbook, a jail orientation video, or a video tutorial on how to use ConnectUs™ is possible. You can make the video available for viewing any time or only during defined hours.

Law Library Application

Benefits

- Compliance to legal and mandatory requirements to provide

LAW LIBRARY

The ConnectUs Law Library Application makes legal research simple. Adhere to your legal obligation while reducing costs when inmates perform their legal research using the Securus Law Library Application. This Application provides full access to

inmates access to the courts (1977 Supreme Court Ruling; Bounds vs. Smith)

- Reduce or eliminate inmate complaints and litigation
- Always up-to-date information; automatic updates provided at no extra cost
- Free up staff time with and easy and safe solution
- Eliminate the need for housing large book collections, additional hardware, network, or electrical equipment because the application rides on Securus' ConnectUs inmate platform
- Reduce costly and time-consuming inmate movement by hosting law library search resources in the housing units rather than escorting them to a physical library or terminal
- Receive turnkey service; Securus takes care of everything

inmates to complete legal research without the need for transporting inmates to a facility library or special computer.

The inmates can remain in their housing unit and research legal topics through this ConnectUs application. Unlike large book collections that require costly replacement of revised material, the Law Library application includes nightly automated updates that are provided to the County at no extra charge.

ConnectUs Job Search Application Benefits

JOB SEARCH
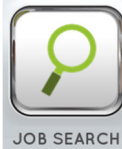
- Minimize job-seeker training costs because the terminal is self-explanatory
- Provide job listings in cities nationwide for all types of jobs and levels of experience
- Eliminate the need for additional hardware, network, or electrical equipment because the application rides on Securus' ConnectUs inmate platform
- Reduce costly and time-consuming inmate movement by hosting job search resources in-house rather than issue passes for off-site job searches
- Track and measure the job search activity with detailed reports
- Receive turnkey service; Securus takes care of everything

The ConnectUs Job Search Application makes searching for a job simple. It allows inmates to perform job searches and view current local and nationwide jobs in numerous fields using Securus' Job Search Application. This application will assist in meeting one of the objectives of your facility in preparing inmates for life on the outside by reducing recidivism rates. The Job Search Application provides full access to inmates to complete job searches without the need for transporting inmates to a facility library or special computer. The inmates can remain in their housing unit and research employment options through this ConnectUs application.

eMessaging Application

Benefits

- Improves correctional staff utilization and efficiencies using all-digital review and distribution technology
- Automates message screening; visual alerts flag inappropriate words for quicker review
- Reduces traditional paper mail and efforts to search for contraband
- Increases investigative data collection and analysis
- Facilitates constituent and incarcerated communication
- Uses existing facility and inmate hardware and network connectivity

eMessaging allows inmate to communicate with their family & friends through a text based message or picture. Based on the most widely used messaging platform in the corrections industry, Securus eMessaging improves the efficiency of staff and reduces paper mail by transmitting communication electronically – all at no cost to the facility. eMessaging is configurable to allow constituents to send a digital message with the option to include a photo and even purchase an inmate reply – or can be set to only allow incoming messages.

All messages flow through the eMessaging facility portal for analysis, review and release to intended party if approved. Unlike physical mail, all messages are stored electronically for investigation and analysis and are easily accessed using intuitive sort and search tools.

Sick Call Application

Benefits

- Automates manual processes
- Enables staff to focus on security
- Eliminates the unnecessary movement of inmates within the facility
- Allows authorized infirmary staff to access calls anytime/anywhere
- Provides a higher quality of service to inmates, reducing grievances

The Securus Sick Call application allows an inmate to report an ailment to facility staff by selecting from a predetermined list.

Digital Bulletin Board

Benefits

- Automates manual processes
- Enables staff to focus on security
- Keeps inmates informed of important facility-related information without requiring additional work by the staff.

ConnectUs™ allows you to easily publish notifications that are always displayed on the ConnectUs™ terminal. In addition to providing pertinent facility-related information, these messages can be used to promote new products, services, and promotions such as Video Visitation.

VRS

Benefits

- Provide VRS-capable inmate call devices that fully conform to the rigorous needs of the correctional environment
- **Unlike our competitors, manage VRS calls using the same controls as are used for traditional inmate calls**
- Record VRS calls in accordance with the same recording controls that govern whether or not to record traditional inmate calls
- Ensure equal access to visitation with friends and family.

ConnectUs™ provides support for hearing-impaired inmates through an easy-to-use Video Relay Service (VRS) application.

- **systems and equipment that support Dallas County's call monitoring/security needs, including terminals, and digital recording equipment as determined necessary;**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide the systems and equipment that support Dallas County's call monitoring/security needs, including terminals, and digital recording equipment as determined necessary.

NextGen SCP, our Secure Communications Platform, is cloud-based and Web-enabled, and has virtually unlimited capacity to support facility expansion. It automates the management of the inmate communications system, and delivers an array of cost reduction functions and safety enhancement features. Authorized users can access the system anytime and anywhere from a workstation or mobile device that has Internet access.

NextGen SCP User Interface

The User Interface is the County's window to all NextGen SCP features. The SCP is one of the only **single-point-access** user interfaces in the industry. We built it to allow our partners to have complete control over their systems in a simple, reliable, and secure environment. Authorized users can easily audit call data, turn on a phone, restrict a phone, create alerts, change a blocked number, and manage features and applications — all in real time. As a result, **facilities benefit from increased efficiency, increased flexibility, on-demand access to call recordings, and unequalled investigative access to potential criminal activity.**

- **creation of a centralized database which shall contain all data elements necessary for provision of monitoring services, reporting and historical call transaction information;** **SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.**

NextGen SCP has a centralized database that contains all data elements necessary for provision of monitoring services, reporting and historical call transaction information. We also offer a full suite of investigative tools at no cost to Dallas County that are fully integrated with the calling platform.

THREADS™ Analytic Data Platform—Overview

Securus understands that during an investigation, the law enforcement community is inundated with tasks and gathering intelligence. Identifying relevant data can be a challenge at times when new data are identified. This results from numerous different sources, formats, and potential leads that require identification. **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 can be managed remotely at any time through an assigned web-based portal.** This means that Dallas County can access data remotely from any location that provides internet access.

THREADS Brings Big Data Capability to the Corrections Industry

CUSTOMIZABLE DASHBOARD

COMMON CONTACT
SPECIFIC LIST OF INDIVIDUALS
ENTITY LINKAGE
COMMON CONTACT
CONCURRENT COMMON CONTACT

SUSPICIOUS ACTIVITY

BOUNCE LIST
ENTITY LINKAGE
ENTITY LIST

HERE WE CAN CALL OUT
ANY OTHER TYPE OF REPORTS
OR INTELLIGENCE

THREADS™

THREADS WORKSPACE
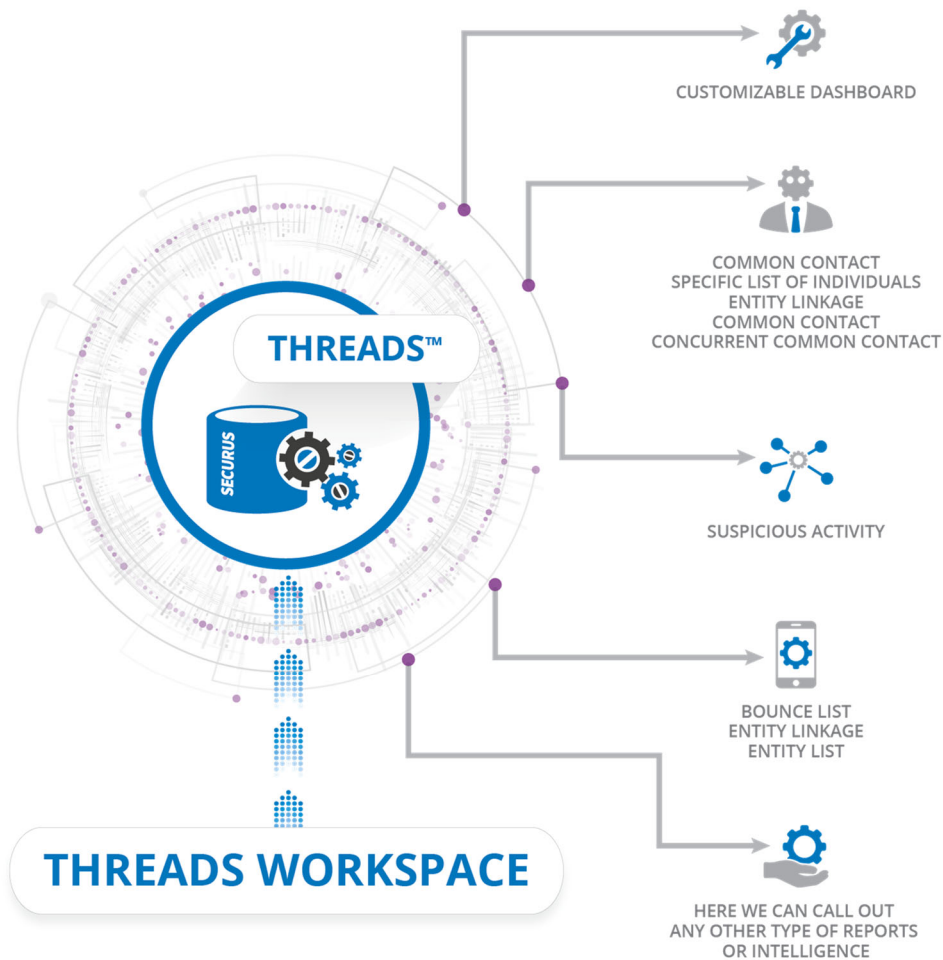
THREADS Applies Big Data Search Algorithms to Investigative Support

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.

Data Pulled from Multiple Databases
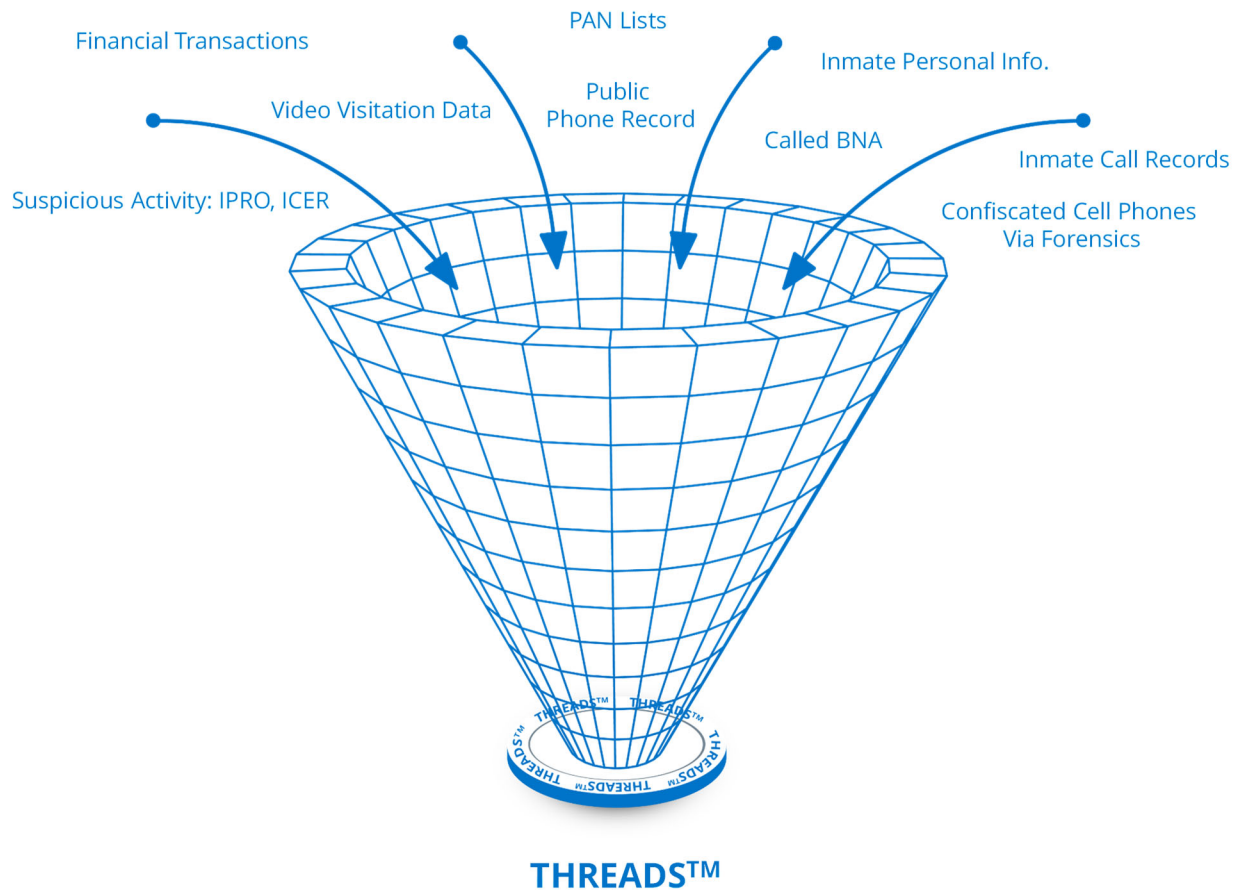
THREADS™

THREADS automatically imports information from NextGen SCP's telecommunications database, inmate information from JMS, and financial data. Multiple sources of data and databases are combined into the THREADS' analytic framework to reduce the time required for investigators to find suspicious patterns. Such patterns may be an indication of planning or commissioning crimes.

Widely-Used Investigative Telecommunications Platform

THREADS is the most widely used investigative telecommunications platform in the industry today, with more than 1.5 million inmates served, multiple 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 inmate 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' robust and accurate analytics engine is intuitive and easy to use, making it the ideal tool for any investigative officer operating within a correctional institution.

THREADS Was Developed Specifically for the Corrections Industry

Unlike other investigational software, which requires users to manually upload facility data, THREADS automatically consumes facility data on a nightly basis and does not require any equipment to reside on site. **The unique algorithms within THREADS were designed in conjunction with high-profile investigators, bringing more than 50 years of combined experience in communications, data, and training.** What can take an entire day with multiple officers working eight-hour shifts now takes just moments.

Primary Benefits of THREADS to the Prison Community

The primary benefits of THREADS to the prison community include:

- Visually-based linkage reports that make the identification of communication patterns and the identification of inmate activities and communications quick and easy to understand.
- Significant reductions in the amount of investigative time required to produce documented and actionable results.
- Community Data Sharing that allows facilities to run reports on a much larger data set to expand their investigative reach.
- Customizable facility dashboard with configurable display-based facility metrics.
- Discovery and disruption of inmate-based criminal activities.

Importing Information

THREADS will automatically import the **following types of corrections information**:

- Inmate call records
- Inmate personal information, such as name, account number, PIN, DOB, SSN, and more
- PAN lists
- Called party billing name and address information
- Video visitation data
- Suspicious activity, through IPRO and ICER for example
- Financial transaction metrics

THREADS can also import **information from external data sources, such as:**

- Confiscated cell phones—calls, text messages, emails, videos, contacts, etc.
- Public phone records
- Events and places of interest
- Mail
- LexisNexis

THREADS Communities

THREADS further separates itself from other inmate telephone service providers by providing a national community database where facilities can choose to share their data to expand and identify more investigative opportunities and leads. Facilities can choose to share data with other local, regional, or national agencies depending on their investigative needs.

Through this community of data sharing, THREADS users can leverage the resources of other agencies to understand the breadth of their investigations and, therefore, close cases faster. By joining the THREADS community, users can run reports, uncover data correlations, and gather contact information unlike any other data analytics solution.

THREADS Communities Share Data Between Multiple Jurisdictions
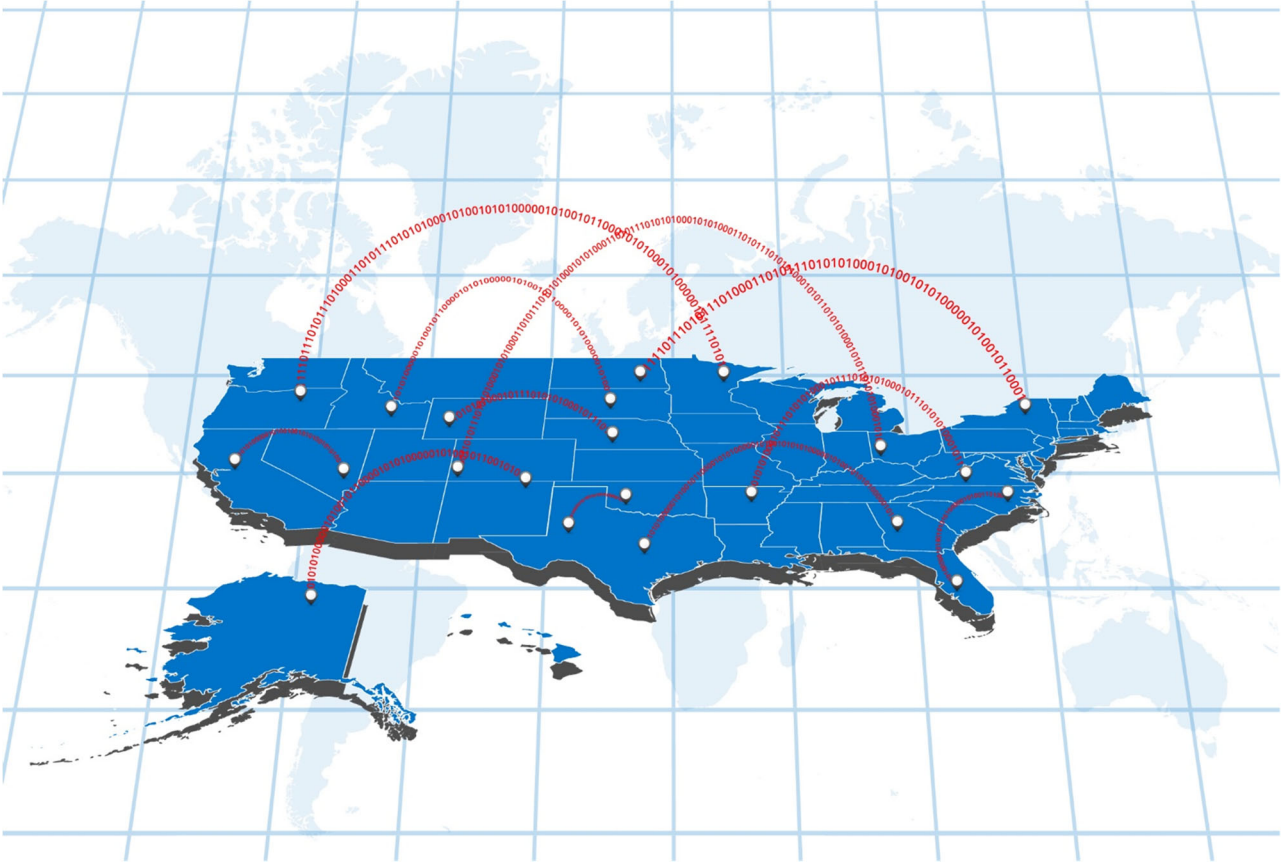
Discover / Analyze / Import

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. Details of what items are contained in each section are provided below:

- **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 reocrds; confiscated cell phone forensics; data extracted from JMS, RMS, and other systems and data.

THREADS *Discover* Landing Page (Dashboard)

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 Inmates, Top Contacts, and Recent Records.

Securus understands that during an investigation, the law enforcement community is inundated with tasks and gathering intelligence. Identifying relevant data can be a challenge at times when new data are identified. This results from numerous different sources, formats, and potential leads that require identification. 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 can be managed remotely at any time through an assigned web-based portal. This means that Dallas County can access data remotely from any location that provides internet access.

THREADS further separates itself from other inmate telephone service providers by providing a national community database where facilities can choose to share their data to expand and identify even more investigative opportunities and leads. Through this community of data sharing THREADS users can leverage the resources of other agencies to understand the breath of their investigations, and therefore close cases much quicker.

Please read more about the most frequently used features of THREADS at **Exhibit C**.

- **hosted video visitation services**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus video visitation solution is web-based and fully hosted by Securus.

- **any value-added service features not specifically outlined within**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is pleased Dallas County to offer the following value-added products and services:

AIS (Automated Information Services)

Securus is also pleased to support **Automated Information Services at Dallas County.** Automated Information Services (AIS) uses the latest in voice response technology to automatically handle internal inquiries from inmates as well as outside calls from friends, family members and other agencies. AIS automates upwards of 80% of standard inquiries, allowing staff to be redirected to more critical issues and tasks in the jail.

Enabling Automated Information Services automates over 80% of incoming calls allowing the public to 'self-serve' on repeated requests of inmate information, visitation information, etc. **Inmates are also able to 'self-serve' information on upcoming court dates, bail amount and charges greatly reducing kites, grievances and staff time.**

Inmate Inquiries Handled with Less Staff Interaction and No New Equipment!

Without staff involvement, the public can access important information about inmates and facilities.
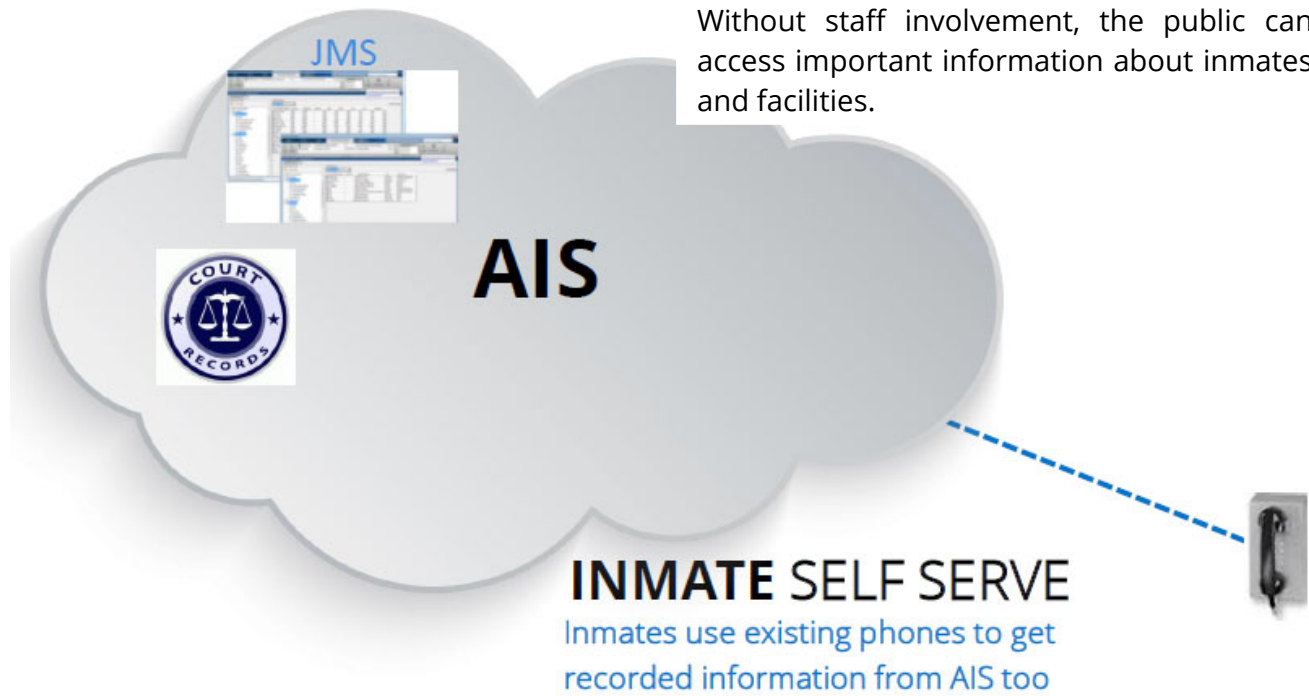
Securus' AIS is the correctional industry's first and only hosted full speech recognition IVR system that automatically provides inmate-specific and general facility information to constituents and inmates alike that is customizable to your facility's needs.

Inmate Tablets

We promote equal access to content for all inmates with our free community tablets. At no cost to the inmate, they can have access to books, mental health podcasts, religious material, a job search engine and educational content.

If an inmate would like to keep their tablets for the entire month, we offer that for the low cost of $5. There is no one else in the industry as committed as we are to providing access to this technology for as low a cost as possible. We recognize how important it is for all inmates to have access to opportunities for self-improvement and enrichment.

The Many Uses of SecureView Inmate Tablets

SECUREVIEW BETTERMENT & WELLNESS CONTENT

MENTAL HEALTH

ADDICTION RECOVERY

PERSONAL DEVELOPMENT

EDUCATION

RELIGION

Available and Accessible
for all inmates at **no cost**

EMPLOYMENT RESOURCES

& MUCH MORE

Education Options

SecureView Tablets have **robust education capabilities**:

KA LITE

KA Lite is a Securus-customized, easy to use offline education application that allows inmates to access K-12 educational content such as Math, Science, History, Computing, and much more. KA Lite offers practice exercises, instructional videos, quizzes, and test prep.

KA LITE

Securus took leading offline education application, KA Lite, and customized it to be optimized for inmates

PROVIDES:
- Self-paced learning
- Complete K-12 education
- Prep for GED
- Reporting
- Securus "Customized for Corrections" Platform
- Multiple language support

SUBJECTS AVAILABLE:
- Math
- Science
- Career Exploration
- Health/Mental Health
- Grammar
- Computer Programming/Science
- History
- Entrepreneurship
- Personal Finance/Accounting
- And More

Educational Videos Available **7000**

25,000+ Exercises and Skill Checks

Unlimited Learning Opportunities with Lantern

Securus facilitates implementation of any educational content (including from local area colleges) to offer inmates additional learning opportunities through our Lantern LMS.

Lantern is a technology-driven education program featuring a comprehensive Learning Management System, enabling educational opportunities for inmates through the use of tablets.

LANTERN

Education leads to increased employment opportunities for inmates upon re-entry and reduces recidivism

- More than **80,000** inmates have enrolled in classes via Lantern
- More than **33,000 college credits** earned
- Over **4.5 million** education course files downloaded

"I've learned that at 37 years old **I can take classes successfully**." - Lantern Student

Lantern hosts facility-approved content, which is consumed by inmates on their SecureView tablets. **Inmates 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.

Content from the Recovery Resource Council and TORI (Texas Offenders Re-entry Initiative), as well as UT Southwestern's Healthy Relationship and HIV Prevention Classes and the OSHA certification classes, can be offered to Dallas County inmates on the SecureView tablets using Lantern.

College Credits through Ashland University

If your agency chooses to participate in **offering college courses**, Securus is partnered with Ashland University, an accredited university that offers free college courses to the incarcerated using 2nd chance Pell Grants. Securus and Ashland provides a turnkey solution so no extra facility staff time is needed to support this Education option.

- Exclusive to the **Ashland University partnership**.
- Students enrolled in Ashland University courses access courses from an Ashland University app
- App launches a browser that only accesses corrections-grade Blackboard LMS (learning management system) site, or, alternatively, counties can choose our exclusive Lantern learning system.
- Students also utilize Mobi Office Suite (Word, Excel, PowerPoint) to create assignment files. This special office suite was customized for Securus to meet the security needs of our customers.

Inmate Enrichment

In addition to **free learning management software** and **college courses**, SecureView Tablets offer:

- Tens of thousands of **free eBooks**.
- **Mental Health and self-help books** and podcasts
- Religious materials
- Access to valuable **law library** content
- Access to job searching through JobView

ADDICTION RECOVERY

Multiple Addiction Recovery programs are available through SecureView Tablets

RESOURCES INCLUDE:

- Thriving After Addiction
- AA/NA
- Opiate Addiction
- 12 Step Programs
- Healing
- Recovery Tips
- Other content can be uploaded at the request of the County

Updated daily to provide the latest content

MENTAL HEALTH

Hundreds of hours of Mental Health programming are available for inmates to utilize

RESOURCES INCLUDE:

- Anxiety Relief
- Depression Assistance
- Relationship Guidance
- Guided Meditation
- Breathing Exercises
- Self-Reflection

Updated daily to provide the latest content

Securus is the only provider that utilizes Officer Tablets. Securus' unmatched Command & Control officer tablets enable facility staff to easily control who gets a tablet, when the inmate can use it and what is on it.

Command & Control Officer Tablets

The Officer tablets are customized Nexus 7 SecureView tablets and are provided at the POD level or as required by your facility. Officers have the ability to monitor any individual inmate activities as well as close out or activate individual applications by inmate or across multiple users. Additionally, an officer can deactivate all tablet functions by inmate, group of inmates or all inmates under his control - all in real time. Securus knew this level of control was critical for a successful tablet program.

SecureView tablet existing clients have confirmed that the ability to view activity by inmate and the ability to shut down applications and tablet access by inmate, group of inmates or the entire system has provided them with the administrative control necessary to ensure for overall safety and security. Command & Control officer tablets allow designated facility personnel to remove any or all tablet functionality, which may be used as a means of discipline.

The Officer tablets have a detailed dashboard views that allow your staff real-time search functionality and analytics. Administrative functionality on Dashboards is comprehensive and flexible. We can provide more officer control or less officer control based on your facility's desired specifications.

The Command & Control tablet will allow your facility to control and offer required and optional services to inmates in an easy, efficient and cost effective way; all while promoting positive inmate productivity and betterment. Securus again proves its dedication to partnering with corrections to modernize incarceration and connect what matters.

Sub Manager App

The Sub Manager Application is utilized by corrections staff for the command and control of Inmate Tablets.

Behavior Modification

The ability to remotely behavior modify an Inmate Tablet allows for an added level of safety and security, by removing the need for facility staff to interact physically with an inmate in order to control applications on a tablet, a group of tablets, or an entire facility of tablets.

Scheduled Behavior Modification feature allows authorized users to elect to have the request expire:

- Until manually changed by the user or someone with authorized permission

- Within "X" number of hours / days / weeks / months

- Until a selected Date / Time

Eligibility Check

Eligibility allows authorized users:

▪ Ability to determine if an inmate is eligible to receive a tablet

▪ Provides an explanation of ineligibility

▪ Provides the ability to place an inmate on the eligibility or ineligibility list

Availability Restrictions

The Availability Restrictions feature allow authorized users full control over when applications are available.

The ability to create application schedules to allow select applications to be active or inactive based on:

- o Days of week
- o Time of day
- o Both days of week and time of day

Availability Restrictions may be activated for:

- o Specific housing location(s) of tablets
- o Entire facility of tablets

Availability Restrictions are designed to be customizable to fit the needs of your facilities scheduled events, such as Commissary distribution times, meal times, count times, etc.

Messages

The Messages feature provides authorized users the ability to have critical information and notifications regarding the status of all tablets.

Tablet Inventory

Securus automatically maintains the inventory by location. From the Inventory Page in SubManager, staff can see the number of tablets by location and tablet type.

When Community Tablet inventory goes beneath the predetermined threshold, Securus will automatically ship additional Community Tablets to the facility. The shipment date will be noted on this page.

Staff can also view the number of pending subscriptions (those that family and friends purchased) and who still needs to activate their subscription through the Make Mine application. This information is all available by location.

Please see more about our SecureView Tablet program at Exhibit D.

BE AWARE: Video visitation on tablets is frequently promoted by other service providers. Although we can activate video visitation on our tablets, we do not recommend it for the following reasons:

- Cameras on tablets can reveal sensitive facility information to third parties, compromising inmate and staff safety

- Video visits from fixed locations, via kiosk, are safer because it allows for staff oversight on inmate conduct during the visit

- Video visits that occur in private locations (due to the mobility of the tablets) increase PREA risks

- The "facial recognition" claimed by other providers is really just technology that senses a face within certain visual parameters to keep the video link open. When inmates move around with their tablets during video visits, the camera turns off, resulting in audio visits—at the higher billing price of a video visit.

BE AWARE of the costs of tablets by other providers. Some providers charge by the minute for tablet use, resulting in large, burdensome monthly bills. Other providers make inmates purchase their tablets, preventing equal access to valuable content from which many inmates would benefit.

Securus provides free community tablets to all inmates, with the option of renting a tablet, for exclusive personal use, for five dollars a month. With Securus, ALL inmates will have FREE access to job searching, law library, ebooks, forms and grievances, and educational materials.

Investigator Pro (IPro)

Investigator Pro (IPro) is the most powerful voice biometrics solution in the industry. Using advanced voice biometrics technology developed for the U.S. Department of Defense, IPro goes far beyond the limited capabilities of standard biometric verification systems by identifying all the inmates speaking on a call. IPro biometrically analyzes the entire phone call, detecting suspicious voice prints and automatically presenting findings. It flags potential criminal calling activity and immediately alerts investigators to those calls.

Through its near-instantaneous collection and analysis of vast amounts of information, IPro allows Securus partners the ability to pre-empt and unravel criminal plans.

Securus IPRO voice biometrics is the **most proven system** in the correctional industry with **over 270 deployments**.

Please read more about Investigator Pro in **Exhibit F.**

ICER

Inmate-to-inmate communication (ITIC) 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: **inmate-to-inmate 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 inmate phone calls, we offer cutting-edge technology based on state-of-the-art, patent-pending, call-matching technology that identifies ITIC even when it's between two different correctional facilities across the country.

Please read more about ICER in **Exhibit E.**

Securus' Digital Mail Center

Securus understand that contraband is one of the many items that plague today's correctional facilities. Ensuring that contraband stays outside of facility walls allows for a safer environment for both facility staff and inmates. With Securus' Digital Mail Center solution, facilities control contraband introduction through the postal mail delivered to your facility.

Converting physical postal mail into electronic communications creates measurable results:

- Dramatically improves investigative intelligence
- Eliminates contraband entering through postal mail

- Immediate notifications to staff and investigators when particular inmates receive mail creates timely intelligence

The Securus Digital Mail Center eliminates contraband entering correctional agencies through the postal service by scanning physical mail and delivering it electronically to inmates through Securus' ConnectUs inmate terminals and Tablets. The Digital Mail Center software allows authorized Provider staff or correctional agency staff to scan certain physical mail and electronically deliver it to inmates through Securus' Digital Mail Center Dashboard. The Securus Digital Mail Center Dashboard then provides the following capabilities and information:

- Ability to view, approve, reject, and manage scanned mail
- Ability to set alerts when specific inmates receive mail
- Audit logs of activity associated with the Securus Digital Mail Center for increased administrative oversight

After the mail has been scanned and reviewed, Digital Mail Center then delivers a scanned copy of the mail electronically that can then be delivered and viewed by the incarcerated individuals through ConnectUs phone terminals and/or Tablets.

The Digital Mail Center Dashboard. Within the Dashboard provides facility staff with a full suite of capabilities:

- View, approve, reject, and manage all scanned mail.
- Ability to create text and email notifications when specific inmates receive mail.
- Full audit logs of all activity for increased administrative oversight.
- Easily configurable to automatically release scanned mail to inmates, allow for administrative approval for all mail prior to being electronically released and delivered, or require administrative approval for inmate-specific mail.
- Custom Watch Word List automatically identifies when content is inappropriate. NOTE: Custom Word Watch List active only if agency uses Manual Transcription feature

All information associated with the letter, including sender name, time, date, address, and content, are stored for the life of the contract. This creates permanent investigative intelligence that is impossible to achieve through standard physical mail processing. The facility may also determine whether physical mail that has been processed will be returned back to the facility or destroyed. Contraband will be delivered to local law enforcement for processing and facilities may request that a case be opened for senders of contraband material. If mail originating from an attorney's office or other private/privileged establishments is received, it is immediately sent back to the correctional agency for physical deliver in order to ensure attorney/client privilege is maintained.

- **Contractor personnel to perform oversight, administration, operational assistance and maintenance and repair to the IPS system and equipment. It is anticipated that at a minimum, the system administrator and a technician will be assigned on-site, full time;**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus personnel will perform oversight, administration, operational assistance and maintenance and repair to the IPS system and equipment. Securus will provide four fulltime onsite technicians and administrators.

- **ongoing maintenance, repair, and/or replacement and/or upgrades of all equipment, systems and software as determined necessary to ensure service delivery;**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus ongoing maintenance, repair, and/or replacement and/or upgrades of all equipment, systems and software as determined necessary to ensure service delivery.

- **all required training and instructional materials required for use of the telephone services as applicable to inmates, families, and/or County staff; and**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide all required training and instructional materials for use of the telephone services as applicable to inmates, families, and/or County staff.

- **TX Commission on Jail Standards minimum standards and mandates must be applied.**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will apply and maintain all TX Commission on Jail Standards minimum standards and mandates.

- **all related support services not otherwise indicated herein.**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide all related support services not otherwise indicated herein.

Dallas County has prepared a matrix of system functionality and technical requirements. (System Matrix ATTACHMENT 6) Respondents shall complete this matrix. The evaluation committee will review the information provided in this matrix to evaluate the qualifications of each Respondent.
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Securus has provided a thorough response to all of the requirements stated in Dallas County's Statement of Services Sought and looks forward to the opportunity to demonstrate our solution. Our internally developed systems meet and exceed all stated requirements and provide additional options to deliver flexibility to Dallas County in how the system is deployed.

Please see the completed **Attachment 6** on the following pages.

Attachment No.6

System Functionality/Technical Requirements Matrix

Vendors must submit a completed matrix with their RFP response and provide one of the following response codes for each item listed.

Y =   **this feature is currently in production in vendor's proposed system (i.e., fully implemented and in use) in another entity's operations.**

T =   **this feature is currently developed and is in Alpha or Beta testing and is provided with the proposed solution**

U =   **this feature is not currently developed but can be added to the system. Please provide additional information if this response is provided.**

P =   **this feature is only partially available in the proposed solution.**

M =   **a modification would need to be made to the proposed solution to provide this feature.**

N =   **this feature is not provided.**

Additional comments are encouraged and should be placed next to the response code.
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

FUNCTIONALITY	RESPONSE CODE	COMMENTS
Security		
System contains security features which prevent unauthorized individuals from accessing any information held by the Contractor	**Y**	Please see our comments below.
NextGen Secure Communications Platform™ (NextGen SCP™) uses security roles to determine user permissions. They define what actions a user can and cannot do within the system. NextGen SCP contains default security roles, identified by the eyeball ( ) icon. While these predefined roles cannot be modified, they cover many customers' needs for granting access and denial rights based on common job functions. NextGen SCP provides more options for Dallas County to further customize access privileges by allowing authorized administrative users to either create a new user-defined role or create a new role using an existing role as a base and further modifying it. The user-defined role can be customized to meet Dallas County's specific needs when a default role does not. These roles are identified by the pencil ( ) icon. In addition, the Dallas County administrator can assign multiple roles to a user to tailor their access to exactly what is needed. This provides virtually unlimited options for customizing users' access.		

Sample Security Roles

Password Policies

NextGen SCP uses strong passwords that require users to update passwords regularly. Passwords must comply with the following rules:

- 8 – 12 characters
- No spaces
- Cannot contain the user's first or last name
- At least three of the following types of characters must be used:
  - English uppercase letter
  - English lowercase letter

- o At least one number
- o At least one special character

Passwords can be configured by location, days to expire, and even the number of password cycles before password reuse. Additional configuration options include reminders for password expiration and minutes of allowable inactivity before session timeout.

The "Forgot Your Password?" feature available from the login screen offers online support for users who have forgotten their password or for those who did not change their password before expiration. System security requires users to provide the correct answers to preset questions before their password can is reset. Once a new password is created, NextGen SCP emails confirmation to the address linked to the user ID.

Secure access to the system and the database shall be maintained at all times	**Y**	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) is a single platform for managing, researching, monitoring, investigating, and exploring information through Securus products and services.

> NextGen SCP will be an upgrade from classic SCP.

NextGen SCP's user interface is Dallas County's window to all of its features. Because it is entirely web-based, authorized users can access the system at any time, from any location. This design delivers investigative recordings with digital clarity and provides easy remote monitoring from any secure web browser with internet access.

This system is one of the only single-point-access user interfaces in the industry, built to allow our customers complete control over their systems in a simple, reliable, secure environment. Authorized users can easily apply settings and configurations to turn on a phone/terminal, restrict a phone/terminal, change a blocked number, administer approved call and visitor lists, and turn on or off features and applications — all in real time. All of the integrated features are accessed easily with the click of a mouse. As a result, facilities get the following benefits:

- Increased efficiency for staff
- Increased flexibility
- Quicker "on-demand" access to communication detail records and communication event recordings
- Unequalled investigative access to potential criminal activity

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.

Each user has access rights assigned by the administrator, allowing the county jail to control access based on the facility's security clearance objectives. Administrators can limit individual

access to each application, and can also limit access to each function within each application. A user log documents the user, time of access, and accessed modules as an added security measure.

For even more security and control, user access can be programmed to restrict users to specific IP addresses within certain time limits. For example, a user could be restricted to access the NextGen SCP user interface from their workstation (and only their workstation) between the hours of 8:00 AM and 5:00 PM and their access blocked outside the facility.

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.

From a single login, authorized users can manage SCP and SVV.

Securus infrastructure servers and all workstations require anti-virus protection and receive regularly scheduled security patches and updates.

Login Screen

SECURUS
Technologies

SECURUS
NEXTGEN SECURE COMMUNICATIONS PLATFORM

WELCOME

Welcome to the **SECURUS NextGen Secure Communications Platform (NextGen SCP)**. If you have a Secure Communications Platform account, login on the right.

To sign up for a SECURUS NextGen Secure Communications Platform account, please contact your Securus Account Manager or call Securus Technical Support at 1.866.558.2323.

PLEASE LOGIN

USERNAME

PASSWORD

LOGIN

Forgot your password?

Call Restrictions

System restricted to outgoing calls only.	**Y**	Please see our comments below.

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 inmate.

Securus has performed full testing of these trunks, verifying compliance with this requirement.

System provides a programmable time limit for calls with warnings for remaining time as call progresses.	**Y**	Please see our comments below.

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 inmate a verbal announcement one minute prior to end of their call and then enforces the facility policy with a hard stop.

System allows for Dallas County to program times when the system will be operational, i.e. available or unavailable for inmate calls.	**Y**	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) calling services has automated calling schedules that allow 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 inmates 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.

During the call set-up process, the system provides a pre-recorded announcement identifying that the collect call is coming from a specific inmate at a Dallas County Jail.	**Y**	Please see our comments below.

When a called party answers, the Securus calling service announces a collect call from an inmate and states the name of the calling institution. The inmate's recorded name is played to the called party as part of this call acceptance message to provide identification of the calling inmate.

For example, a typical announcement would say, "*You have a collect call from an inmate, "John Doe," at the Dallas County Jail. This telephone call may be monitored or recorded.*"

Each facility can customize the facility name used in call announcements.

System states rate and complaint information, contains a toll free number for the consumer's use, announces this information to the answering party with the statement "All telephone calls will be recorded except attorney calls".	**Y**	Please see our comments below.

The Securus calling service includes an Interactive Voice Response (IVR) system that provides Automated Operator Services (AOS). This automated assistance uses clear and concise, professionally recorded voice prompts to establish call acceptance and to assist inmates and called parties throughout the calling process.

When the called party answers the phone, the calling service's advanced answer detection triggers the call acceptance voice prompt. The called party hears, "Hello, you are receiving a collect call from [inmate's name], an inmate at the Dallas County Jail. This call is subject to monitoring and recording." 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."

Additional options provided by AOS include:

Available Options to Called Parties	**Available Options to Inmates**
- Request a rate quote - Hear the name of the facility and inmate 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 - Choose to hear the prompts on the system in English, or the language selected by the inmate (if configured for this option) - Pay for the incoming call with InstantPay (if available) - Hear optional marketing message (by request of Dallas County) - Block their number prior to accepting a call using the system's Perma Block technology*	- Listen to prerecorded announcements - Choose to place a collect or debit call; if debit, PIN entry is requested, the inmate 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 inmate call time limits based 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 marketing message (by request of Dallas County)

*The calling service's automated operator also provides a <u>Perma Block process</u>, which allows a called party to block their number permanently. This feature may be used to block calls from any inmate 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.

Language Requirements

System contains an automated announcement function capable of processing calls on a selective bilingual basis: English and Spanish.	**Y**	Please see our comments below.

The Securus calling service default system setup provides message prompts in both English and Spanish. Inmates select a specific language 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 and then receives an option to continue in the language the inmate selected. This fraud deterrent feature eliminates possible attempts by the inmate to confuse the called party with a language they do not understand.

Securus provides durable printed dialing instructions in both English and Spanish on each inmate telephone, using materials and techniques appropriate for the correctional environment that explain the process in a clear, easy to read manner:

Sample Dialing Instructions in English and Spanish

This Call is Being Recorded	Esta Llamada va Hacer Gravada
DIALING INSTRUCTIONS	**INSTRUCCIONES PARA LLAMADA**
Press '1' for English	Marque '2' para español
For a collect call, press '1'	Para llamada a cobrarse, marque '1'
For a debit call, press '2'	Para llamada de débito, marque '2'
TIPS Hotline, press '8'	Para linea de aviso secreto, marque '8'
Enter your PIN number	Marque su numero de identificación personal
Enter your area code and phone number	Marque su numero de telefono, incluya su codigo local o lada
You may hear silence during the acceptance of your call. Please continue to hold.	Vas a oir silencia mientras aceptan su llamada. Continue esperando por favor.

Inmate has ability to select the preferred language.	**Y**	Please see our comments below.

The Securus calling service default system setup provides message prompts in both English and Spanish. Inmates select a specific language at the beginning of the call process by dialing a single digit.

System Requirements

System de-activates the PIN feature by individual inmate telephone, groups of telephones and/or entire facilities.	**Y**	Please see our comments below.

With Securus' NextGen Secure Communications Platform™ (NextGen SCP™), each inmate telephone is individually programmed for Personal Identification Number (PIN) or non-PIN operation. This provides maximum flexibility in PIN placements. For example, a facility may wish to allow PIN operation in maximum security or long-term areas, while allowing an "all calls" option in overnight, work release, or trustee areas. The calling service has no limit or restrictions on the number of PIN or non-PIN inmate telephones operating at the facility.

Some facilities may choose to assign each inmate a unique PIN that they must enter before making a telephone call. PINs also provide an audit trail of the inmate who placed each specific call. PINs also allow the facility increased control over which inmates can call which numbers.

Each inmate is assigned a unique PIN, ranging anywhere from 4 to 16 digits. This range creates a maximum number of 9 billion PIN combinations.

Facilities can choose one of the following three primary modes to a single phone or group of phones in a facility:

- Mode 1, Open PIN
- Mode 1, Open PIN with Restrictions
- Mode 3, Closed PIN

Mode 1, Open PIN

This is the most basic mode of operations, and the simplest to administer. Each inmate is assigned a unique PIN to make a phone call. There are no individual phone number restrictions or calling lists in this mode. NextGen SCP applies global system calling restrictions to every call.

Mode 2, Open PIN with Restrictions

Mode 2 builds on the Mode 1 Open PIN feature and adds the ability to place call restrictions and limits on specific call types while allowing all other phone numbers to process as they would in an Open PIN system. Mode 2 restrictions can include the recording and alarming of

numbers and the use of the facility or global number lists for special circumstance numbers, such as attorneys and external crime tip numbers.

Mode 3, Closed PIN

Mode 3 provides the most restrictive calling privileges. It also requires the most administration of the three modes. Each inmate registers telephone numbers on their calling list. The total number of destination numbers available is unlimited. The facility determines the maximum number of telephone numbers each inmate can register. Telephone number registration includes the number, name of the called party, and their relationship to the inmate. The telephone numbers that each inmate registers are associated with the inmate's PIN and reside in the system. Only that PIN may validate calls to those numbers. Updating calling lists is a continuous process as inmates are booked into, or released from the facility, or as the inmates request changes to their calling lists. This type of control is usually recommended only for facilities with a low rate of inmate population turnover, or where such extreme security measures are desirable. Note that in a Closed PIN environment, the facility may choose to make certain telephone numbers commonly available to all inmates. The common numbers may be assigned global or facility accounts.

The system can set a maximum time limit for any call or all calls from an individual PIN or all PINs. Administrators can tie many additional restrictions to any PIN or telephone, or telephone number associated with a PIN such as:

- Time of day and/or day of week
- Maximum duration of a call for that PIN or phone
- Maximum number of calls or minutes an inmate may use per day, week, or month

The calling platform automatically manages all imposed calling restrictions.

Securus provides an automated PIN and PAN management system called E-Imports that can off-load facility labor required to enter PINs and PANs manually.

System restricts inmate calls to prepaid collect and normal collect calls. Prepay calling option must allow friends and family members the ability to establish an account directly with the inmate.	Y	Please see our comments below.

Securus offers friends and family members of inmates a wide variety of options to set up and fund prepaid accounts. Convenience drives account creation, and account creation drives more calling, so Securus has made the funding process easy. To create and fund a pre-paid calling account, friends and family members can:

- Call our Customer Service center and speak with a live operator
- Use our automated interactive voice response system
- Use our mobile-friendly website
- Fund accounts by mail

- - Visit one of more than 35,000 MoneyGram locations such as Walmart and CVS Pharmacy
- Visit one of more than 58,000 Western Union locations.

Securus currently does not charge a fee to establishing a prepaid collect account.

System has the capability to be deactivated (shut down), by County or Contractor staff, quickly and selectively, at an individual facility, partial facility or on a global basis and to restrict all PIN access.	**Y**	Please see our comments below.

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 with access to the Internet. This capability is available anytime, from anywhere, 24x7x365.

This function allows authorized users to kill all calls immediately or allow current calls to finish while not allowing any new calls.

Disabling Telephones
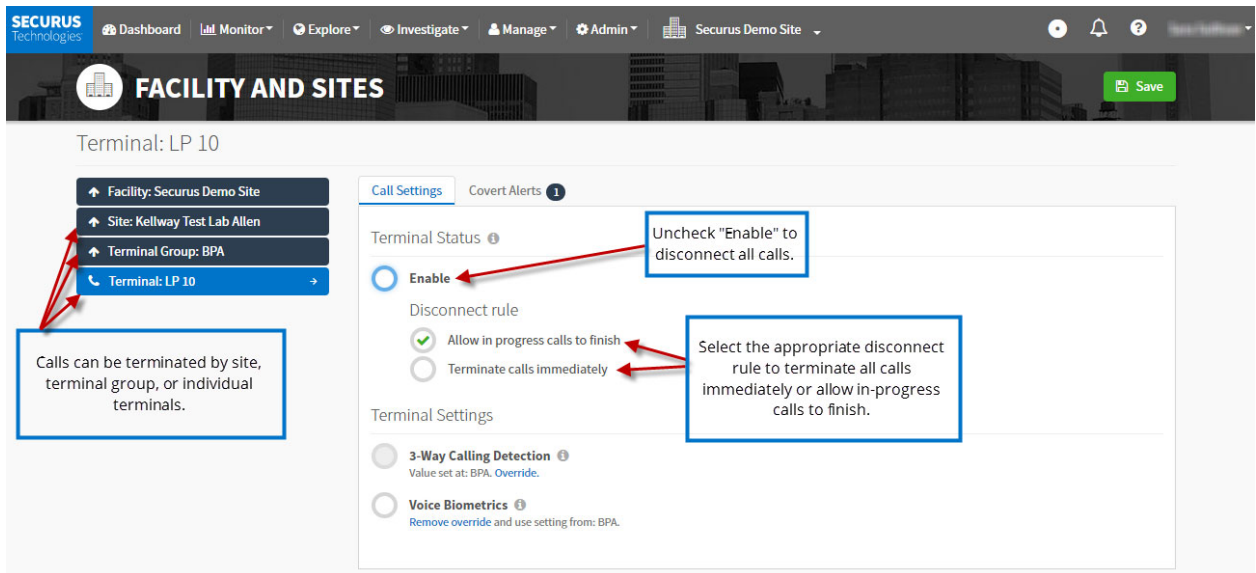
System provides the capability to flag any individual telephone number in the inmate's "Approved Number List" as "Do Not Record".	**Y**	Please see our comments below.

The Securus calling service can automatically bypass monitoring and recording special calls by designating phone numbers, such as those to attorneys, clergy or doctors, as "private."

The web-based user interface, NextGen SCP™ makes it easy for administrators to maintain this database and, as always, Technical Support is available 24 hours a day, seven days a week to assist with any service needs in maintaining this data. New numbers added are updated for all facilities within the county jail network.

To further maintain the integrity of attorney-client and other privileged calls, Securus offers an optional patented service called Two-Party Active Consent. Two-Party Active Consent ensures that both the inmate and called party give their "permission" to record and/or monitor their call.

System provides capability for assigning an inmate's phone access to an individual telephone or group of telephones so that the inmate's account may only place calls from those designated telephones.	Y	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) allows for the facility to restrict selected PINs to specific inmate phones.

Inmate telephones are usually consolidated into a group because housing units have more than one telephone. Securus has created another phone grouping method by associating and locking PINs to a group of phones based upon the housing unit identified during the enrollment.

When an inmate moves to another housing unit, the site administrator can easily change an inmate's location/housing unit through the inmate profile on NextGen SCP. Our data import application, E-Imports can also be used to automate this process.

System has a "smart fail-safe" power down service which is initiated upon alert by the uninterruptible power supply (UPS) that the UPS has switched to battery power because of a commercial power failure or irregularity.	Y	Please see our comments below.

Securus will maintain an uninterruptible power supply (UPS) backup for the equipment installed on County 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.

System maintains all currently ongoing telephone calls for up to ten (10) minutes while blocking any additional call attempts after any commercial power failure or irregularity.	**Y**	Please see our comments below.
The Integrated Access Device (IAD)s and uninterruptible power supply (UPS) units 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.		
The system is able to detect, notify, and prevent three-way or conference calls, except for those calls to attorney's or other approved numbers. Please provide a description of the process you have deployed on your platform and why you feel the technical approach provides the best 3-way detection solution.	**Y**	Please see our comments below.

The Securus calling service's three-way call prevention system is one of the best three-way call detection systems in the world and is protected by several patents. Independent tests have proven and certified the effectiveness of the Securus three-way call detection feature. With the release of the Securus digitally clean line transmission, our three-way prevention system has increased its capabilities to efficiencies never before achieved.
 	
 A facility can direct the system to do one of two things after detecting a three-way event:
 	
   ▪ Disconnect the call with messaging to inmate and called party, and note the event in the call record
   ▪ Mark the call in the call record with no interruption to the call
 	
 This feature prohibits a major fraud practice possible with other automated and live-operator systems. With traditional systems, inmates enlist the aid of an outside accomplice to "conference" them, via three-way calling, to an "unrestricted" line, bypassing system controls. Without three-way call detection, inmates have unrestricted access to the outside world, defeating the correctional objectives and policies of the institution and subjecting the public to inmate harassment and fraud. NextGen Secure Communications Platform™ (NextGen SCP™) is unique in its ability to detect and defeat an accomplice's attempt to activate the three-way call feature. NextGen SCP has the unique ability to disable three-way call detection on a particular number or groups of numbers, such as attorneys.
 	
 Detecting and preventing three-way or conference calls is a <u>very</u> important aspect of an inmate calling service and Securus leads the industry in this area. We would be pleased to demonstrate these tests and accuracies as needed for Dallas County. With an accurate three-way detection system, Dallas County can retain valuable investigative intelligence while curtailing revenue leakage from calls that should not be connected.		

With all three-way call blocking methods, the technology requires "specific usage finessing" as well as science. Securus will customize the configuration to adjust sensitivity parameters and thresholds for optimum performance.

The system prevents the inmate or called party from dialing extra digits after the call is accepted unless to authorized destinations.	**Y**	Please see our comments below.

The Securus calling service dual-tone-multi-frequency (DTMF) detection is a fraud prevention tool included with every installation. The system, by default, does not allow the inmate 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 calling service controls the call and buffers digits between pressing and sending. For example, when the calling service 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 digits. This makes it impossible for inmates to receive a secondary dial tone or call anyone by dialing additional digits after call connection.

The system allows extra digits to specified dialed numbers by the facility. Please describe process.	**Y**	Please see our comments below.

The Securus calling service can allow inmates to dial extra digits after call connection at a facility's discretion. Authorized users can use the calling service user interface to specify destination numbers that allow extra digits and specify the maximum number of digits allowed. The system will continue to detect and log the digits that an inmate presses, maintaining a complete record of the inmate's actions.

The system provides remote monitoring of Inmate calls and can send calls in progress to investigators.	**Y**	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) Live Monitoring has a call forwarding feature that allows authorized users to forward a live call in listen-only mode to an investigator or other authorized personnel. This provides real-time intelligence on an inmate conversation so that a real-time response can be coordinated when appropriate.

Forwarding a Call in Progress
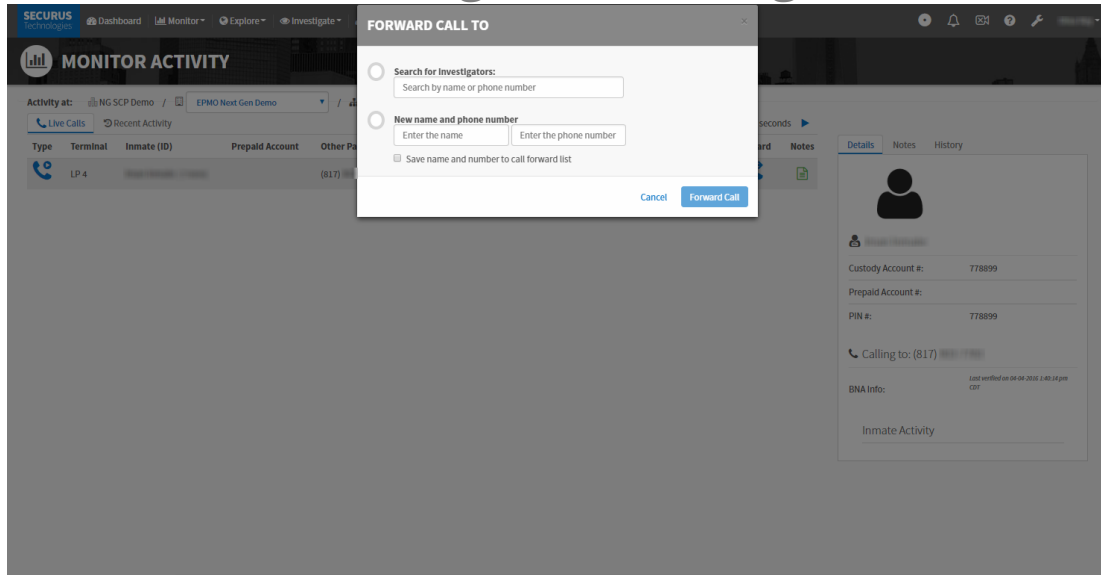
The system identifies the name of the facility and the inmate placing the call to the called party.	**Y**	Please see our comments below.

When the called party answers the phone, the calling service's advanced answer detection triggers the call acceptance voice prompt. The called party hears, "Hello, you are receiving a collect call from [inmate's name], an inmate at the Dallas County Jail. This call is subject to monitoring and recording."

The system prevents "Hook-switch dialing," and other fraudulent activities. Please describe.	**Y**	Please see our comments below.

A significant number of emerging threats are call diversion schemes that mask the true destination of calls. Securus provides the most advanced fraud detection capabilities in the correction industry. The Securus calling service continuously analyzes call data and system parameters to detect any anomalies, hardware failures, fraud indications, or unusual usage patterns. The system logs all telephone activity and statistically analyzes it to detect attempts at call forwarding, three-way calling, 'hookswitch dialling', 'black boxing', 'hacking', and other fraudulent telephone activities.

The calling service will provide, at a minimum, the following fraud prevention aids:

- Detection of three-way calls (patented)
- Elimination of secondary dialing
- Prevention of switchhook dialing
- Limits the number of times an inmate can redial a telephone number within a specific period (parameters to be set by the Department)
- Collection and prevention of DTMF
- Detection of call forwarding

The system, by default, does not allow the inmate to press additional digits. It uses our patented DTMF collection techniques to collect and only act upon digits that the system is expecting. Unlike traditional premises-based systems, the calling service controls the call and buffers digits between pressing and sending. For instance, when the system 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 inmates to receive a secondary dial tone or call anyone by dialing additional digits after call connection. This patented feature is only available on the Securus calling service.

The system allows call blocking of specific numbers for the entire agency and is configurable by each site.	Y	Please see our comments below.

The Personal Allowed Number (PAN) feature in the NextGen Secure Communications Platform™ (NextGen SCP™) provides an approved calling list for each inmate. Authorized Dallas County users can add both allowed and blocked numbers to the PAN list.

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 Dallas County) to be added to the inmate's PAN list automatically. The quantity of numbers allowed is configurable.   This is the most popular method of PAN administration. Numbers are loaded immediately without the intervention of staff.

- Inmate Managed PAN: Allows inmates 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 inmate 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 inmate's PAN list. No staff time is required to administer this process. With the extra step of validation, the county jail has maximum control of each added number.

- Manual PAN Entry: Authorized facility personnel can accept calling lists from inmates, 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 inmate's allowed number list.

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 system provides the ability to approve and disapprove specific phone numbers by telephone.	**Y**	Please see our comments below.

The SCP system provides the ability to approve and disapprove specific phone numbers by telephone. We can turn on a phone group by the phone level which turns on a global list for the phone.

The system has the capability to suspend an inmate privileges from placing a call and set a beginning and end date without the need to manually re-enable privileges.	**Y**	Please see our comments below.

As inmate 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, Dallas County may use call restrictions to regulate inmate access to ensure access by all inmates.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides calling restrictions to give Dallas County control of calling activity at the inmate, 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 minutes 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.

The system allows the inmate to record their name one time and store this recorded name for all future calls.	**Y**	Please see our comments below.

The Securus calling service allows inmates to record their name, associated with their custody account and PIN, once. The recorded name is then played on all calls the inmate makes with their PIN. If PINs are not required, the system will ask the inmate to state their name on each

call, the recording of which is then played to the called party. All pre-recorded inmate names are to be played to the called party when announcing the call.

For maximum flexibility, this function is configurable to use pre-recorded names, or not, per inmate, facility, and customer level. A pre-recorded name may also be reset, forcing the inmate to record their name again.

The system provides a real time validation and prevention of calls that are forwarded. Please provide a description of the process you have deployed on your platform.	**Y**	Please see our comments below.

Securus uses industry leading voice biometric technology for real time validation and prevention of call forwarding.

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 was initially developed by JLG Technologies, which Securus acquired in 2014.

IPRO includes a wide range of tools that identify voices by name, deter inmate PIN abuse, and provide leads for investigators pursuing illicit activity carried out over the inmate telephone system.

Investigator Pro is a Securus solution and Securus manages the solution roadmap. It is fully integrated with the Securus call 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 inmate 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 inmates by name no matter how many inmates 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 inmates.
- Voice search for inmates and called parties on both sides of calls using voice samples taken from either side.

- Inmate-to-inmate communication reporting through the seamless integration of ICER™, the Inmate 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 inmates and phone numbers, and to search on that information.

Investigator Pro Capabilities

Inmate Enrollment Method Choices

The agency can choose supervised or covert enrollment to create a voice-ID/PIN pair for each inmate. It can switch from one method to the other at any time. It can also choose to enroll existing inmates covertly and new ones through a supervised process.

Supervised enrollment creates a staff-verified voice sample for each inmate ID/PIN. Investigators then have a known audio file of each inmate to play. In covert enrollment IPRO learns a voice and associates it with an inmate ID/PIN. There is no staff involved and inmates are not asked to record their voices. Inmates 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 inmate begins a call IPRO verifies in real time that the inmate'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 inmate 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 inmate(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 inmates.

Voice Search

The investigator can search for calls that have a particular voice on the inmate or called party side of the call. He can do a voice search by inmate name, inmate 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, inmates, or phone numbers involved.

IPro Voice Search

Voice search results include facts about the voice and links to the relevant calls, inmates, 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 inmate names, calls and voices further.

Inmate-to-Inmate Communication Reporting

IPRO detects inmate-to-inmate calls no matter how or where they happen because ICER, the Inmate Intercommunication Evaluation and Reporting System, is integrated into Investigator Pro. ICER finds these calls whether the inmates are within a facility or in different facilities across the country, and whether the two inmates 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 inmate searches, and in the call player.

IPro Quick Find

An inmate search from the home screen gives valuable information, including details about inmate-to-inmate calls.

Call Player

Investigator Pro has a full-featured call player that makes listening to inmate 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.

IPro Call Player
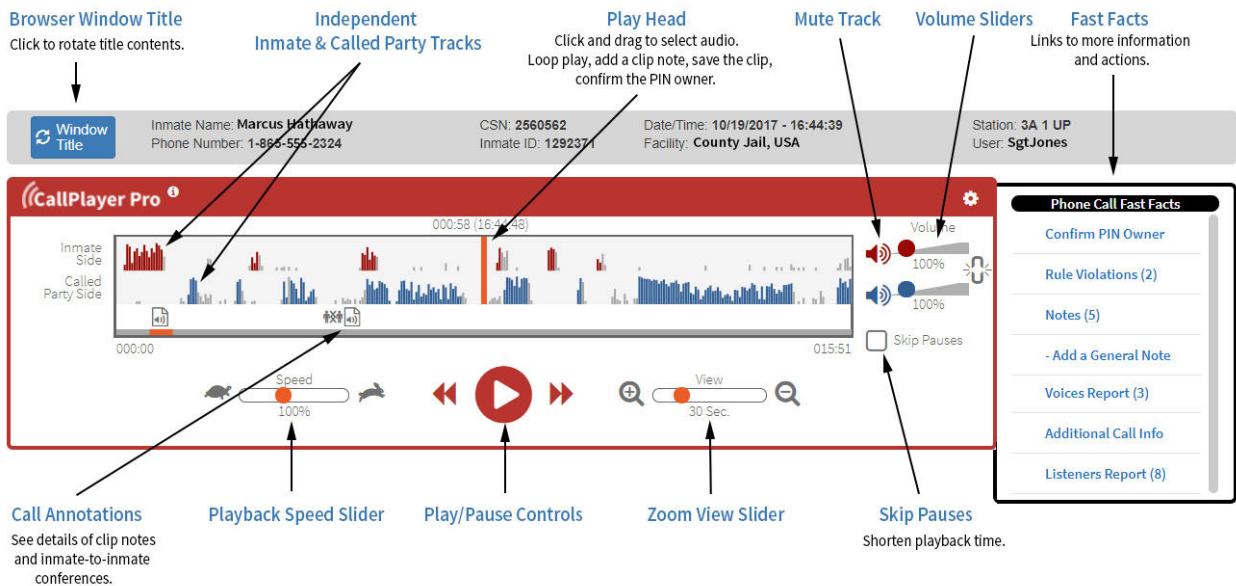
Investigator Pro's call player makes listening easy and efficient. The Fast Facts box beside it has links to more information and actions for the investigator.

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, inmates, voices, and telephone numbers. Investigators can search the database by criteria such as inmate name, inmate ID, date range, saved voice sample, custom High Interest Group label, inmate-to-inmate (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 inmates 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 inmates 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.

The system has the capability to move an inmate or group of inmates from one facility to another without the need to re-enter information.	Y	Please see our comments below.

An easy-to-use PIN transfer module is available for site administrators to transfer a single PIN or a group of PINs when inmate(s) are moved to another housing unit. This process may also be automated through our data import process.

The system allows department personnel to assign surveillance alerts by individual inmate PIN or dialed number. These alerts should include, but not be limited to, the following features: **a. Alert to an investigators cell phone or any direct dialed number.** **b. Allow real time listening of conversation in progress.** **c. Allow the ability to disconnect the call in progress.** **d. Allow barge-in and talk capabilities and return back to listen only mode.** **e. Allow investigators to assign and enter a PIN when alert call is received.** **f. Allow the ability to hide the alert from other authorized users that have access to the system.** **g. Allow investigators to enter optional e-mail address to receive notification of calls by inmates and to dialed numbers that are under surveillance.**	**Y**	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) includes the Covert Alert feature that will call an investigator at a designated phone number to offer real-time monitoring of a call to a watched number or a call that is placed by a watched inmate.

Covert Alerts can be set through the inmate information page or through the Covert Alerts administration page.

Creating an Alert Notification

Covert Alert can bridge a call to an authorized remote number for dialed numbers, phones, or inmate 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 inmate, or to a phone number 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 send emails to the investigator(s) with information about a Covert Alert call including date, time, inmate PIN, originating telephone, and dialed number immediately after the called party accepts the call. The following figure provides a sample e-mail alert:

Alert Notification E-Mail and Text Message
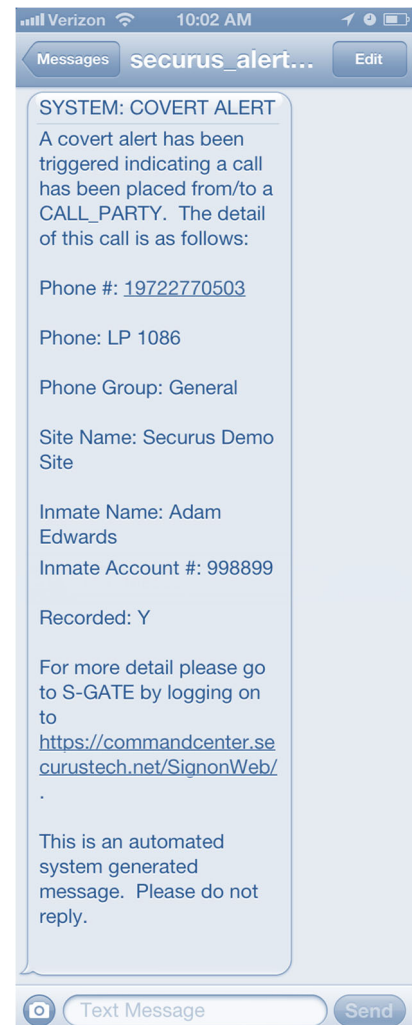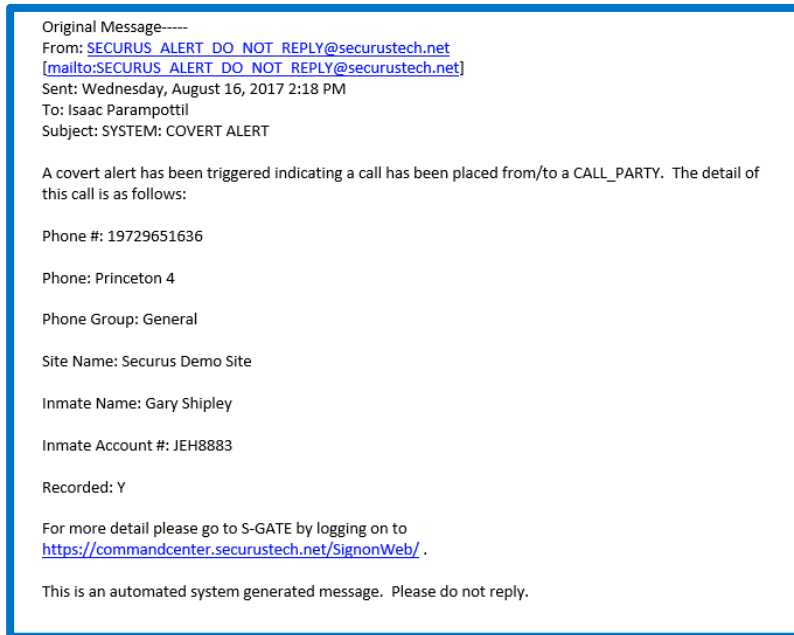
Investigators can also choose to receive a covert alert via text message. The text message includes the date, time, inmate PIN, originating telephone, dialed number, and an indication if the call has been recorded. The preceding figure provides a sample text message alert.

Additional Security Feature

For extra security, Coverts 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 inmate at Dallas County Jail. 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 inmate 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.

Covert Alert Call Detail Report

The system provides the ability for investigators to attach case-notes to a call and view it from a report such as a call detail report.	Y	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) allows authorized users to add notes and tracking numbers to communication detail records associated with recordings. This feature is accessed via the notepad icon in the communication detail record and allows authorized users to add notes—such as a tracking number, gang affiliation, duration into the call, and any other notes associated with the call—to an inmate communication. This feature also allows authorized users to either keep the note private to their investigation or to share the note with other users. From the Notes tab on the communication detail record, users may also view previous public notes associated with the communication.

Adding a Note to a Communication Detail Record

Authorized Dallas County users can search for notes through the Advanced Search function. This feature allows searches on the CDR tracker number, note type (no notes, my private notes, or shared notes), or keywords—such as a gang affiliation—within the CDR tracker notes. As with every report in the NextGen SCP user interface, the search results are exportable to Excel, PDF, or CSV.

The system provides the ability for investigators to perform analytical data research of inmate calls and numbers called.	**Y**	Please see our comments below.
Securus is pleased to offer Dallas County our cutting edge THREADS Analytical Platform. Please see **Exhibit C** for an overview of the THREADS capabilities.		
System provides the capability to identify calls to Cell Phones and provide the following investigative capabilities: **a. Display and store cell phone termination locations at call acceptance and call end** **b. Ability for user to create user-defined geofences through which the user can specify a mileage radius around a facility address or around a known point of interest such as a drug house.** **c. Set up Covert Alerts to notify the user when a call is placed to a cell phone within the defined GEO fence.** **d. Provide real time notifications of calls terminating within a GEO fence.** **e. Display location of cell phone calls on an active integrated map.** **f. Obtain location of a single phone number in real time from the wireless carriers when uploading a warrant or court order**	**Y**	Please see our comments below.
While our system is developed with these capabilities, we are not currently offering the products dependent upon location-based data from cellular providers. All of the major cellular carriers have publicly announced that due to consumer privacy discussions with Congress and the FCC they are not making such data available. This applies to all corporations and no one in the industry should be able to provide this service until such time as Congress and the carriers finalize discussions to maintain consumer privacy.		
The system allows investigators to share notes about a call or keep them private if they choose and use text entries, such as a case number or a specific gang affiliation in the case-notes as the search criteria to retrieve specific case-notes with the associated call detail record as well as providing the ability to do a full text search against the notes attached to the call.	**Y**	Please see our comments below.
Investigator Pro lets investigators add their own information to the database and find it in searches later. They can tag inmates 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.		

The system protects the recording from being purged when the client storage policy expires by allowing the investigators or other authorized staff to extend the expiration date of the associated call or download.	Y	Please see our comments below.

NextGen Secure Communications Platform™ (NextGen SCP™) can be used to extend the expiration of a recording. At times, investigators may not want recordings from active investigations to be purged from the system—regardless of the recording retention policy in effect. Authorized users can protect a recording from being purged by extending the expiration of the call by 30, 60, or 90 days by clicking the Extend Time icon.

In addition, NextGen SCP™ allows authorized users to copy recorded conversations and visitation sessions to an external media device connected to the user's PC, such as CD, DVD, mp3 player, or USB drive. This feature facilitates easy sharing of recordings for investigative or court purposes. 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.

The system has the capability to download a call directly from the call detail report as well as allowing authorized staff to copy multiple calls to a folder for download at a later time with the option to e-mail a link to calls resident in the folder. The system allows recordings to be downloaded in the recording's native format as well as .WAV and .MP3 formats and allows recordings to be downloaded as a compressed file.	Y	Please see our comments below.

NextGen Secure Communications Platform™ (NextGen SCP™) allows authorized users to copy recorded conversations and visitation sessions to an external media device connected to the user's PC, such as CD, DVD, mp3 player, or USB drive. This feature facilitates easy sharing of recordings for investigative or court purposes. 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.

Downloading Communication Events to External Media
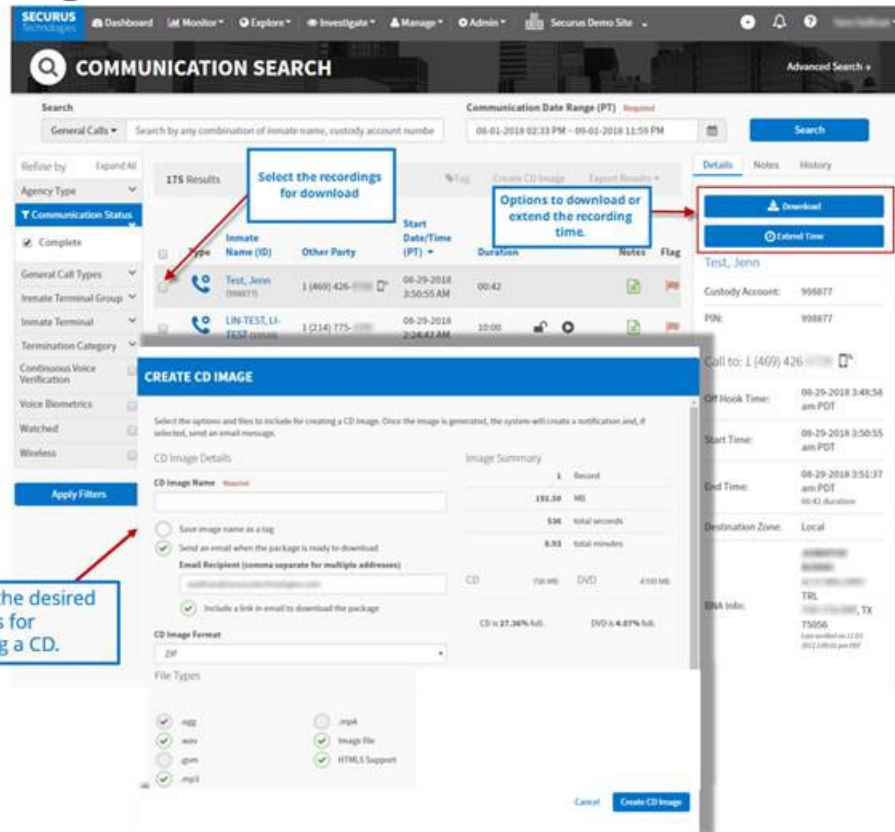
When downloading communication recordings from NextGen SCP, users create a CD image. This allows users to add multiple recordings to an image, select the file type, view file size, and select an email notification when the CD image is ready to download. When a CD image is downloaded, any associated communication Note entries can also be exported to the CD image.

Securus allows investigators to access to all investigative tools via the NextGen SCP user interface. Investigators can search for calls using criteria such as called party, calling phone, date, time, PIN, account, duration, and locations. Searches can be across a single site or group of sites based on the user's security authorization. Searches can include all call attempts or just completed calls. The search results provide detailed information about the call and indicate the presence of a recording.

Investigators can listen to recordings, within the limits of their security access, using the powerful call player integrated within the NextGen SCP system. The player includes easy-to-use search capabilities, and features such as pause and fast-forward. A visual waveform helps investigators bypass areas of limited talk time and to quickly identify particular events.

When listening to a recording, the audio is "streamed" to the user's computer. This safeguards the original recording. Chain of Evidence safeguards prevent access to the original recording to eliminate any chance of intentional or accidental manipulation or deletion.

Network and Infrastructure Requirements		
System includes a monitoring component that is capable of being accessed from a vendor provided dedicated monitoring terminal and/or through a vendor provided secure Internet connection from desktop, laptop or remote means by authorized County personnel who have appropriate security clearance.	Y	Please see our comments below.

The NextGen SCP Monitor Activity function allows for real-time monitoring of calls in progress via a multi-media PC workstation. Facility personnel (with appropriate privileges) can monitor live calls by highlighting the call in progress and clicking on the

handset icon ( ). This process is undetectable by the inmate or the called party and does not disrupt the recording process. Concise descriptions of activity appear for each phone in use. For example, the system shows the inmate name and ID, dialed number, start date/time, and duration. NextGen SCP also shows whether the call was accessed, call notes that may be available, or whether the call is flagged. Clicking on a call opens a side-bar with additional details of 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 language of the call prompts. This side-bar also provides an easy method to download the call recording, extend the expiration date of the call recording retention period, add a note to the CDR, or view the recording access history—all with a single mouse click.

NextGen SCP can also automatically eliminate all monitoring or recording of special calls, such as calls to legal counsel, by designating the number as a "private" number. NextGen SCP prevents all unauthorized attempts to listen to private calls—the user interface displays a distinct call icon to indicate that there is no recording to play for private calls. The call record also lists the call as "private" on the user interface.

Indicate the numbers of authorized users that will have access to the monitoring capability.	Y	Please see our comments below.

The number of authorized users is only limited to the number authorized by the County.

System capable of interfacing with network services provided by local exchange carriers as well as inter-exchange carriers. This includes analog, digital or VOIP facilities.	Y	Please see our comments below.

NextGen SCP is capable of interfacing with network services provided by local exchange carriers as well as inter-exchange carriers. This includes analog, digital or VOIP facilities.

List the types of network services to which the system will interface and the purpose (use of a specific application) of such services for Dallas County.	Y	Please see our comments below.

Through our partnership, we've developed specific ways to handle day-to-day issues. We've integrated processes, systems, and applications. We know how to work with your existing vendors and equipment. By selecting Securus, you will avoid the difficult process of re-mapping, re-engineering, re-developing, and re-training integration links. Vendor continuity prevents system interoperability issues during the transition.

Securus has proven experience with Integration. Securus currently integrates with more than 110 different vendors worldwide and more than 60 independent, facility-owned systems and shared databases.

Securus has a dedicated integration department that integrates various systems and products in the corrections environment. This dedicated integration department allows Securus to deliver fast and flexible solutions for our customers. The Securus technology has the flexibility to work with facility-owned systems, jail management system (JMS), commissary, banking, and kiosk vendors. Securus will fully cooperate with your facility and your vendors to automate systems and ensure system interoperability.

The most common technologies Securus uses include SOAP Web Services, HTTP, FTP push or pull of files in any textual format, JSON, XML-RPC, and TCP Sockets. All of these methods integrate over secure connections.

Securus can modify your data format for migration into our platform, without costly code modifications. Securus integration engineers consult with facilities' IT departments or system providers to determine the best integration strategy for each specific application.

Securus Integration Process

Securus' dedicated integration team designs, develops, tests, and implements all custom integrations with corrections industry vendors and banking systems to deliver fast and flexible solutions for our customers. This process is part of the overall project plan for the installation of the NextGen Secure Communications Platform™ (NextGen SCP™). Major milestones include:

- Collect preliminary needs/requirements
- Contract signed
- Finalized requirements document
- Approved scope statement
- Finalize design document
- Schedule customer implementation
- Develop custom integration solution

- Test custom integration solution
- Implement custom integration solution
- Customer approval and sign-off

Database Requirements

System maintains a data record of all transactions made (attempted calls, completed calls, blocked calls, etc.) through the inmate telephone system be maintained in a database for monitoring and analysis of inmate telephone calls.	**Y**	Please see our comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) provides authorized personnel and investigators single-point access to research Dallas County communication records and recordings.

Users can specify search criteria, such as called party, calling telephone, date, time, PIN, custody account number, duration, and location, and search across a site or group of sites based on their security authorization. NextGen SCP searches communication 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 communication 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 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.

System alerts staff of possible trends with inmate calls that could jeopardize the security of inmates, staff, or facilities.	**Y**	Please see our comments below.

Threads, ICER and IPro contain a variety of mechanisms and reports to alert staff of possible illegal or dangerous activity**.**

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.

THREADS automatically imports information from NextGen SCP's telecommunications database, inmate information from JMS, and financial data. Multiple sources of data and databases are combined into the THREADS' analytic framework to reduce the time required for investigators to find suspicious patterns. Such patterns may be an indication of planning or commissioning crimes.

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 inmate names, calls and voices further.

Inmate-to-Inmate Communication Reporting

IPRO detects inmate-to-inmate calls no matter how or where they happen because ICER, the Inmate Intercommunication Evaluation and Reporting System, is integrated into Investigator Pro. ICER finds these calls whether the inmates are within a facility or in different facilities across the country, and whether the two inmates 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 inmate searches, and in the call player. Please see a sample ICER report below.

ICER Event Report

Event Identified On: Sep 23, 2019
10:00 am (EDT)

An Inmate Inter-Communications Event has been detected involving an inmate at your facility. The details of which follows below:

Inmate	Inmate 1 - name redacted	Inmate 2 - name redacted
Agency	DALLAS COUNTY TX	FANNIN COUNTY JAIL TX
Site	Dallas County Lew Sterrett North Tower, TX	Fannin County Detention, TX
Inmate ID	Inmate 1 - ID redacted	Inmate 2 - ID redacted
Called Number	14693092378	18027290073
Station Name	3 West-T03 PH2	B13 Left
Call ID	12809430922	12809416934
Call Start Time	Sep 22, 2019 09:01 pm (EDT)	Sep 22, 2019 09:03 pm (EDT)
Time into Recording (H:M:S)	03m:27s (207 sec)	01m:43s (103 sec)
Duration of Event (H:M:S)	12m:49s (769 sec)	12m:49s (769 sec)

System generates/creates a centralized system database that provides the capability for every call in and out of the system to be recorded with a transaction record that includes, at a minimum, a recording of the telephone call in a .wav or other format.	Y	Please see our comments below.

All non-private calls are recorded and maintained in a centralized database for easy search, retrieval, listening and download.

The integrated calling services recording application works independently, so there is never a need for integration of a third-party manufacturer's product. This allows the facility to deal with a single vendor if any issues arise. NextGen SCP can also be used to burn the information to a digital file that can be transferred to CD or DVD for additional back up, if necessary.

The system records the entire conversation from call acceptance to termination. And all calls are associated with a call detail record.

Database is maintained in such a manner as to allow authorized personnel the capability to review and monitor inmate call data regardless of which County facility is housing the inmate.	Y	Please see comments below.

NextGen SCP is a web-based centralized system that enables authorized personnel to review and monitor inmate call data regarded of which County facility is housing the inmate.

Database has the capacity to contain multiple data fields.	Y	Please see comments below.

Our SCP database has the capacity to contain multiple data fields.

System provides the capability for Dallas County to download reports from the database, through secured internet access.	Y	Please see comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) has a dedicated report writer that provides investigative information based on the communication detail records. This sophisticated reporting tool provides a reporting interface into all communication activities.

Reports can be generated online and exported in the following formats:

- Microsoft® Excel
- CSV (Comma Separated Values)
- Adobe® PDF

Authorized users can search and analyze communication details on all communication events through NextGen SCP. These details include date, time, duration, telephone number, origination, destination, inmate ID, termination reason, and more.

NextGen SCP retains communication details on all communication attempts. Users can customize the standard reports by varying search criteria, such as date range, facility, or call length.

NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on the following criteria options:

- Date range
- Inmate identifier, such as ID, PIN, and first or last name
- Communication type (calls and video)
- Communication status (complete or incomplete)
- Destination number (partial or full number entry)
- Call type
- Three-way or Remote Call Forwarding detected, watched status, wireless indicator, or Continuous Voice Identification
- Visitor and visit type (SVV)
- Visitor contact number
- Visitor identifier, such as first or last name, email, and visitor ID
- Per phone/terminal, per location, and per offender
- Number restriction and/or status assignment
- Broad search with no data entry
- Suspected fraudulent call activity
- Prepaid account number
- Destination zone (local, interLATA, interstate, intraLATA, international)

Sample Communication Detail Results Screen

Access provided to the database through a secure web server so Dallas County can retrieve and download and further analyze certain data. The response should detail how the Contractor proposes to provide this access.	Y	Please see comments below.

NextGen Secure Communications Platform™ (NextGen SCP™) uses security roles to determine user permissions. They define what actions a user can and cannot do within the system. NextGen SCP contains default security roles, identified by the eyeball (👁) icon. While these predefined roles cannot be modified, they cover many customers' needs for granting access and denial rights based on common job functions.

NextGen SCP provides more options for Dallas County to further customize access privileges by allowing authorized administrative users to either create a new user-defined role or create a new role using an existing role as a base and further modifying it. The user-defined role can be customized to meet Dallas County's specific needs when a default role does not. These roles are identified by the pencil (✏) icon.

In addition, the Dallas County administrator can assign multiple roles to a user to tailor their access to exactly what is needed. This provides virtually unlimited options for customizing users' access.

Sample Security Roles

Password Policies

NextGen SCP uses strong passwords that require users to update passwords regularly. Passwords must comply with the following rules:

- 8 – 12 characters
- No spaces
- Cannot contain the user's first or last name
- At least three of the following types of characters must be used:
  - English uppercase letter

- o English lowercase letter
- o At least one number
- o At least one special character

Passwords can be configured by location, days to expire, and even the number of password cycles before password reuse. Additional configuration options include reminders for password expiration and minutes of allowable inactivity before session timeout.

The "Forgot Your Password?" feature available from the login screen offers online support for users who have forgotten their password or for those who did not change their password before expiration. System security requires users to provide the correct answers to preset questions before their password can is reset. Once a new password is created, NextGen SCP emails confirmation to the address linked to the user ID.

System capable of recovering all inmate telephone data for all locations, to the point of full service operation, using a data backup.	Y	Please see comments below.

Backups alone are not enough to adequately protect yourself from the many threats to critical data. A daily backup of data using the same single data cartridge will not protect against many types of disaster.

Securus uses a digital backup system to minimize the cost of ownership related to data cartridges and tape. By incorporating a mix of daily, weekly, monthly, and quarterly backups, facilities will have a complete history of their CDRs and visitation records from various points in time.

Communication recordings are available for playback immediately. As an additional layer of protection, Securus replicates communication recordings between its Dallas and Atlanta data centers.

System performs all service and database back-ups and archiving.	Y	Please see comments below.

Securus automatically services, monitors, backs up and archives all data.

Contractor provides all archival hardware, supplies, network and recovery procedures that will ensure that no data is lost.	Y	Please see comments below.

Securus provides all archival hardware, supplies, network and recovery procedures that will ensure that no data is lost.

Database has duplicate data storage devices with automated fail- over and automatic reestablishment of the duplicate databases upon replacement of the failed storage device and shall be equipped with automated fire detection and suppression equipment.	**Y**	Please see our comments below.

Securus operates and maintains two major data centers networked to the equipment installed on Dallas County premises. Each data center has an uninterruptible power supply (UPS), and a generator to provide maximum network uptime. The traditional data circuits (MPLS, Frame Relay, VoIP) all have dual connectivity feeds to/from the telecommunication carrier to each of our data centers.

Our data centers are equipped with automatic fire detection and suppression equipment.

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.

Data Center Power Conditioning

The uninterruptible power supply (UPS) system filters, spikes, sags, surges, transients, and all other over/under voltage and frequency conditions, providing clean power to connected critical loads. 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.

Diesel Generators Facts:
- Multiple diesel generators provide standby power to the data center. The fuel is located within the facility.
- Five underground fuel tanks store 70,000 gallons of diesel on-site.
- Both sites test the generators on a weekly basis and alert central station for any test failures.
- Both sites have multiple fuel vendor agreements.

System provides that all data be recorded with a historical transaction record and stored/archived for retrieval/backup in a database that is available when requested.	**Y**	Please see our comments below.

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. Traditional premises-based platforms use local hard drives that may fail and are susceptible to local disasters. Premises-based systems needed manual backup schemes that are unnecessary with NextGen SCP. 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.

Current and historical call detail data files retained for a period of three (3) years by the Contractor.	Y	Please see comments below.

Current and historical call detail data files will be retained for a period of three (3) years.

Archived/historical information available at no charge to Dallas County after termination of the contract. All data shall remain the property of Dallas County.	Y	Please see comments below.

Securus will allow Dallas County to access and download archived/historical information at no charge after termination of the contract. All data will remain the property of Dallas County.

System Calling Protocol Requirements

System only initiates calls in a "collect call" mode (prepaid or normal collect calls) to land lines (non-cellular) and to cellular phones (prepaid) with Billing Number Addresses (BNA's).	Y	Please see our comments below.

NextGen SCP only initiates calls in a "collect call" mode (prepaid or normal collect calls) to land lines (non-cellular) and to cellular phones (prepaid) with Billing Number Addresses (BNA's).

Call set-up time does not exceed six (6) seconds from completion of dialing to first ring.	Y	Please see comments below.

NextGen SCP ensures call set-up time does not exceed six seconds from completion of dialing to first ring.

System does not provide a second dial tone to an inmate telephone without the inmate hanging-up the telephone receiver after the first call is completed.	Y	Please see comments below.

NextGen SCP does not provide a second dial tone to an inmate telephone without the inmate hanging-up the telephone receiver after the first call is completed.

Each call placed through the system is electronically identified by the system as being a call originating from a Dallas County Jail in 100% of the cases with or without the accompanying inmate PIN.	Y	Please see our comments below.

Called parties can identify calls from an inmate at a Dallas County facility through their caller ID. Collect call charges from the Dallas County facility on phone bills include the contact information for the Securus customer service center, Securus Friends and Family Call Center

(SFFCC). Should the friends or family members have any questions regarding their collect call charges, they can use this contact information from their bill to contact SFFCC.

Caller ID

The default configuration for caller ID shows Securus Correctional Billing Services toll-free number, not the Dallas County Facility. Additional configuration options include:

- Caller ID can display a number supplied by Dallas County; the name associated with that number through your local telephone provider will also appear on the caller ID.
- Any other number can be assigned to display on calls from Dallas County Facility, however unless associated with a name through a local telephone company, only the telephone number will appear to called parties, not a name.

Selected phones can be programmed to place calls without PINs.	**Y**	Please see our comments below.

Securus can configure selected phones to operate with PINS.

System provides the option of either English or Spanish voice messages or prompts as programmed through a single prompt at the beginning of each call.	**Y**	Please see our comments below.

NextGen SCP provides the option of either English or Spanish voice messages or prompts as programmed through a single prompt at the beginning of each call.

The language provided is controlled by the inmate's account information. Note: Contractor shall provide a list of available languages.	**Y**	Please see our comments below.

The Securus automated operator uses clear, concise, professionally recorded voice prompts to assist the inmate 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. Calling services can be configured to provide prompts in as many as nine languages.

Some examples of languages that Securus has implemented in the past include:

- English
- Spanish
- French
- Haitian Creole
- Hmong
- Navajo
- Polish
- Portuguese

- Russian
- Somali
- Vietnamese
- Chinese Mandarin

After the language prompts are set up in the calling service system, inmates 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 inmate. This fraud deterrent feature eliminates inmate attempts to confuse called parties with a language they do not understand.

Securus will also provide at each inmate telephone location durable printed dialing instructions in English, Spanish, and the other languages specified by the County. These instructions explain the process in an easy-to-read manner for all inmates.

As a security measure, Securus will use materials and techniques appropriate for the corrections environment.

· **System provides automated notification to an inmate of the call status (i.e., ringing, busy, etc.). This notification may either be in the form of ringing, busy tones, Special Information Tone (SIT), or appropriate recorded messages.**	**Y**	Please see comments below.

NextGen SCP will provide an automated messages informing the inmate of the status of their call.

System allows the inmate to hear the processing of the placed call to determine if a SIT with message or an answering device (i.e., answering machine, voice mail, etc.) has answered the call.	**Y**	Please see comments below.

The Mute Acceptance and Call Progression feature in Securus' calling service can be configured to either allow the inmate to hear or mute call progression.

In the un-muted form, the inmate will hear the call setup and processing to determine if a busy, reorder, or SIT tone with a message played, or if an answering machine, voicemail, or other automated device answers the phone.

For security purposes, the system always mutes the inmate's line until the system detects positive acceptance key press by the called party. The inmate can never speak to the called party until the end user positively accepts the call. This applies to both collect and prepaid calls.

Allow incoming callers the option to leave a voice mail for offender (recorded and stored).	Y	Please see comments below.

Voice mails may be left for inmates which will be recorded and stored.

At no time does the system allow the inmate to speak (restricted voice channel) until the called party has accepted the call.	Y	Please see comments below.

The Mute Acceptance and Call Progression feature in Securus' calling service can be configured to either allow the inmate to hear or mute call progression.

For security purposes, the system always mutes the inmate's line until the system detects positive acceptance key press by the called party. The inmate can never speak to the called party until the end user positively accepts the call. This applies to both collect and prepaid calls.

System has the capability of announcing to the called party the name of the calling inmate, informing the called party how to accept calls and announcing to the called party the call charge rate, prior to acceptance, when a call is placed. The activation or deactivation of these features is determined by Dallas County.	Y	Please see comments below.

The Securus calling service includes an Interactive Voice Response (IVR) system that provides Automated Operator Services (AOS). This automated assistance uses clear and concise, professionally recorded voice prompts to establish call acceptance and to assist inmates and called parties throughout the calling process.

When the called party answers the phone, the calling service's advanced answer detection triggers the call acceptance voice prompt. The called party hears, "Hello, you are receiving a collect call from [inmate's name], an inmate at the Dallas County Jail. This call is subject to monitoring and recording." 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."

Additional options provided by AOS include:

Available Options to Called Parties	**Available Options to Inmates**
• Request a rate quote • Hear the name of the facility and inmate calling • Accept or reject the call	• Listen to prerecorded announcements • Choose to place a collect or debit call; if debit, PIN entry is requested, the inmate hears the available balance in their account and the cost of 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 • Choose to hear the prompts on the system in English, or the language selected by the inmate (if configured for this option) • Pay for the incoming call with InstantPay (if available) • Hear optional marketing message (by request of Dallas County) • Block their number prior to accepting a call using the system's Perma Block technology*	• 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 inmate call time limits based 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 marketing message (by request of Dallas County)

*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 inmate 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.

If the party called does not accept a call, or if no one answers the call, the system informs the inmate of the situation and does not simply disconnect the call.	**Y**	Please see comments below.

NextGen SCP informs the inmate why the call was not completed before disconnecting.

System allows for a minimum "ring time" prior to disconnecting the inmate call.	**Y**	Please see comments below.

NextGen SCP can be programmed to allow a minimum ring time prior to disconnecting.

System has the capability of allowing a called party to deny all future calls of a particular type from an inmate and shall provide notice to the inmate placing the call of such action.	**Y**	Please see comments below.

NextGen SCP has the capability of allowing a called party to deny all future calls of a particular type from an inmate and shall provide notice to the inmate placing the call of such action.

System has the capability to accept the called party's response via Dual Tone Multi Frequency (DTMF) Touch-Tone Pad input from the telephone and voice response.	**Y**	Please see comments below.

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 inmate'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.

System has the capability to interject messages into a telephone call at random intervals (i.e., "this call is from a Dallas County Jail", "remaining time is _minutes" etc.).	**Y**	Please see comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) calling services allow voice overlay messages throughout the call as an additional fraud protection feature. An example of a voice overlay message is "*This call is from a correctional facility.*"

Voice overlays can be configured to:

- Play the message randomly or a fixed number of times per call
- Set the number of times to play the message during the call
- Change the time between when the message plays and when to play the next message
- Set the delay between call acceptance and when to play the first message
- Set the amount of time before the end of the call to play the message

List any other functionality provided by the system.	**Y**	Please see comments below.

NextGen Secure Communications Platform (NextGen SCP™) is a single platform for managing, researching, monitoring, investigating, and exploring information through Securus products and services. Dallas County will benefit from NextGen SCP's fast and efficient access to communication data, increased security, unparalleled control over inmate communications, and real-time alerts.

NextGen SCP, our newest platform, has been designed specifically for the corrections customers who use our products on a daily basis. It is a powerful multi-product technology solution that is squarely focused on putting information in the hands of our customers when and where they need it.

New technologies at the heart of the platform make NextGen SCP more intuitive, more efficient and much more responsive – and lay the foundation for future innovations. NextGen SCP refines the features Dallas County use every day and adds new innovative features and functionalities. It's inmate communications management at its highest level yet.

With NextGen SCP, Dallas County will:

- **Enjoy refinements in the user interface**
  - Easily maneuver with action-based navigation
  - Use Google-like single entry search fields
  - Get more information with less effort in a shorter amount of time

- **Interact with information immediately on the new dashboard**
    - See summary overview of facility communications immediately upon login
    - Gain quick access to BNA and PAN frequency search functionality
    - Access upcoming video visitations
- **Improve your records search experience**
    - Increase the speed from request to data easing the burden of investigative time
    - Get multi-product results with a single search
    - Take advantage of the integrated new backend technologies allow for analysis when data is ingested and stored for faster, more efficient accessing
    - Run reports in the background while you continue to work and be notified when they are ready
- **Step up to the new standard for overseeing inmates**
    - Get comprehensive overview of inmate communications with an activity stream listing past, present and future events
    - Manage settings and suspensions for calls, video and other products independently
- **Manage video visitations in the same platform as calling**
    - Get information about and manage visitors using the new Contact Profile page
    - Set up facility or site level approvals to suit your needs
    - Conveniently approve visits either first visit only, every visit or automatically
- **Upgrade the access and security of users**
    - Provide users with only the information they need to see, edit, manage or interact with
    - Easily craft custom task-based permissions for users
    - Protect your facility access with required strong passwords and enforced regular password updating
    - Provide facility affiliated personnel with access to video visitation

The Contractor can maintain a grade of service of P.01 (one caller out of 100 will be blocked) regardless of the number of telephones, facilities, application or users.	**Y**	Please see comments below.

Securus can maintain a grade of service of P.01 (one caller out of 100 will be blocked) regardless of the number of telephones, facilities, application or users.

System Disaster Recovery		
System includes a written Disaster Recovery Plan and Continuity of Operations Plan and associated internal system equipment that shall be capable of providing for support in case of failures in power, telephone system, data networking and Contractor's equipment at IPS host site through the user-level equipment provided by the Contractor, and for all natural or man-made disasters including flood or fire at the host facility.	**Y**	Please see comments below.

Securus has designed and implemented a robust network architecture that provides for 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:

Tier 1 – Basic
Small Business

- 99.671% availability
- Susceptible to disruptions
- Single path for power
- No redundant components

Tier 2 – Redundant
Medium Business

- 99.741% availability
- Less susceptible to disruptions
- Single path for power
- Redundant components

Tier 3
Large Business

- 99.982% Availability
- Planned activity without disruption
- Multiple paths for power
- Redundant components

Tier 4
Multi-Million $ Business

- 99.95% Availability
- Can withstand at least one worst-case event
- Multiple paths for power
- Redundant components

TIA-942 Infrastructure standards for data centers
Telecommunications Industry Association

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

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 NextGen Secure Communications Platform™ (NextGen SCP™). While operating on a single platform, Securus' NextGen 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 NextGen 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 NextGen 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 inmate calls from the NextGen SCP 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.

Restoration

Platform and Network

In the event of a disaster impacting NextGen 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 inmate 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 for Secure Call Platform

Historic Platform Availabilty
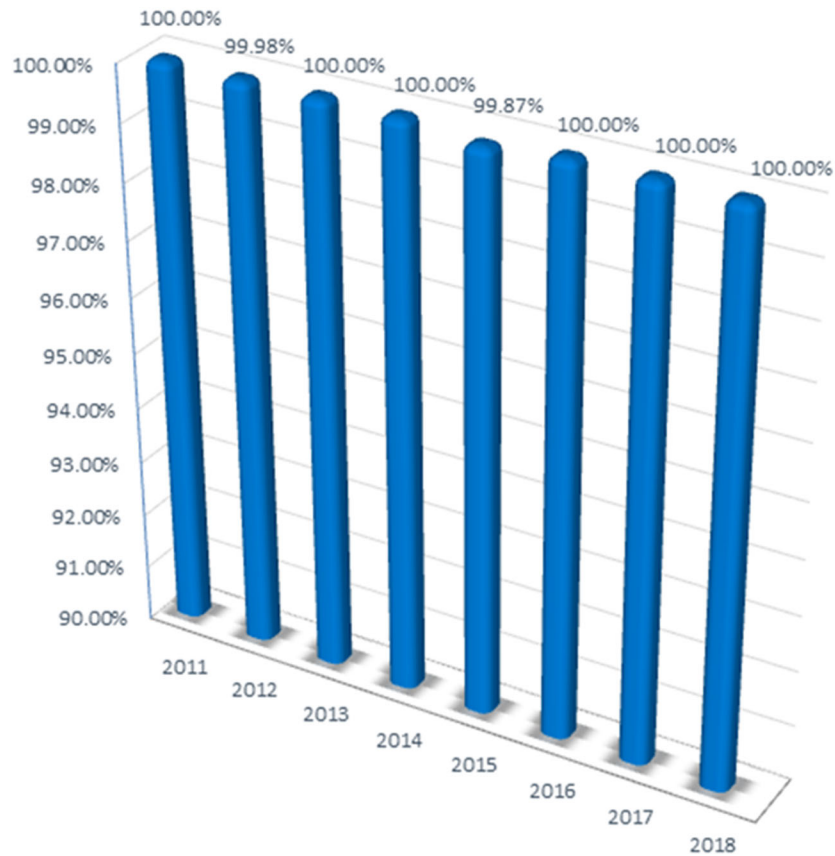
The Secure Call Platform (SCP)'s reliability will extend to NextGen SCP, as they are based on the same centralized infrastructure, proven efficient and reliable over the past 12 years.

NextGen SCP is a redesigned version of our existing Secure Call Platform (SCP)—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.

The system is capable of recovering from a power outage automatically or remotely once commercial power is restored.	**Y**	Please see comments below.

NextGen SCP automatically recovers from a power outage and restores service when power is returned.

Redundant Data Center – must have a second "off-site location" to store all phone/video/grievances/Kites	**Y**	Please see comments below.

Each day, **all centralized platform servers and NAS storage devices are backed up to tapes that are kept off-site, at two separate locations for redundancy, in an environmentally controlled media storage facility**. Most platform elements are independently fault tolerant (dual power supply, dual network interface cards, dual processor). Redundancy is through either an active/active or an active/passive configuration with failover from the active to the passive element. This fault-tolerant and redundant configuration of platform elements allows higher platform availability for both call processing and user access. Through this configuration system, outages and disruptions are kept to a minimum.

System Technical Assistance

The Contractor can provide remote diagnostic support and trouble- shooting technical assistance for system and equipment twenty-four (24) hours a day, seven (7) days a week, including holidays.	**Y**	Please see comments below.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services 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 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.

SolarWinds® Typical Monitored 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 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.

SolarWinds® Facility Monitoring Example

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.

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. Additionally, change control practices have been reviewed and are compliant with Sarbanes-Oxley.

Securus Calling Platform Provisioning Standards

All Securus calling platforms interface with industry standard analog and digital provisioned telephony circuits, such as the following services:

- POTS (plain old telephone service)
- ISDN (Integrated Services Digital Network)
- PRI (Primary Rate Interface)
- DS-1/T-1 (Digital signal 1, also known as T1)
- DS-3 (Digital Signal 3)

The PRIs (Primary Rate Interfaces) provide detailed information for advanced call routing and call progression and enforce outgoing service for our legacy platforms. Our newest centralized, packet-based platform—NextGen SCP—uses MPLS (Multiprotocol Label Switching) circuits, DSL (Digital Subscriber Line), and POTS lines.

The Contractor can provide the authorized users a toll free contact number, answered, twenty-four (24) hours a day, seven (7) days a week for the purpose of reporting problems that might be experienced.	**Y**	Please see comments below.

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 Contractor will provide on-site IPS Administrator.	**Y**	Please see comments below.
Securus will provide an on-site IPS Administrator.		
The Contractor will provide on-site IPS Technician.	**Y**	Please see comments below.
Securus will provide an on-site IPS Technician.		
Full Time on site Video Visitation Service Technician	**Y**	Please see comments below.
Securus will provide a full time on-site Video Visitation Service Technician.		
Full Time dedicated system administrator for Video/Grievance/Kite resolution	**Y**	Please see comments below.
Securus will provide a full time dedicated system administrator for Video/Grievance/Kite resolution.		
Personal Identification Numbers (PINs)		
A PIN system is currently in use in Dallas County. The Contractor's implementation plan must address creating/retaining PINs for current inmates. The Contractor must also provide procedures for updating and deleting these PINs upon an inmate's release.	**Y**	Please see comments below.
Securus will provide all required functionality related to PINs and our deployment plan contemplates the required integrations for system interoperability. Our Implementation Plan can be found as **Exhibit D.**		
The system provides Personal Identification Numbers (PIN) for Inmates	**Y**	Please see comments below.
With Securus' NextGen Secure Communications Platform™ (NextGen SCP™), each inmate telephone is individually programmed for Personal Identification Number (PIN) or non-PIN operation. This provides maximum flexibility in PIN placements. For example, a facility may wish to allow PIN operation in maximum security or long-term areas, while allowing an "all calls" option in overnight, work release, or trustee areas. The calling service has no limit or restrictions on the number of PIN or non-PIN inmate telephones operating at the facility. Some facilities may choose to assign each inmate a unique PIN that they must enter before making a telephone call. PINs also provide an audit trail of the inmate who placed each		

specific call. PINs also allow the facility increased control over which inmates can call which numbers.

Each inmate is assigned a unique PIN, ranging anywhere from 4 to 16 digits. This range creates a maximum number of 9 billion PIN combinations.

The system can restrict use of the service through authorized PINs assigned to each inmate.	**Y**	Please see comments below.

As inmate 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, Dallas County may use call restrictions to regulate inmate access to ensure access by all inmates.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides calling restrictions to give Dallas County control of calling activity at the inmate, 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 minutes 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.

Contractor issues and maintains all PIN information	**Y**	Please see comments below.

Securus will issue and maintain all PIN information. The SCP system can be set to automatically generate inmate PINs. In addition, the SCP system, through an interface with Dallas County's JMS provider can maintain all PIN information.

System allows individual PINs to be shut-off upon request of staff at the facility.	**Y**	Please see comments below

Individual PINs can be shut off upon request of Dallas County staff. PIN operations through SCP are highly flexible. Facilities have the ability to enable or disable PIN operations as needed at the facility, inmate 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 inmate telephones operating at the facility.

For those phones that have been programmed for PIN operations, each inmate must enter their PIN before making a telephone call. By using their PIN, they create an audit trail that that shows authorized personnel the inmate that placed the call, the date and time of the call, and the number that was dialed. PINs also enable facility staff to authorize or restrict specific inmates from calling specific numbers.

When an inmate transfers to a different facility, that inmate's PIN account also transfers.	**Y**	Please see comments below.

PINs, and the telephone which are associated with the PIN, will be moved when the account transfers. An easy-to-use PIN transfer module is available for site administrators to transfer a single PIN or a group of PINs when inmate(s) are moved to another housing unit. This process may also be automated through our data import application E-Imports

System utilizes the PIN feature for any call mode, either prepaid or normal collect calls.	**Y**	Please see comments below.

The SCP system, when programmed to use PINs, will use PINs for any call mode, whether prepaid or normal collect calls.

Each PIN has a "class of service" assigned. For example, each PIN has a list of allowable telephone numbers, and or other information.	**Y**	Please see comments below.

The Personal Allowed Number (PAN) feature in the NextGen Secure Communications Platform™ (NextGen SCP™) provides an approved calling list for each inmate. Authorized Dallas County users can add both allowed and blocked numbers to the PAN list.

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 Dallas County) to be added to the inmate's PAN list automatically. The quantity of numbers allowed is configurable.

This is the most popular method of PAN administration. Numbers are loaded immediately without the intervention of staff.

Inmate Managed PAN: Allows inmates 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 inmate 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 inmate's PAN list. No staff time is required to administer this process. With the extra step of validation, the County has maximum control of each added number.

Manual PAN Entry: Authorized facility personnel can accept calling lists from inmates, 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 inmate'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 Dallas County.

<p align="center">PAN Features</p>

PAN Feature	Primary Benefit	Description
Global Allowed List	Efficiency	Certain phone numbers, such as attorney numbers, can be authorized for all inmates 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 inmate's PAN list as "verified" or "not verified." If the PAN is "not verified", the inmate 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 inmate'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 inmate 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 Inmate 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.

PIN feature ensures that the automated operator function uses the inmate's pre-recorded name (recorded in either the inmate's voice or language, or in the voice of an administrator) to announce to the called party from whom the call is originating. Identification of the specific inmate and thus the announcement of the inmate's name are performed by the PIN assignment.	**Y**	Please see comments below.

Securus SCP calling platform allows for inmates to record their name once which is associated with the inmate's custody account and PIN.

The recorded name will be played on all calls the inmate makes with their PIN. If no PIN is required for the inmate, the system will ask the inmate on each call for their name which is played to the called party. All pre-recorded inmate names are to be played to the called party when announcing the call.

To provide the facility with the maximum flexibility, this function is configurable to use pre-recorded names, or not to use pre-recorded names per inmate, facility, and customer level. A pre-recorded name may also be reset, forcing the inmate to record their name again if necessary.

System allows for approved destination telephone numbers to be assigned and restricted by individual PIN.	**Y**	Please see comments below.

NextGen SCP allows Approved destination telephone numbers cab be assigned and restricted by individual PIN.

The PAN feature in the SCP provides an inmate approved calling list. This is a restrictive list in which the phone number entries on the PAN list are the only numbers that the inmate can call. However, regardless of a PAN list, the system also provides the inmate with the ability to make attorney calls or other allowed called placed on the "global allowed list".

Securus' Personal Allowed Numbers (PAN) feature allows administrators to associate a "personal allowed number" list with each PIN, so that the inmate cannot make calls, except to those pre-specified numbers on his or her list.

To provide facilities with further control over inmate telephone usage, authorized personnel may program telephones with specific call restrictions and call durations by PIN. After a number is restricted or blocked in the system, calls to that number are prohibited until otherwise modified by authorized personnel.

The system can also assign a speed dial number to each PAN to further alleviate the problem of inmates stealing or using other PIN/PANs. As with most SCP centralized platform features, authorized personnel can make these changes from any location at any time 24-7.

Like all other features of SCP, the PAN lists are flexible and may be administered in various ways. The system may allow authorized users to manually enter and administer approved numbers as well as automate the process by allowing the first numbers called by the inmate

and accepted by the called party to be added to their list. Additionally, the system allows for the importing of personal allowed numbers through our E-Imports application to add number, associate relationships, and deactivate numbers. SCP allows for a variety of other tools that may include, but are not limited to, the inmate calling into an automated system with their PAN requests.

PINs allow each inmate to maintain a list of authorized telephone numbers not to exceed a maximum total of ten (10) numbers not including privileged telephone numbers.	**Y**	Please see comments below.

The PAN feature in the SCP provides an inmate approved calling list.

This is a restrictive list in which the phone number entries on the PAN list are the only numbers that the inmate can call. However, regardless of a PAN list, the system also provides the inmate with the ability to make attorney calls or other allowed called placed on the "global allowed list".

Securus' Personal Allowed Numbers (PAN) feature allows administrators to associate a "personal allowed number" list with each PIN, so that the inmate cannot make calls, except to those pre-specified numbers on his or her list.

To provide facilities with further control over inmate telephone usage, authorized personnel may program telephones with specific call restrictions and call durations by PIN. After a number is restricted or blocked in the system, calls to that number are prohibited until otherwise modified by authorized personnel.

PIN feature allows the recording of inmate calls to be discontinued when certain predetermined telephone numbers (privileged telephone numbers) are called.	**Y**	Please see comments below.

SCP can automatically eliminate monitoring and recording of special calls, such as to attorneys, clergy, or doctors, by designating numbers as "private."

Inmate Phone Access Information/Approved Number List		
A number list option is currently in use in Dallas County. The Contractor's implementation plan must address transitioning these lists for current inmates. The Contractor must also provide procedures for updating and deleting these lists upon an inmate's release.	**Y**	Please see comments below.

Securus Technologies is proud of our 5 year association with Dallas County. We believe our longtime partnership has proven we bring technology capabilities that set Securus Technologies apart from any other vendor. We have worked closely with Dallas County to deploy new and existing technologies to meet the needs of the county and its constituents.

We know this RFP is about the future and choosing a supplier that will meet your needs over the next 5 years. We believe our track record and our response to this RFP demonstrate that we will continue to bring value to the partnership going forward. We also ask that you

consider the following additional advantages of continuing to work with Securus versus selecting another provider:

The Personal Allowed Number (PAN) feature in the SCP provides an inmate approved calling list. The PAN restricts inmate calling to only those numbers included on their list. Securus built this feature specifically for the corrections industry with the awareness that each facility has unique needs for implementing allowed calling lists.

Like all other features of SCP, the PAN lists are flexible and may be administered in various ways: PANs can be configured manually, automatically, or by importing through E-Imports. The PAN configuration options include the following:

Auto Pan – Allows the first "X" amount of numbers—amount is defined by Dallas County— number of called numbers to be added to the inmate's PAN list automatically. The amount of numbers allowed is configurable and will not allow the inmate to exceed that number.

This is the most popular method of PAN administration. No staff time is required for this process and numbers are loaded immediately to maximize revenue potential.

Inmate Managed PAN – Allows inmates to manage phone numbers on their list such as adding a new number, removing a number, checking the status of a phone number, or hearing, which phone numbers are on their list. With this system, when an inmate 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 a valid BNA is found, the automated system calls the phone number requesting to be added and asks the called party if they wish to be placed on the specific inmates PAN list.

No staff time is required to administer this process. With the extra step of validation, the County has maximum control of each added number.

Adding PANs by System Integration – SCP allows for the importing of personal allowed numbers through our E-Imports application to add number, associate relationships, and deactivate numbers.

No staff time would be required to administer this process. This is a specialized form of PAN administration, based on specific integration requirements of a facility.

Contractor provides Service Representatives (can be accomplished by assigned site personnel) for entering Inmate Phone Access Information in the Inmate Telephone System. What is the timeline for the entry of this data? Inmate Phone Access information fields shall include, but not be limited to, inmate name (first, middle, last), PIN number (5 digits minimum), County facility, ten (10) approved telephone numbers by terminating number, privileged numbers; comments field, language preference field, account activation date, date of arrival, current status, alert levels, etc.	**Y**	Please see comments below.

With the Onsite Administrators (Service Representatives), entering inmate phone access information can be accomplished same-day. Data should be entered within 24 hours.

Authorized County personnel have the capability to enter, modify and delete any information for any inmate phone access information including an inmate's "Approved Number List".	Y	Please see comments below.

Authorized users can access, view and modify all system features and functionality including an inmate's "approved number list.

Call Requirements

Contractor ensures that prepaid and collect calling is available for all locations within the North American Dialing Plan. In addition, the Contractor provides a list of all countries (outside of the United States) that can be reached via the IPS operating in a "collect call only" mode.	Y	Please see comments below.

Securus provides traditional Collect calling to North American Numbering Plan (NANP) international destinations such as Canada and some Caribbean locations. Securus recommends not enabling international collect calling to non-NANP countries due to greatly increased financial exposure. Billing and collection options are extremely limited with little or no rights and remedies for non-payment. For this reason, Securus does not process non-NANP international collect calls and provides additional options to process International calls via prepaid services.

Call acceptance by the called party accomplished through caller confirmation ("positive acceptance").	Y	Please see comments below.

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 inmate'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.

At no time shall an inmate be automatically connected to a "live" operator. The only exception to this requirement is that international collect calls through a live operator will be allowed when the country being called accepts collect calls.	Y	Please see comments below.

NextGen SCP does not permit or require access to live operators.

Collect calls not connected nor does billing commence until the called party indicates acceptance of the call. All non-prepaid calls shall be directly billed to the Billing Number Address (BNA) by the Contractor.	Y	Please see comments below.

Billing for inmate calls begins upon positive acceptance of a call by the called party.

The Securus Inmate Telephone System (SITS) requires positive called party acceptance using touch-tone telephones before the conversation can begin. When the called party answers the phone, answer-detection technology triggers the call acceptance message. This message announces the inmate'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 his or her telephone to accept the collect call charges, or hang-up to disconnect the call and refuse charges.

Contractor provides a toll free number which will be clearly shown on the called party's bill for assistance in billing matters.	**Y**	Please see comments below.

A toll free number for assistance in billing matters is clearly shown on the called party's bill.

Securus is unique among its national competitors in offering an in-sourced, US-based call center to provide customer service to friends and family members of inmates. Our 200+ seat call center employs Dallas area customer service representatives who are trained and managed by Securus.

Live agent support is available to friends and family members 24x7x365.

Customers can use our toll-free number (1-800-844-6591) to speak to a live agent or use an intuitive, automated interactive voice response system to help them with their needs.

For added convenience, we also offer personal account access via our website (www.securustechnologies.com). End-users can also now access Securus customer service via online "chat" 24 hours a day, seven days a week.

The Contractor ensures Caller ID is not available for any call placed through the system and the called party has no other means of identifying the number from which a call is placed.	**Y**	Please see comments below.

Called parties can identify calls from an inmate at a Dallas County facility through their caller ID. Collect call charges from the Dallas County facility on phone bills include the contact information for the Securus customer service center, Securus Friends and Family Call Center (SFFCC). Should the friends or family members have any questions regarding their collect call charges, they can use this contact information from their bill to contact SFFCC.

Caller ID

The default configuration for caller ID shows Securus Correctional Billing Services toll-free number, not the Dallas County Facility. Additional configuration options include:

- Caller ID can display a number supplied by Dallas County; the name associated with that number through your local telephone provider will also appear on the caller ID.

▪ Any other number can be assigned to display on calls from Dallas County Facility, however unless associated with a name through a local telephone company, only the telephone number will appear to called parties, not a name.		
Contractor does not charge for calls that result in Special Information Tones (SIT), "ring/no answer", or "busy" conditions.	**Y**	Please see comments below.
Billing for inmate calls begins upon positive acceptance of a call by the called party. The Securus Inmate Telephone System (SITS) requires positive called party acceptance using touch-tone telephones before the conversation can begin. When the called party answers the phone, answer-detection technology triggers the call acceptance message. This message announces the inmate'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 his or her telephone to accept the collect call charges, or hang-up to disconnect the call and refuse charges.		
The Contractor provides local exchange service for collect-only calling use at each County facility listed at Attachment 1. The Contractor ensures that the system is capable of identifying a dialed number as local, based on the pay telephone calling area, and of correctly rating and routing the call.	**Y**	Please see comments below.
Securus employs the most sophisticated intelligent validation network in the industry. As a real-time, computer telephony-based switching system, the Securus calling service never connects an inmate to a conventional dial tone. All dialed numbers—whether prepaid or collect—are thoroughly analyzed before the call is allowed to process. This includes determining if the area code and exchange are valid, checking the number against any restrictions such as customer requested blocks, confirming the payer has available funds or is credit worthy, and verifying through the national Line Information Database (LIDB). The system will only dial a number after passing all of these tests. # 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
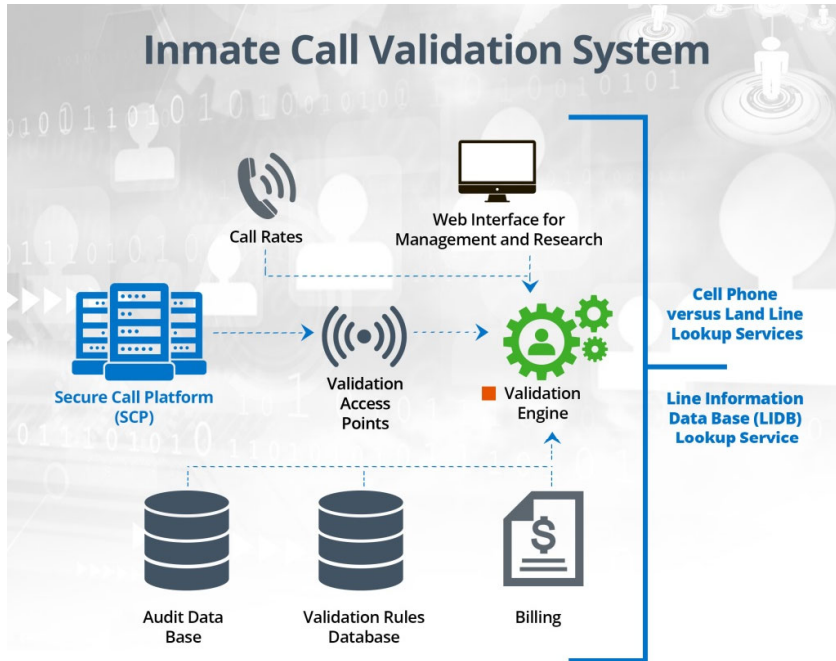
The following checks are performed during the validation process:

- If the facility uses personal allowed number (PAN) lists, the first check ensures that the number dialed is on the inmate'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 that un-allowed numbers are not called

- All collect calls are validated through AT&T's line information database (LIDB) to determine if the number has calling restrictions.

Prepaid Collect Call Service (PPCCS)

Contractor allows families and friends to establish a PPCCS account(s) with the Contractor for billing purposes so that inmates can call pre-authorized numbers that may not be accessible via normal collect calling. Any calls billed to a family or friend's prepaid account shall meet the same security requirements as set forth for normal collect calls.	**Y**	Please see comments below.

An AdvanceConnect™ account is a prepaid account that allows friends and family members or special account groups, such as bail bondsmen and attorneys to receive collect calls from inmates and have the charges deducted automatically from the prepaid account.

Contractor ensures that notice of the prepaid account availability is provided when a party receives a call and shall offer the option of being connected to a live operator for the purpose of establishing a prepaid account, if a normal collect call cannot be completed by the inmate due to billing issues.	**Y**	Please see comments below.

When an inmate or detainee at your facility makes a call, our validation system will route the call ,through multiple means, to connect the call, including offering the friend or family member the option of speaking to a live customer service representative.

Contractor's PPCCS shall allow the called party (family and friends) to deposit money into a PPCCS account by multiple means (i.e. check, money order, credit card, and/or latest pay system).	**Y**	Please see comments below.

Securus offers friends and family members of inmates a wide variety of options to set up and fund prepaid accounts. Convenience drives account creation, and account creation connects more calls, so Securus has made the funding process easy. To create and fund a pre-paid calling account, friends and family members can:

- Call our Customer Service Center and speak with a live operator 24x7x365
- Use our automated interactive voice response system
- Use our mobile-friendly website (Android and iOS)
- Fund accounts by mail
- Visit one of more than 35,000 MoneyGram locations such as Walmart and CVS Pharmacy
- Visit one of more than 58,000 Western Union locations.

Friend and Family Funding Options	**Means to You**
In-house Call Center • Available 24 hours a day, seven days a week and 365 days a year • Staffed with Dallas-based Securus employees • Use automated telephone access or talk to a live agent • Fund an account o Accept Visa and MasterCard • Manage account (e.g. open accounts, make or check payments, confirm rates, obtain credit limits, review call history, review account	Securus believes the customer experience should not be out-sourced to an outside vendor. As a result, our customer satisfaction scores are 20 percent higher than the industry standard. We are available so that you do not have to use staff time to answer questions on telephone account issues.

balances, manage account notifications, and get questions answered)

Website Access

- Create an account
- Mobile-friendly
- Fund an account
  - o Accept Visa, and MasterCard
- Manage account (see above description)

This is a popular option for those parties that wish to fund without interacting with a call center agent. Funding drives more calls.

Lockbox

- Accept personal checks, money orders, and cashier's checks mailed to Securus
- No funding minimum

Cash conscious parties can fund without a transaction fee or a minimum. This allows inmates to talk with called parties who would not ordinarily be able to set-up accounts.

MoneyGram

- Fund at over 35,000 Walmart and CVS Pharmacy locations

For those without credit cards or who want immediate account set-up with no minimum fee, we provide funding options at any MoneyGram or Western Union location.

Western Union

- Fund at over 58,000 locations

Inmate Funding Options	Means to You

Inmate Debit

- Integrated with trust fund or telephone fund accounts

The integrated option allows inmates access to other accounts to fund telephone calls on all devices

Contractor provides instructional brochures explaining the process for establishing prepaid collect services for family and friends' prepaid accounts.	**Y**	Please see comments below.

Securus supplies professional-grade, high-quality inmate flyers and friends and family posters that communicate the products, how they work, and how to connect to Securus. Upon installation, Securus supplies these materials including an initial stock of brochures that educate friends and family about using our accounts, contacting Securus, and terms conditions. We supply these brochures to the facility at no cost, including a brochure stand. Each piece includes the Securus customer service number and Website so that friends and family may easily connect with our self-help or agents 24x7x365. Upon request, Securus can provide DVD instructions about how to use certain features, such as debit or PINS. Our in-house graphic design department creates these DVDs.

Securus will also provide online instructions for friends and family, specifically for the Dallas County Jail website.

Inmate Hotline		
Contractor has a component within the system that creates an inmate "hot line" accessible from any telephone instrument within the system.	**Y**	Please see comments below.

The Securus Crime Tip feature is an inmate crime reporting tool that gives inmates an anonymous and secure way to provide crime tips to corrections officers. The Securus calling services system anonymously records all messages left on the Crime Tip Hotline, so inmates do not have to risk being identified as an informant.

Inmates can choose to report:

- Information about possible criminal activity, including narcotics
- A crime that has already taken place
- A threat to their safety
- Threats to the safety of others

While tips are anonymous as a default, informants may choose to leave their name.

The Securus Crime Tip feature includes:

- A pre-arranged telephone number (designated by the facility), provided to all inmates
- An option to listen to all or selected recorded messages
- An option to burn specific information onto CDs for use as evidence
- A way to generate reports of all recorded messages with the date and time of the message
- A way to leave an anonymous reply message to the inmate

Inmate Phone Station Equipment ("IPSE")		
All IPSE required for service delivery is new or refurbished to like new condition and consists of two (2) types of telephones: • **Type 1, which will be the majority of inmate telephones installed, shall be permanently mounted wall telephones meeting the specifications outlined in this RFP.** • **Type 2 shall be portable or "movable" cordless inmate telephones.**	**Y**	Please see comments below.

Securus' inmate telephones are the strongest and most reliable units available and are designed specifically for the prison environment. Securus is proposing Wintel® brand 7010 phone model. The following information is the manufacturer-provided telephone specifications:

The Industry Standard

These phones are the overwhelming choice for state prison systems, the Federal Bureau of Prisons, county, and city facilities nationwide because of their proven reliability, durability, and flexibility.

Features/Options

The proposed phone models include the following features:

- Built-in user controlled volume "LOUD" button for ADA-mandated volume control (user must have control of volume amplification, AND volume must reset to normal with hang up to meet ADA requirements)
- Cold rolled steel provides rugged vandal resistant telephone housing designed for inmate use
- Confidencer technology, built into every dial, filters out background noise at the user's location, allowing better sound to the called party
- All-in-one electronic dial features modular incoming line and handset connections for quick maintenance. Carbon (HS) and DuraClear® (DURA) Handsets have separate 4-pin connections.
- Heavy chrome metal keypad bezel, buttons, and hook switch lever withstand abuse and vandalism
- Armored handset cord is equipped with a steel lanyard (1000-pound pull strength) and secured with a 14-gauge retainer bracket for maximum vandal resistance
- Handset has sealed transmitter and receiver caps, suitable for heavy use and abuse locations
- Pin-in-head security screws minimize tampering
- Hearing aid compatible and FCC registered US: 1DATE05BITC-254, IC: 3267A-ITC254

Cordless Phone

Securus will provide the Clarity XLC2 DECT 6.0 Amplified Cordless Big Button Speakerphone with Talking Caller ID or similar cordless phone for Dallas County. The following information is the manufacturer-provided specifications.

The XLC2 is a loud, simple and easy-to-use amplified cordless phone featuring up to 50 decibels of Digital Clarity Power™ amplification, DECT 6.0 technology and a loud and clear speakerphone. Large, high contrast buttons are easy to press and see, and speaks the numbers as they are dialed.

Features:

- Digital Clarity Power™ amplifies incoming sound up to 50 decibels
- Three tone settings for a customized listening experience
- Amplifies outgoing speech up to 15 decibels for others to hear you better
- DECT 6.0 technology for interference-free communication
- Loud and clear speakerphone for hands-free conversations
- Illuminated talking dial pad with large buttons that speak the number that is dialed
- 12 speed dial buttons
- Flashing Visual Ringer
- Can be wall mounted to avoid using counter or desk space
- Hearing aid compatible and TIA-1083 compliant
- Direct connection to assistive listening devices or headset (2.5mm and 3.5mm)
- Dual Power Battery Backup lets you make calls when the power is out
- Backup batteries included

Phone Application on SecureView Tablets

For facilities that use the Securus SCP Inmate Telephone Service, the SecureView Phone application will allow the SecureView tablet to function as a telephone extension of the SCP platform. Just like SCP, the SecureView tablet has the feature that will only allow that inmate to make calls from the housing unit where he resides.

All the features and restrictions of the SCP Inmate Telephone Service will apply such as PIN/PAN lists, velocity controls, family and friend billing/customer service, and recording and monitoring. There are no additional fees or rate increases applied.

Capabilities:

- Allows inmates to place calls through the Secure Calling Platform (SCP)
- Phone Groups for locking a tablet to a housing area
- Volume controls
- Standard 9-Key dialing pad
- Visual call timer

Benefits:

- Intuitive design and use
- Ability to place calls with more privacy and safety
- Assists in avoiding and minimizing confrontation in common areas

All IPSE has the physical and design characteristics that meet or exceed all of the following technical standards: • **A chrome-plated Dual Tone Multi-Frequency DTMF tone dial that is water, flame and shock resistant.** • **A hearing aid compatible handset.** • **A steel housing that protects the electronic components of the telephone.** • **A paint/finish that is mar and scratch resistant.** • **A faceplate with concise dialing and operating instructions.** • **An industry standard design.** • **A tamper-proof housing.** • **A floating case hardened metal plate to prevent side drilling entry.** • **Dialing Instructions and "This Call is Being Recorded" warning statements in English and Spanish on each telephone instrument in a manner that reduces the possibility of the notice being destroyed. Labels or other accessible surface instructions will not be acceptable to meet this requirement. This information must be kept legible and accurate throughout the duration of the Contract.** • **A unique number, physically imprinted on each telephone instrument so that Department staff can see the number for the purposes of reporting trouble and troubleshooting problems. As telephone instruments necessitate replacement, they shall be numbered by the Contractor. As new telephone instruments are added or replaced, they shall be identified in the same manner and all appropriate paper work shall be updated to reflect the addition.** • **An armored handset cord that is resistant to stretching and breaking.** • **Installation reinforced by security studs to prevent easy removal of telephone.**	**Y**	Please see comments below.
All Securus IPSE meets the above requirements.		
The IPSE does not include coin entry slots or coin return slots regardless of whether these functions are disabled on the station equipment (standard pay telephone requirements excluded).	**Y**	Please see comments below.
The IPSE does not include coin entry slots or coin return slots		

All IPSE meets or exceeds the following capabilities: • **True dual-tone multi-frequency (DTMF) compatibility.** • **The IPSE shall not be capable of being used to program any feature of the IPS.** • **The IPSE shall not be programmable for any purpose.** • **Reduction of background noise through the use of confidencers or directional microphones in the handset.** • **Volume controls that allow inmates to amplify the called party's voice.** • **Powered by the telephone line and requiring no additional power source, with the exception of cordless telephones as described above.** • **Compatible with Telecommunications for The Deaf (TDD/TTY) equipment.**	Y	Please see comments below.
All Securs IPSE meets the capabilities listed above.		
All IPSE capable of being Americans with Disabilities Act (ADA) compliant. Twenty-five percent (25%) of all phones have volume control capability.	Y	Please see comments below.
All Securus IPSE is ADA compliant and have volume control capability.		
Coin (pay) phones are of a type equivalent to those currently installed at those locations reflected at Attachment 2.	Y	Please see comments below.
Securus can supply the pay phones requested in the locations listed in Attachment 2.		
TDD/TTY Equipment		
TDD/TTY is provided for inmate use at all locations specified at Attachment 1 except Cook Chill.	Y	Please see comments below.
Securus shall provide TDD/TTY phones in all locations specified in Attachment 1.		
Minimum requirements for TDD/TTY equipment include: • **Portability, such that it can be used with any IPS station set at Dallas County institution.** • **The ability for keyboard entry.** • **A display (i.e., LCD, LED, etc.) and a printer device.** • **System shall have the ability to accommodate inmates needing to communicate using American Sign Language (ASL). A basic Video Relay Services (VRS) feature are required.**	Y	Please see comments below.

Securus will provide accommodations necessary to comply with the Americans with Disabilities Act (ADA). The Securus program for inmates who are deaf or hearing impaired allows those inmates to place outgoing telephone calls using a text telephone (TTY) device integrated with NextGen Secure Communications Platform™ (NextGen SCP™).

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 inmate placing the handset on the TTY device and entering the speed-dial number initiates the call. The inmate then communicates using the TTY device through the Securus Inmate Telephone System (SITS) to the state's telecommunication relay center (TRS). The information includes the option of including the inmate'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 inmate 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 inmate 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.

SCP provides support for hearing-impaired inmates 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 inmate call controls, management, and investigative abilities expected for inmate calls.

Video Relay Service

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 Dallas County 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 inmates with "equal access" to communication services while allowing Dallas County to provide, manage, and investigate inmate VRS calls in a manner consistent with traditional inmate calls.

Securus VRS provides equal access by allowing Dallas County to:

- Provide VRS-capable inmate 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 inmate calls
- Record VRS calls in accordance with the same recording controls that govern whether or not to record traditional inmate calls
- Include VRS call recordings in investigations including inclusion in CD images and individual downloads.
- **EXCLUSIVE TO SECURUS.** 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.

Securus VRS call recordings include the visual component of the inmate call for both the inmate and the other end of the video portion of the VRS call. The other end of the VRS call might be the inmate'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 inmate call management control structures as for traditional inmate 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 inmate PAN lists
- Call recording
- Collecting VRS calls in inmate calls for investigations and evidence

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

Inmate access to Securus VRS is provided as an application available through ConnectUs—the controlled inmate interface provided on inmate kiosks. ConnectUs can be configured to present numerous applications to Dallas County inmates, which allows inmates to use the same multi-function terminal for Securus VRS calls as for standard inmate calling, Securus Video Visitation, Inmate Forms, and more.

Because VRS calls are required by the FCC to be free, all inmate VRS calls will be provided at no cost to the inmate. To ensure Dallas County can prevent the unauthorized use of Securus VRS to place free calls, the Securus VRS is also integrated with SCP to allow Dallas County to designate which inmates are allowed to place VRS calls. The Securus VRS ConnectUs application requires inmates to enter their designated inmate 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, Dallas County 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.

Coin-Operated Public Telephone Equipment

Coin-operated telephones are provided for public use at those locations identified at Attachment 2. These telephones meet all FCC regulations regarding alternate carrier access.	**Y**	Please see comments below.

Securus will provide coin payphones at all identified locations, which feature the following manufacturer-provided specifications:

- Line-powered, no electricity required
- Accepts quarters, dimes, and nickels
- High-quality handset with reinforced 32-inch armored cord
- Vandal-proof locks (high-security Medeco locks are available for an extra charge)
- Coin box
- Full spectrum answer supervision
- Power requirements: telephone line powered, 30 volts DC (on-hook), 23 milliamp(mA) loop current
- Internal rechargeable lead-acid gel cell (off-hook), 6 volt, 1.2 ampere-hour. No electricity required
- Operating temperature range:-4° to +140°Fahrenheit
- Relative humidity range: 0 to 95 percent, non-condensing
- Grounding requirement: Earth ground
- Surge protector: on-board, solid-state transient surge protector on telephone line
- Telco line type: POTS line, COCOT (PAL) B-1, loop start standard dial tone 600/120 Hertz
- Loop current range: 23 mA to 80 mA

- Complies with Part 68 and Part 15 of the US Federal Communications Commission rules and regulations and is in general compliance with all requirements described in applicable CCITT recommendations
- Ringer equivalency number (REN):1.0 B
- Telco line interface: Internal to payphone, RJ11C jack on printed circuit board
- Coin relay driver: Internally provided +/- 80 volt DC (COCOT B-1)

Response and Repair Times for Service Calls		
For routine service, the Contractor responds to the service problem within four (4) hours of initial request for service report by a Dallas County facility.	Y	Please see comments below.
Securus will respond to service problems within four (4) hours.		
Contractor provides the Dallas County facility with the status of requested items within six (6) hours of the initial service request.	Y	Please see comments below.
Securus will provide the facility with the status of the request within six (6) hours.		
All routine service completed within twenty-four (24) hours of the initial service request.	Y	Please see comments below.
Securus will complete all routine service within 24 hours.		
For a major emergency, the Contractor responds to the service problem within one (1) hour of initial request for service report by a Dallas County facility.	Y	Please see comments below.
For a major emergency, Securus will respond to the service problem within one hour.		
The Contractor provides the Dallas County facility with the status of the emergency within 3 hours.	Y	Please see comments below.
Securus will provide Dallas County with the status of the emergency within 3 hours.		
All major emergency service completed within twelve (12) hours of the initial service request	Y	Please see comments below.
All major emergency service requests will be completed within 12 hours.		
Contractor provides escalation procedures to address inadequate response to service calls, frequent repetition of the same service problem, inadequate repairs to service, etc.	Y	Please see comments below.
Securus will provide four full-time onsite technicians/administrators to ensure prompt issue resolution and seamless customer experience. In addition, 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

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.

Reporting Requirements

Inmate Telephone System Generated Reports	Y	Please see comments below.
System allows Dallas County to generate the following "canned" reports directly through an interface accessible through a secure internet site or via dedicated monitoring terminals. The database is capable of maintaining a record of all reports that are downloaded, with the date and time of the download, and the name of the person who performed the download. All reports have the capability of being queried, sorted or filtered by any field contained in the report or by data parameters, as applicable, and reports shall be readable on screen, printable and shall be downloadable into a Microsoft Excel format. Reports can also be viewable via a user-friendly interface. This interface shall be, at a minimum a Graphical User Interface (GUI) such as Windows 10 min. • *Authorized Users Report*: **The system provides a real time report of all County and Contractor authorized users. This report includes user name, status (active or inactive) and corresponding dates, user title and facility location.** • *Approved Calling List Report*: **The system provides a real time report of each inmate's approved calling list of ten (10) numbers. This report includes inmate name, inmate PIN #, inmate's facility location, name and phone numbers of everyone on the inmate's calling list and Billing Number Address (BNA) for all numbers. The system also maintains a cumulative historical calling list for each inmate, showing all numbers that have been added or deleted from the inmate's list and the corresponding dates.** • *Comprehensive Outgoing Call Report*: **The system provides a real time report of all outgoing calls made from all Department facilities. This report includes inmate name, inmate PIN #, inmate's facility location, phone number called, date and time of call, length of call and BNA for number called.** • *Duplicate Number Report*: **The system provides a real time report of all outgoing telephone numbers that appear on the active call lists of two or more inmates. This report includes phone number, BNA for number called, inmate**		

name, inmate PIN #, and inmate's facility location. • *International Call Report*: The system provides a real time report of all overseas/international calls made. This report includes inmate name, inmate PIN #, number called, BNA for number called, inmate's facility location, date and time of call, length of call. • *Alert Level Report*: The system provides a real time report of all calls that generated an alert notification in the system. This includes three-way calls, as well as any other calls programmed to send an alert notification. This report includes date and time of call, number called, BNA for number called, inmate name, inmate PIN #, and type of alert. • *Ad Hoc Reports*: The Contractor provides Dallas County ad hoc reporting from the system upon request from the County. Responses should include the time frame within which these reports will be made available.		

The NextGen Secure Communications Platform™ (NextGen SCP™) has a dedicated report generating function that provides investigative information based on the communication detail records. This sophisticated reporting tool provides a reporting interface into all communication activities.

Reports can be generated online and exported in the following formats:

- Microsoft® Excel
- CSV (Comma Separated Values)
- Adobe® PDF

Users can search and analyze communication details on all communication events through NextGen SCP. These details include date, time, duration, telephone number, origination, destination, inmate ID, termination reason, and more. NextGen SCP retains communication details on all communication attempts. Users can customize the standard reports by varying search criteria, such as date range, facility, or call length.

NextGen SCP provides standard reports with parameter fields that allow the user to define the information content of each report based on the following criteria options:

- Date range
- Inmate identifier, such as ID, PIN, and first or last name
- Communication type (calls and video)
- Communication status (complete or incomplete)
- Destination number (partial or full number entry)
- Call type
- Three-way or Remote Call Forwarding detected, watched status, wireless indicator, or Continuous Voice Identification
- Visitor and visit type (SVV)
- Visitor contact number
- Visitor identifier, such as first or last name, email, and visitor ID
- Per phone/terminal, per location, and per offender
- Number restriction and/or status assignment
- Broad search with no data entry
- Suspected fraudulent call activity
- Prepaid account number
- Destination zone (local, interLATA, interstate, intraLATA, international)

Sample Communication Detail Results Screen

Contractor Submitted Reports **The following reports (except the Annual Commission Report) are capable of being submitted by the Contractor in "electronic" format on a monthly basis no more than fifteen (15) days following the end of the previous month.** • *Commission and Call Detail Report/Supporting Documentation for Monthly Activities*: **The Contractor submits as supporting detail for the monthly activity, Call Detail Report in detail sufficient to allow the County to audit charges to the inmates.** • **The Activity and Call Detail Report consists of the following: A list of all inmate calls made by PIN, time connected, time disconnected, rate charged [both per minute and total charge, separating any surcharge], duration of call, and called number and any other information necessary for the Department to independently calculate the gross revenue. The report is submitted monthly shall be – electronical and shall also reflect the gross revenues generated by all inmate phones. Hard copies available upon request** • *Equipment Report:* **The system provides a real time report of all assigned equipment (in use) and inventoried equipment containing a serial number. This report includes description/type of equipment, serial number, facility location (including specific dormitory or other unique location), and assigned telephone number (for phone instruments).** • *Trouble Ticket/Repair Time Report*: **The system provides a real time report of all trouble tickets and repair times that are reported to the Contractor. This report includes the assigned number with trouble, location (including specific dormitory or other unique location), date and time trouble was reported, cumulative downtime as a result of trouble, downtime reason (e.g. processor failure, power failure, station failure, trunk failure, etc.) and date and time trouble was cleared.**	**Y**	Please see comments below.

• *Ad Hoc Reports*: **The Contractor provides Dallas County ad hoc reports upon request of the County. Responses should include the time frame within which these reports will be made available.**		

All the above listed reports can be supplied within 15 days. Ad hoc reports will be provided within 15 days as well.

Staff/Service Requirements

The Contractor has direct oversight and will be responsible for and monitor the performance of all contractor staff performing services under the Contract.	**Y**	Please see comments below.

Securus will have direct oversight and will be responsible for and will monitor the performance of all contractor staff. Moreover, **Securus is committed to using a certified-SBE vendor for its subcontracted services and support.**

The Contractor provides an adequate level of staffing for provision of the services outlined herein and shall ensure that staff providing services is appropriately trained, qualified and licensed, if required.	**Y**	Please see comments below.

Securus provides highly reliable service from initial system design and installation through ongoing maintenance and support. Our service and maintenance program includes integrated remote programming, diagnostics, downloading, and troubleshooting capabilities. Securus does not charge for maintenance, support, training, and repair of system software and equipment.

The local Securus service and account management team provide support 24 hours per day, seven days per week, and 365 days per year (24x7x365). The local team of Securus employees have demonstrated their dedication to the counties in the state of Texas.

The following in-house Securus teams work together to support our customers' technical needs:

- Your Securus account team
- Network Operations Center
- Technical Support Center
- Field services team

These teams ensure Dallas County's system is running at peak performance levels.

Technical Support Center

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 100+ 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

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

The Securus Field Services Team

The Securus Field Services organization is one of the largest in the inmate phone system industry. Our team consists of approximately 224 Field Service Technicians (FSTs) located throughout the United States, including a team to support the systems in Texas. Our teams have expanded based on our growing customer needs.

Our field services team installs and maintains inmate phone systems for a million inmates in 47 states. The Securus Field Operations Director manages four Regional Service Managers who possess more than 60 years of combined field service experience.

Field Service Technicians

Securus requires that all FSTs have an extensive telecommunications background and tests each applicant before employment. Additionally, FSTs receive extensive Securus training and certifications to support our product offerings.

FSTs respond to critical issues within four hours (or less if required by specific County requirements). The technician is required to follow a structured technical and management escalation process if they are unable to isolate the problem within four hours. Our integrated support model keeps our centralized technical support team engaged through problem resolution. FSTs and the technical support team have direct access to product and development engineers, enabling them to expedite repairs and minimize customer downtime.

Securus field service technicians maintain a working level of spare parts for minor repairs consisting of telephone sets, handsets, dials, and replacement circuit boards, either on-site or in their truck. If a technician does not have a required part, Securus will drop-ship the item to the site. Securus will ship counter-to-counter on the same day in critical situations.

Field Service Manager

In addition to FSTs, Securus customers are supported by field service managers who:

- Conduct remote visits via phone bimonthly. Based on information obtained from call, a trouble ticket may be opened
- Work with the account team quarterly to evaluate contract progress with the County
- Provide the facility with applicable site information that assists them based on the account profile
- Monitor ticket traffic
- Resolve escalation issues, as needed.

Each field service manager possesses the skills required to perform the duties of the field service technician and can provide additional or backup support as needed.

Field Service Technician (On-Site)

- Notify the site contact when on-site
- Perform on-site routine hardware maintenance on monthly
- Check each phone at a minimum of once month for problems
- Adhere to the contractually defined maintenance schedule
- Maintain a detailed log reflecting the date each phone was last checked
- Open service ticket to address all issues
- Repair faulty hardware as required

- Conduct additional on-site visits as requested by the Securus Field Service, or Territory Managers
- Track ticket history and closure as required by the Service Manager.
- Complete site visit log
- Serve as Securus liaison
- Attend safety meetings as required by the County
- Escalate issues as needed

The Contractor, in compliance with Texas Commission Jail Standards, provides the following positions, at a minimum, in support of this contract: **1. *IPS System Administrator*** **The IPS System Administrator position is a minimum full- time position, dedicated to Dallas County, directly responsible for overall operational performance of the contract, including account management, troubleshooting, training, and any other responsibilities agreed upon by the County and the Contractor. This individual shall have a minimum of three (3) years' experience within the last five (5) years at the management level, providing direct administrative oversight of telephone services.** **2. *Field Repair/Site Technician(s) (state number provided)*** **Field Repair/Site Technician positions shall be directly responsible for providing preventative maintenance on the system, shall assist with installation of equipment, provide technical support and repairs as necessary, assist in on- site instruction and provide training for Department personnel to ensure customer satisfaction. These individuals shall possess a High School Diploma or GED and have two years' minimum experience with a computer-based telephone system similar to the type required in this contract.** **3. *Service Representative(s) (state number provided)*** **Service Representative positions shall be directly responsible for making changes to the inmate phone access information including entering of approved inmate PIN and authorized calling numbers, verification of Billing Number Addresses, assistance to authorized County personnel, and shall provide**	**Y**	Please see comments below.

customer service relative to the Inmate Phone Service. These individuals shall possess a High School Diploma or GED, be computer literate and have related experience in the provision of services of the type required in this contract.		
Securus shall provide at a minimum four on-site technicians to serve Dallas County.		
Vendor can respond to all major service outages within two hours. Major outage is defined as the loss of 25% or more of the functionality of the system.	**Y**	Please see comments below.
Securus can respond to all major service outages within two hours.		
Vendor has established service policies and procedures (attach this to the response).	**Y**	Please see comments below.
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 Platform™ UI, all phones down.	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 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 • Technical Support Director & Field Service Director • VP Service & Operations
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 • Technical Support Director & Field Service Director • VP Service & Operations
P3	A P3 assignment defined as less the 5% of the functionality of the System	72 hours	• Securus Technical Support	• If response is delayed, escalation procedures within

		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.		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	Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request • Technical Support Manager & Field Service Manager • Technical Support Director & Field Service Director • VP Service & Operations

Vendor has an established maintenance and quality assurance program for telephones to be installed.	Y	Please see comments below.

Securus continually invests in technology and staff to maximize customer satisfaction. We do this through a comprehensive approach that includes our culture, our locally-sourced 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.

Dallas Area 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 Dallas County.

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 Dallas County will get accurate and timely reporting and commission 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.

Vendor has an established method of determining service interruptions and service call priorities. List response time for each priority and the level of expertise devoted to each priority.	Y	Please see comments below.

Service Response Times and Escalations

Priority Level	Service Priority Description	ResponseTime	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 Platform™ UI, all phones down.	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 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 • Technical Support Director & Field Service Director • VP Service & Operations
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,	24 hours	• Securus Technical Support Center notifies the facility when the service issue is resolved • If a technician is required,	• If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request

	unblocks, block numbers, missing CDRs, call searching.		Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival	• Technical Support Manager & Field Service Manager • Technical Support Director & Field Service Director • VP Service & Operations
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 • Technical Support Director & Field Service Director • VP Service & Operations •

System has remote diagnostic capability.	**Y**	Please see comments below.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services 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 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.

SolarWinds® Typical Monitored Application Elements

Average CPU Load & Memory Utilization
THRESHOLDS EDIT HELP

9 %
Avg CPU Load

57 %
Memory Used

Average Response Time & Packet Loss
THRESHOLDS EDIT HELP

0 ms
Avg Resp Time

0 %
Packet Loss

Monitored Sessions
EDIT HELP

22
TotalCalls

Current Sessions - MonitoredSessions
MIN/MAX Average Statistic Data
TODAY (Every Hour)

Top CPUs by Percent Load
EXPORT EDIT HELP

Mar 24 2019, 1:40 pm - Mar 25 2019, 1:30 pm

Zoom 1h 12h 24h

Network Latency & Packet Loss
EXPORT EDIT HELP

Mar 25 2019, 12:00 am - Mar 25 2019, 1:30 pm

Zoom 1h 12h 24h

X-Position: **672** px
Col Width: **462** px

☑ ▮ Response Time
☑ ▮ % Packet Loss

Disk Volumes
EDIT HELP

	VOLUME	SIZE	SPACE USED	
▯	C:\ Label: 346b9856	278.3 GB	55.2 GB	20 %
▯	D:\ Label:Data 2c7978c4	557.6 GB	164.6 MB	0 %
▦	Physical Memory	31.9 GB	18.2 GB	57 %
▤	Virtual Memory	36.7 GB	19.6 GB	53 %

Last Events
EDIT HELP
LAST 3 MONTHS

3/6/2019 2:36 PM	↺		rebooted at 3/6/2019 3:36:00 PM

Current Hardware Health
MANAGE SENSORS EDIT HELP

SENSOR NAME	STATUS	VALUE
▸ 🖥 Fan		
▸ 🔌 Power Supply		
▸ 🌡 Temperature		
▸ 💽 Disk		

Current Percent Utilization of Each Interface
EDIT HELP

STATUS	INTERFACE	TRANSMIT	RECEIVE	
● Up	🖧 Intel(R) Gigabit 4P I350-t rNDC - LAN1	0 %	0 %	☁
● Up	🖧 Intel(R) Gigabit 4P I350-t rNDC #3 - LAN3	0 %	4 %	☁
● Up	🖧 Microsoft Network Adapter Multiplexor Driver - Team#1	0 %	2 %	☁

Components
EDIT HELP

COMPONENT NAME	STATISTIC	MESSAGE	RESPONSE TIME	PORT
▦ ActiveCallsCurrent	440		0 ms	N/A
▦ ActiveCallsMax	465		0 ms	N/A
▦ CallDenialsCurrent	0		0 ms	N/A
▦ CallsTotal	749		0 ms	N/A

Hardware Details
EDIT HELP

🖥 Server

Hardware Status	Up
Manufacturer	▦ Dell Inc.
Model	PowerEdge R630
Service Tag	
Last Poll Time	3/25/2019 1:34:49 PM
Dell OpenManage	v9.1.0

Disk Volumes
EDIT HELP

	VOLUME	SIZE	SPACE USED	
▯	C:\ Label: 346b9856	278.3 GB	55.2 GB	20 %
▯	D:\ Label:Data 2c7978c4	557.6 GB	164.6 MB	0 %
▦	Physical Memory	31.9 GB	18.2 GB	57 %
▤	Virtual Memory	36.7 GB	19.6 GB	53 %

Application Overview

Application Count: 51

51	Up	0	Warning		
0	Critical	0	Down		
0	Unknown	0	Other		

Up

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.

SolarWinds® Facility Monitoring Example

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.

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. Additionally, change control practices have been reviewed and are compliant with Sarbanes-Oxley.

Securus Calling Platform Provisioning Standards

All Securus calling platforms interface with industry standard analog and digital provisioned telephony circuits, such as the following services:

- POTS (plain old telephone service)
- ISDN (Integrated Services Digital Network)
- PRI (Primary Rate Interface)
- DS-1/T-1 (Digital signal 1, also known as T1)
- DS-3 (Digital Signal 3)

The PRIs (Primary Rate Interfaces) provide detailed information for advanced call routing and call progression and enforce outgoing service for our legacy platforms. Our newest centralized, packet-based platform—NextGen SCP—uses MPLS (Multiprotocol Label Switching) circuits, DSL (Digital Subscriber Line), and POTS lines.

Hosted Video Visitation – Hardware Requirements

Inmate kiosks and visitor terminals include, at a minimum:
 	
    • **A detention grade hardened steel enclosure with rounded corners which prevents spills from entering the enclosure**
    • **A shatterproof 15-inch minimum LCD or larger touchscreen monitor**
 	
    • **A camera**
 	
    • **One detention grade audio handset per terminal, or two detention grade audio handsets per terminal**
    • **H.264 standards based videoconferencing Encoder/Decoder**
 	
    • **Assembled from non-proprietary, off-the-shelf computer components**
	Y	Please see comments below.

Video visitation terminals are configured to meet the County's requirements.

The Securus ConnectUs terminal, which provides video visitation, is a correctional facility grade, tamper-proof steel enclosure. The wall-mounted terminal has a shatterproof touchscreen, a high-resolution video camera with integrated lighting, and tamper-proof, and a heavy, molded plastic handset with an armor-reinforced cord for audio communication.

The proposed SVV terminals include, at a minimum, the following:

- A correction grade hardened steel enclosure
- One correction grade audio handset per terminal for the inmate, and two detention grade audio handsets per terminal for the public
- A shatterproof LCD monitor with adjustable, integrated, infinity lens camera
- Spill-proof enclosures
- Terminals without openings exposed to the user, including all wiring and ventilation holes
- Terminals without any external hinges
- Terminals that are powered by 110 VAC
- 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 a standards-based video conferencing CODEC
- Options for re-booting the unit

Terminal can access the web-based application and be enabled for touch screen inputs.	**Y**	Please see comments below.

A decade ago, it was hard to imagine that your correctional facility would need anything more than a telephone on the wall for inmate communications. Today, there are a wide variety of communications options and the device on the wall can be used for so much more than telephone calls.

ConnectUs™ is Securus' vision for the future of inmate communication and self-help services. ConnectUs™ includes an integrated video terminal that facilitates access to Securus and third-party services through a common interface. Your facility can completely manage what an inmate can or cannot do through the ConnectUs™ software.

The ConnectUs™ software enables users to perform multiple operations, similar to a smartphone. Inmates can place a telephone call or join a video visitation session, read a digital inmate handbook, submit a grievance, watch a tutorial video or place a commissary order.

ConnectUs™ also manages which applications are available to inmates and when. It ensures that a scheduled visit is not interrupted by another inmate placing a telephone call or using the device to place a commissary order. Moreover, other vendors easily create and publish an application for use by your inmates through ConnectUs™.

Imagine turning your existing hardware into multi-purpose inmate communication devices...

Which present a familiar interface that completely controls **_everything_** an inmate is presented with...

Yet provides unprecedented communication access within the facility and beyond...

Providing automated reporting compliance, and conflict management...

With an infinite ability to scale—allowing quick implementation of whatever the "next" app might be...

Inspired Design

ConnectUs™ is a collection of intentional details that add up to an impressively powerful inmate communication platform that consolidates all inmate activities into a single unified interface. With a customized mix of applications, your facility can deliver an experience that keeps pace with today's technology while making life better for your inmates and staff.

Multi-language   Digital Bulletin Board   BIG Buttons

Multi-task   Conflict Resolution   Touch Screen

1. Conflict Resolution

ConnectUs™ manages available applications by the time of the day or day of the week. This allows for information applications, such as an inmate handbook, to be available during non-calling hours. ConnectUs™ automatically prioritizes scheduled communication events higher than non-scheduled communication events. If a video visitation is scheduled and another inmate wants to use the same terminal for a telephone call, ConnectUs™ will limit the call duration to avoid conflict with the video visitation session. Similarly, the Telephone Calling Application is disabled when a video visit is scheduled to begin. We manage usage conflicts, so your staff does not have to.

2. Applications

ConnectUs™ provides an "app store" environment where new functionality can quickly and easily be developed and delivered to the inmate.

3. Date/Time

ConnectUs™ continually displays date and time so inmates can manage their schedules and not miss or be late to scheduled communication events.

4. Multi-Language

ConnectUs™ supports the ability to display applications in multiple languages – allowing inmates to use the system in their preferred language and enhancing your facility's support of non-English speaking inmates.

5. Digital Bulletin Board

ConnectUs™ allows you to easily publish notifications that are always displayed on the ConnectUs™ terminal. In addition to providing pertinent facility-related information, these messages can be used to promote new products, services, and promotions such as Video Visitation.

6. Multi-Tasking

ConnectUs™ allows an inmate to use multiple applications at the same time. They can be on telephone call while reading the inmate handbook, or placing a commissary order, or

submitting a grievance. The ability to multi-task allows inmates to accomplish tasks quickly instead of unnecessarily preventing other inmates from using the terminal.

Inmate Telephone Application

Inmates can speak to loved ones using the calling services of our NextGen Secure Communications Platform™ (NextGen SCP™). NextGen SCP delivers the latest in inmate calling technology with improved call quality, more effective investigative tools, and greater flexibility and scalability for future growth. New technologies are applied immediately through quarterly upgrades provided at no cost.

Inmates can place calls with the same ConnectUs™ terminal they use to conduct a video visitation or submit a grievance. All communications are 100 percent monitored and completely secure.

Benefits

- Security
- Controlled Access
- Minimal Disruption
- Easy User Experience
- Multi-purpose device allows more capabilities with less hardware

Video Visitation Application

Nothing beats the ability to "see" a loved one, and Securus Video Visitation makes that and much more possible. While a friend or family member visits from the comfort of their home or office, an inmate visits from their pod, eliminating the need to move the inmate inside the facility.

SVV is a fully web-based visitation system that allows family, friends, attorneys, and public defenders to schedule and participate in video visitation sessions with an inmate – from any computer connected to the Internet. Integration phone calling and video visitation onto a common platform maximizes facility revenue and improves investigative capabilities.

Benefits

- Security
- Controlled Access
- Minimal Disruption
- Easy User Experience
- Multi-purpose device allows more capabilities with less hardware

Inmate Request Form Application

Valuable time is lost every day when officers have to process inmate requests manually. Worse yet, every request must be hand written and there is no easy way to maintain accurate records. This creates unnecessary liability for your facility and leaves inmates believing their requests have been ignored.

Inmates can electronically create and track requests through ConnectUs™ and staff can easily review, respond, and process requests. Requests and responses are tracked and saved for future reference. Two-way communication with inmates could not be easier.

Benefits

- Allow any number of forms made available electronically
- Define custom routing of forms to the correct person
- Enables two-way communication so inmates to receive an electronic response
- Documents and archives all communication

Grievance Application

Grievance administration is often one of the most complicated and manually laborious processes in a correctional facility. Certain inmate rights must be honored, facilities must respond within strict timelines, and all actions must be properly documented. Failure to do so comes with large penalties and fines and creates legal liability.

The Grievance Application is a form submission and routing tool that allows inmates to submit grievances electronically. Correctional staff can then electronically prioritize, route, and respond to the submissions.

Benefits

- Create multiple inmate forms with individualized routing processes
- Configure the Grievance Application to process multiple types of forms and custom routing based on the type of form submitted
- Require responses from jail staff to validate that the response was received
- Eliminate manual administration/paper-handling of grievance forms

How the Grievance Application Works

- First, Securus was pleased to develop and implement a customized grievance system for Dallas County and Parkland Hospital.
- Each form can have an individualized routing process. A medical form can be electronically delivered to your medical staff while all other forms go to your grievance officer.
- Routing can also include an appeals process. If inmates are allowed to appeal a grievance response, the form can automatically be routed to a different member of your staff tasked with managing appeals.
- Inmates access the Grievance Application through ConnectUs™, where they can view and manage existing submissions or create new requests.
- Your staff will use Securus' centralized platform, NextGen SCP™, to view and track all grievances. All steps within the grievance process are time and date stamped to ensure compliance with all necessary standards. A customized Grievance widget within NextGen SCP allows you to process grievances quickly and easily.

Commissary Application

ConnectUs™-enabled devices continue to be useful even when telephone and visitation hours have passed. For example, the devices can be used to place commissary orders. Securus has multiple integration options to display third-party vendors' applications or integrate directly with your facility. Providing inmates better access to a commissary application can have an immediate impact on commissary revenue.

Benefits

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

Inmate Handbook Application

A digital version of your inmate handbook can be accessed through The Inmate Handbook application on ConnectUs™. Inmates can access information without printing or distributing a single piece of paper. Digital versions of other important documents can be available on ConnectUs™ in addition to the Inmate Handbook.

Benefits

- Reduces/Eliminates printing/distribution costs
- Reduces staff workload distributing and replacing handbooks
- Provides instant, electronic updates to documents

Video Education Application

ConnectUs™ provides the ability to upload any MP4 video. Everything from a video version of your inmate handbook, a jail orientation video, or a video tutorial on how to use ConnectUs™ is possible. You can make the video available for viewing any time or only during defined hours.

Benefits

- Communicate information to all inmates, even those unable to read
- Provides a form of communication that is often easier to comprehend, ensuring your message is understood
- Provides educational videos without staff involvement

Prepared for What's Next

The ConnectUs™ platform always remains up to date through regular updates. The platform can be customized to meet your needs and has the flexibility to handle whatever is next. In fact, using standard application programming interfaces, this innovative platform enables almost limitless integration with virtually any application, today or in the future.

Securus' mission is to deliver valuable solutions to our customers through technology. This thinking drives all we do. ConnectUs™ is the latest Securus technological innovation designed to improve the safety of your staff, inmates, and simplify facility operations.
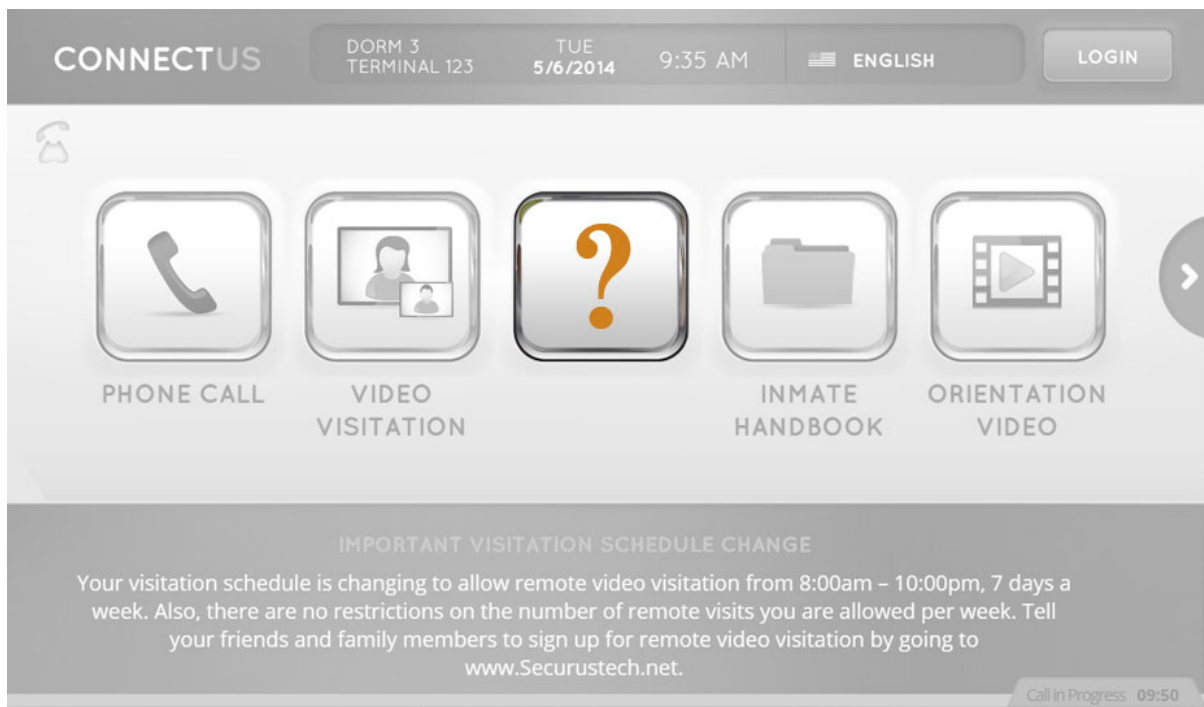
Terminal does not have any openings exposed to the user. This includes all wiring and ventilation holes.	**Y**	Please see comments below.
Our terminals do not have any openings exposed to the user.		
Terminal has built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes and / or disables during all other functions.	**Y**	Please see comments below.

Our terminals have 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.

Terminal has the option for one or two handsets or a hands free device.	**Y**	Please see comments below.

Securus terminals have the option for one or two handsets or a hands free device.

Terminal has sufficient ventilation fans and vents to allow for proper cooling.	**Y**	Please see comments below.

Securus terminals have sufficient ventilation fans and vents to allow for proper cooling.

Proposed terminal for use in inmate areas meets standards for space utilization and equipment as defined by the Texas Commission on Jail Standards.	**Y**	Please see comments below.

Our Proposed terminal for use in inmate areas meets standards for space utilization and equipment as defined by the Texas Commission on Jail Standards.

Provide wireless/rechargeable Kiosk/phone capability where needed - West Tower/Single Cell designated areas	**Y**	

Securus will provide wireless/rechargeable Kiosk/phone capability where needed.

Has the capability to provide tablet technology to compliment the kiosk/video visitation.	**Y**	

Securus has a best-in-class tablet program that can allow inmates to use many of the same features available on our kiosks, including, but not limited to, integrated inmate telephone calls, job search, law library and sick call. In addition, our tablets can complement the kiosks with applications like forms and grievances and inmate educational courses. For a comprehensive overview of our SecureView Tablet program, please refer **to Exhibit E**.

Hosted Video Visitation - Software Requirements

Software updates free of charge to Dallas County.	**Y**	Please see comments below.

We recognize that the challenges you and your officers face every day never stop evolving. When we designed our centralized platform, one of our chief objectives was deploying a system that provided upgrades to all customers at regular intervals with no downtime. We achieved that objective with NextGen SCP™. Securus provides upgrades to all of our customers three to four times annually through a proven and tested after-hours process that allows all sites to immediately realize the benefits each upgrade. Our system delivers proven features driven by input from the most recognized corrections and law enforcement agencies in the nation.

Maintenance events are preceded by an announcement displayed at login notifying the facility of the upcoming upgrade and new features are announced to customers prior to

implementation. These system updates are more than simple changes. They provide meaningful features and new capabilities, which drive greater officer and community safety, staff efficiency and improved investigative response times.

The following image shows the announcement widget, which appears for all users on the NextGen SCP dashboard, and notifies users of upcoming maintenance and upgrades.

Announcement Widget

Capability to scan and add paper documents into existing inmate grievance electronic files - DCSD needs the ability to add a paper documents to an existing electronic grievance submitted by an Inmate	**Y**	Please see comments below.
Grievances can be manually input to provide this function, which is currently in development and will be made available to the County upon completion.		
The system includes visitation scheduling, user management, policy management software, is web-based and allows for administration of visitation sessions and visitation operations based on Dallas County policies.	**Y**	Please see comments below.
Securus recognizes the importance of allowing inmates to stay connected with friends and loved ones while incarcerated. We strive to increase video visits while also giving the facility the control it needs to ensure inmate, staff and public safety. Video visitation rules are highly customizable to adapt to Dallas County visitation policies.		

User Registration

Friends and family members may use any standard web browser to schedule visitation sessions for approval. Securus Video Visitation (SVV) makes the complex tasks of scheduling sessions and managing user accounts easy and secure for the facility, the friend or family member, and the inmate. The lists below provide some of the associated features and functions – inherent in SVV – required for successful deployment.

User Account Set-up and Scheduling Features for Family and friends Members

- Web-based and accessible from any standard web browser
- Simple user interface, enabling account setup and scheduling to be completed in minutes
- Automatically support multiple facilities in multiple locations with multiple housing units, making it easy to "find" the desired inmate
- Automatically display only the visitation times and dates that are available
- Automatically send an email confirmation when a visit is scheduled, modified, or cancelled
- Allow users to easily change their personal information (password, address, phone number, etc.)

Secure, At-Home Visitation Scheduling

User Account Control and Scheduling Features for the Facility

- Secure, web-based access anytime/anywhere – providing different levels of authority and requiring unique usernames and passwords
- Point and click to view thorough user information including photo ID and easily approve or reject user account
- View, manage, report, and modify scheduled visits from the Securus Video Visitation dashboard
- Review historical staff usage through system user logs

Scheduling Features for Inmates

- Terminals with simple touch screens and user friendly, basic icons - providing inmate access in English, Spanish, and any other language requested by CCSO
- Large letters and numbers that clearly display pending visits
- Built in lighting to enhance screen images
- On screen timer to show remaining time left for visitation

Visitor Registration and Approval

Securus Video Visitations visitors are required to provide both a photo of themselves and photo of identification (e.g. driver's license) during registration for Dallas County staff approval prior to a visitation session for user creation.

Visitor Profile Page

Visitors can easily register from any web-enabled device by going to www.securustech.net. When the facility staff approves the account request, the visitor receives an email notification that they have been approved and can now schedule their visit.

Attorneys have a separate registration process from the general public. Attorney accounts will require additional verification, such as a Bar ID.

After completing the process, facility personnel must approve and authorize the user's registration before visitation sessions can be scheduled. This process allows the County to verify a visitor's eligibility to visit with an inmate. NextGen SCP brings a new option to visitor approval. Dallas County can choose to manually approve all visitors or have the system automatically approve visitors. If automatic approval is the default, Dallas County staff can always review the contact profile and manage the visitor as needed.

24-Hour Buffer

When scheduling an appointment on the SVV system, there is a waiting period, or "buffer," between the time the visit is scheduled and when it takes place. The minimum buffer time is configurable between 1 and 48 hours, based on the needs of Dallas County. The SVV system's default setting requires at least a 24-hour buffer period. However, Dallas County can bypass the waiting period and schedule a visitation session within the 24-hours.

Visitation Scheduling Page

Visitation Rules

Visit Rules allow Dallas County to set up rules that determine the frequency of visitation by user, terminal, location, user group, and site. This feature allows authorized facility personnel to create and enforce rules, such as allowing the inmate user group to have a maximum of two on-site visits per week. Visitation Rules do not apply to Emergency calls.

Visitation Rules are accessed through the "Admin" menu.

Creating New Visitation Rules

While in the Visit Rules section, click on "Create Visit Rule" to create a new Visitation Rule.

Create a New Rule

From here, you will define a rule name, and configure the following fields:

- **Status:** Active or inactive
- **Visit Rule Settings**: select the date for the rule to start and stop.
- **Visitor Types:** Home user, attorney, unregistered visitor, visitor
- **Visit Type**:
  - Onsite: Standard on-site visit
  - Remote: Applies to both friends & family home user and attorney home user
- **Rule Reset**: Daily, weekly, or monthly
- **Rule Applied On**: Apply the rule to a specific location

During the creation of a rule, the rule can be associated with a user, terminal, location, user group, or site. Users can create a new rule without an initial association. However, new rules

will not be in effect until there is, at least, one entity associated. Associations, in order of priority, are as follows:

- **User Association**: Rule applies only to a specific Inmate or user
- **Terminal Association**: Rule applies to a specific terminal. This is a cumulative rule applied to the Terminal only – NOT the users under the Terminal*
- **Location Association**: Rule applies to a specific location such as a pod. This is a cumulative rule applied to the Location only – NOT the users under the Location*
- **User Group Association**: Rule applies to every member of the user group to which the rule is associated
- **Site Association**: Rule applies holistically to the Site. This is a cumulative rule applied to the site only – NOT the users under the Site*

The behavior of cumulative rules will soon change such that the rule will apply to all users at the association level.

Rules are also prioritized based on the association level in which they are applied. For example, a visitation rule applied to a User (highest priority) takes higher priority than a rule associated with a Site. This means that if there is a Site level rule that allows inmates to have one on-site visit per 1 month and a User level rule for a specific inmate to have five on-site visits per 1 month, the User level rule take priority.

Example Visitation Rule:

- Rule Name: 2 Visits per Week
- Visitation Type: Onsite
- Quantity: 2
- Frequency: 1
- Duration: Week

Reads: 2 onsite visits per 1 week

If two rules with the same priority conflict, both rules will need to pass to schedule and appointment. An example of this conflict is an Inmate User Group visitation rule to allow one on-site visit per week and an Attorney User Group visitation rule that allows five on-site visits per week. Both rules must pass to schedule a visit.

Associating Visit Rules

Enforcement of a Visit Rule requires association with a user, terminal, location, user group, or site. There are two ways to associate a rule:

- From the Manage > Visits or Visitors menus
- From the Inmate profile page

Editing Visitation Rules

Editing or deleting a visit rule can be accomplished from several different pages, including:

- Admin > Visit Rules
- Manage > Inmates > Visit Settings
- Manage > Visitors

When editing a visitation rule, you can modify all components of the rule as well as add and delete associations. A popup showing the number of impacted sessions displays before saving a rule change. This prevents the unintentional cancellation of previously scheduled visits.

If the rule change does not impact scheduled appointments, a confirmation popup will appear.

Logging

Then NextGen Secure Communications Platform™ (NextGen SCP™) logs all changes to Visit Rules, and this log is accessible from the Explore > System Logs menu.

Logging Changes

Example log outputs include:

Example Log Output

Bypass Visitation Rules and Buffer

NextGen SCP allows authorized facility administrative users to bypass visitation rules and visitation buffers when scheduling appointments for the public.

Bypass Visitation Rules

Example: Facility requires 24 hours visitation buffer and has an active visitation rule that allows inmates to have two on-site visits per week. The facility can choose to override both the buffer policy and visitation rule by choosing "Overrides" and the type of bypass while scheduling the visit.

Appointments scheduled in "Bypass" mode are NOT counted towards visitation rules but will be logged in the system log.

Security Permissions

NextGen SCP security permissions have been modified to accommodate the Visit Rules feature. Facilities that have multiple administrator groups will not be automatically updated.

System includes scheduling, automation, policy management and usability functionality: i. The system assigns a unique identification number to each inmate and user. ii. The system has a multi-lingual interface (English and Spanish at a minimum) iii. The system provides ad-hoc 1-to-1 or 1-to- many chat sessions between authorized users. iv. The system supports multiple facilities in multiple locations with multiple housing units.	**Y**	Please see comments below.

v. The system provides web-based visitation scheduling for authorized users (Corrections Services staff, attorneys, the public) utilizing any standard web browser. **vi. The system displays pending visits** **vii. The system allows users to easily and simply schedule visitation sessions.** **viii. The system requires visitors to provide photo ID for a visitation session.** **ix. The system only displays timeslots that meet Dallas County policies.** **x. The system conducts conflict checking and display times which are available.** **xi. The system allows users to easily change their personal information (i.e., password, address, phone number, etc.).** **xii. The system sends an email to a visitor when a visit is scheduled, modified, or cancelled.** **xiii. The system is capable of rescheduling a timeslot if a scheduled visit is cancelled.** **xiv. The system assigns unique visitation identification numbers for every visit for reporting and tracking.** **xv. The system uses set durations based upon Dallas County policies for each visit.**		

NextGen SCP includes scheduling, automation, policy management and usability functionality:

i. The system assigns a unique identification number to each inmate and user.

ii. The system has a multi-lingual interface (English and Spanish at a minimum)

iii. The system provides ad-hoc 1-to-1 or 1-to- many chat sessions between authorized users.

iv. The system supports multiple facilities in multiple locations with multiple housing units.

v. The system provides web-based visitation scheduling for authorized users (Corrections Services staff, attorneys, the public) utilizing any standard web browser.

vi. The system displays pending visits

vii. The system allows users to easily and simply schedule visitation sessions.

viii. The system requires visitors to provide photo ID for a visitation session.

ix. The system only displays timeslots that meet Dallas County policies.

x. The system conducts conflict checking and display times which are available.

xi. The system allows users to easily change their personal information (i.e., password, address, phone number, etc.).

xii. The system sends an email to a visitor when a visit is scheduled, modified, or cancelled.

xiii. The system is capable of rescheduling a timeslot if a scheduled visit is cancelled.

xiv. The system assigns unique visitation identification numbers for every visit for reporting and tracking.

xv. The system uses set durations based upon Dallas County policies for each visit.

System provides a visual warning message to inform the visitor that the session will be ending in "XX" minutes.	**Y**	Please see comments below.

When live monitoring a video session, Facility Administrators will see a countdown clock for the time remaining on the session.

Visit Countdown Clock

System provides different levels of functionality to users based on user type. For example: **i. Administrators: create/manage/edit – users, schedules, etc.** **ii. Users: create/manage/edit their own schedules** **iii. Read-only user: can only view scheduled visits**	**Y**	Please see comments below.

Using a centralized infrastructure ensures that all aspects of the solution are hosted and managed in an efficient manner. User management of the video communications process including point-to-point connection, scheduling, security, user identification, user management, as well as system usage auditing, reporting, and billing, is achieved through a simple yet powerful web-browser-based interface.

The SVV scheduling application automatically schedules visits according to the housing location of the inmate in the facility, which terminals are available to that specific housing location, and available times for video visitations to be held. Non-visitation hours can be restricted globally by hour and day of the week or by housing location or pod.

Sheriff's Office jail personnel can easily review all upcoming appointments within a specified time frame and can cancel visitations, with an email or SMS text message notification. There is full administrative control, such as create/edit/delete users, employ a variety of visitation rules, scheduled visits, view usage reports, and audit reports

System requires a unique username and password that will dictate to the user their level of functionality.	**Y**	Please see comments below.

All users are required to sign in using their unique username and password. SVV automatically tracks all activities, which can be viewed by administrators at any time, using the user information. All visitation sessions are tagged with a unique session identifier within the SVV system		
System provides information for tracking inmate and visitor activities and patterns by, at a minimum, the following: **i. Inmate booking number** **ii. Inmate name** **iii. Visitor name** **iv. Date and time of visit** **v. Inmate video visitation station and** **vi. Daily, weekly and monthly visit statistics**	**Y**	Please see comments below.
NextGen SCP provides information for tracking inmate and visitor activities and patterns by, at a minimum, the following: i. Inmate booking number ii. Inmate name iii. Visitor name iv. Date and time of visit v. Inmate video visitation station and vi. Daily, weekly and monthly visit statistics		
System provides an audit trail of all activity (i.e., user login times and locations, which users have scheduled/modified/cancelled a visit, etc.).	**Y**	Please see comments below.
SVV provides full audit tracking. All transactions on the system are logged and time-stamped, providing 100 percent traceability. The system allows authorized facility administrators to generate custom Recorded Session Details and Appointment Details reports, which can be exported in multiple common formats such as Microsoft Excel, CSV, and PDF.		
System provides for an Exclusion List which allows Dallas County to set visitor exclusions (i.e., Visitor A is allowed to visit with anyone in the jail EXCLUDING one or more selected inmates) because they are known gang affiliates, contraband smugglers, etc.	**Y**	Please see comments below.
The SVV system includes a User Exclusion List feature that allows authorized Dallas County users to restrict friends and family, and inmate, visitation eligibility within the SVV application. This Block or Allow list functionality is configurable on a site level. # Personal Visitation List		

A Personal Visitation List (PVL) allows authorized Dallas County users to manage family, friends, and attorney eligibility to visit with an inmate within the NextGen Secure Communications Platform™ (NextGen SCP™). Dallas County can select to configure PVL for their facility either as a "Blocked List" or "Allowed List." This functionality is then available at the site or facility level depending on the configuration of visitor approval.

- **Blocked List**:　　Provides a list of visitors who are blocked from visiting with a selected inmate. The Block List does not have a maximum number of entries. It is the standard PVL configuration for sites upon deployment. The facility, when configured for a Blocked List, has the option to hide the inmate name from the search list during visitation scheduling for a visitor on their PVL. In addition, custom messaging can also be set to appear.

- **Allowed List**:　　Provides a list of visitors who are approved to visit with a selected inmate. The inmate would not be allowed to visit with anyone not on their PVL. This selection requires Dallas County staff to approve the visitor and the visitor's request to visit a specific inmate. Dallas County determines a maximum number of allowed visitors per inmate. After the maximum number of entries is reached, Dallas County staff must delete an existing visitor before adding a new one. This type of list can be very restrictive but is useful for facilities that need the highest levels of control over visitors.

Accessing the Inmate Personal Visitation List

The PVL feature indicates the number of current active PCL entries and the date of last update. Authorized Dallas County users can manage—add, edit, or delete—PVL entries for inmates through either the Inmate Dashboard or the Inmate Profile page. Changes to the inmate PVL prompt a warning to appear, notifying the Dallas County user if any previously scheduled appointments violate the change in PVL.

Impacted Visits Warning

IMPACTED VISITS

3 Previously Scheduled Appointments are in violation of this change

Visit ID	Visit Date/Time	Duration	Inmate	Visitor Type	Visitor	Relationship
100000442	10/24/2018 07:30 pm CDT	15		NG Visitor		Facility Admin
100000466	10/25/2018 07:15 am CDT	10		NG Visitor		Facility Admin
100000467	10/24/2018 10:45 am CDT	15		Home User		Aunt

How would you like the system to handle impacted visits?

Select an option

○ Move visits that can be moved and **CANCEL** others.
● Move visits that can be moved and **DO NOT CANCEL** others.

Cancel   **Confirm**

IMPACTED VISITS

0 Previously Scheduled Appointments are in violation of this change

Cancel   **Confirm**

The visitor's Contact Profile page also identifies any active entries on an inmate's PVL. When the Contact Profile page has an active entry, that means the visitor has been listed on an inmate's PVL. Click the "active entries" link on the profile page to see on which inmate PVL the visitor appears. In the following example, the visitor appears on the PVL of one inmate; when selected, the hyperlink opens the inmate's PVL.

Contact Profile with PVL Entry

System provides Cancellation/Interruption Broadcast capabilities. The Dallas County staff will be able to interrupt ongoing visits and deliver either audible, written, or video message (warnings), as well as having the capabilities of reconnecting the session back together.	Y	Please see comments below.

SVV Barge In allows Dallas County staff to break in to an ongoing video visitation session to send a pre-defined visual message. This message can be delivered to the inmate, the visitor, or both parties simultaneously, in English or a second language. This feature is available in both single session and multi-session monitoring.

This text-based barge-in feature automatically captures the sent message and other pertinent data and includes it as a part of the visitation communication detail record(CDR) . An indicator on the CDR denotes that the Barge In feature was used during the video visitation session.

Authorized Dallas County users can search the system CDRs for visitation sessions where the Barge In feature was used.

To provide Dallas County additional control and options, Barge In can be configured at the site level, and each site can have a unique list of messages from which staff can choose.

SVV Barge In Messages, Facility View
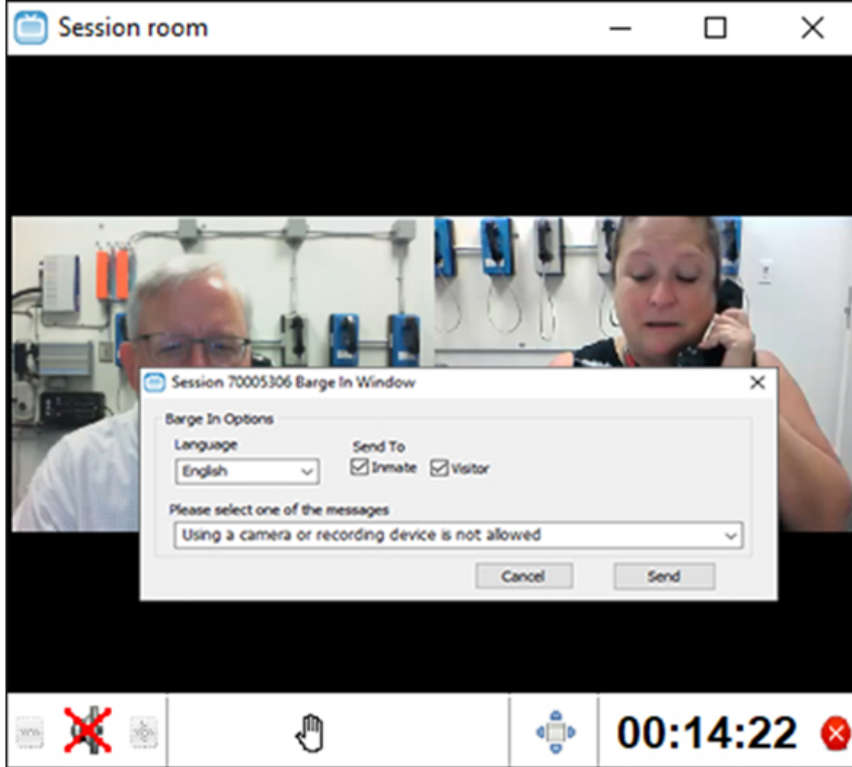
SVV Barge In Messages, Inmate View
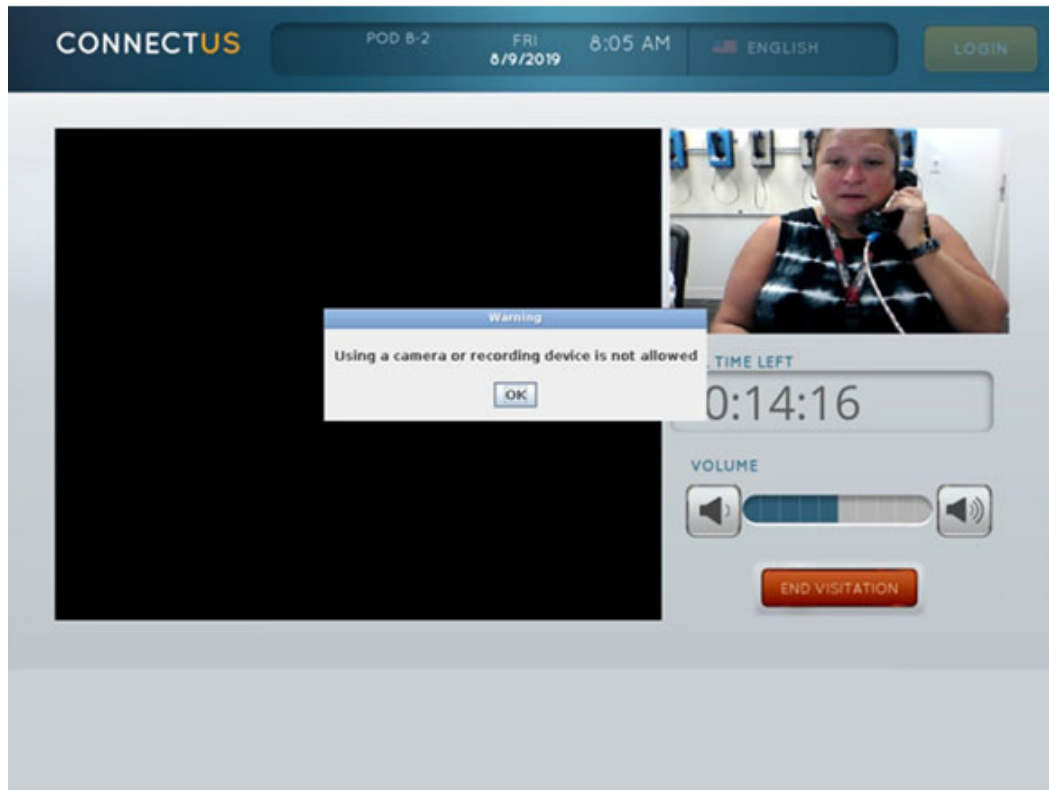
The following table provides some examples of Barge In messages.

Sample Barge In Messages

English	Spanish
STATEMENT	
All visitors must follow the proper dress code	Se requiere que los visitantes sigan el código de vestir
Using a camera or recording device is not allowed	No se permite el uso de cámaras o dispositivos de grabación
Do not drive while using video visitation	No se debe manejar mientras se está usando visitación en video
Registered user must always be present	El usuario inscrito siempre tiene que estar presente
You cannot lay in the bed while visiting	No se puede tenderse en la cama durante la visita
WARNING	
WARNING: Policy violation – Visit may be terminated	AVISO: Violación de política – Se puede terminar la visita
WARNING: Gang signs are not allowed	AVISO: No se permiten señas de pandillas
WARNING: Displaying weapons of any type is not allowed	AVISO: No se permite mostrar ningún tipo de arma
TERMINATION	
Visit will be TERMINATED for violating the rules	La visita será TERMINADA por violar las reglas
Visit will be TERMINATED for violation of dress code	La visita será TERMINADA por violar el código de vestir
Visit will be TERMINATED for handing over to another inmate	La visita será TERMINADA por pasar la llamada a otro recluso
Visit will be TERMINATED for nudity	La visita será TERMINADA por desnudez

System provides for an Inmate Visitation Request which will allow an inmate to request a visit by filling out a form on the visitation terminal and choosing whether to deliver the pre-populated messages via text/voicemail/email.	**Y**	Please see comments below.
Securus Video Visitation provides for an Inmate Visitation Request which will allow an inmate to request a visit by filling out a form on the visitation terminal and choosing whether to deliver the pre-populated messages via text/voicemail/email.		
The system provides authorized users the ability to do searches and create reports.	**Y**	Please see comments below.
Authorized Dallas County users can generate communication reports on all Securus Video Visitation (SVV) events through the NextGen Secure Communications Platform™ (NextGen SCP™) user interface. Dallas County users can perform a dynamic search using the single-input omnibox or an advanced search.		

Searching for SVV Events
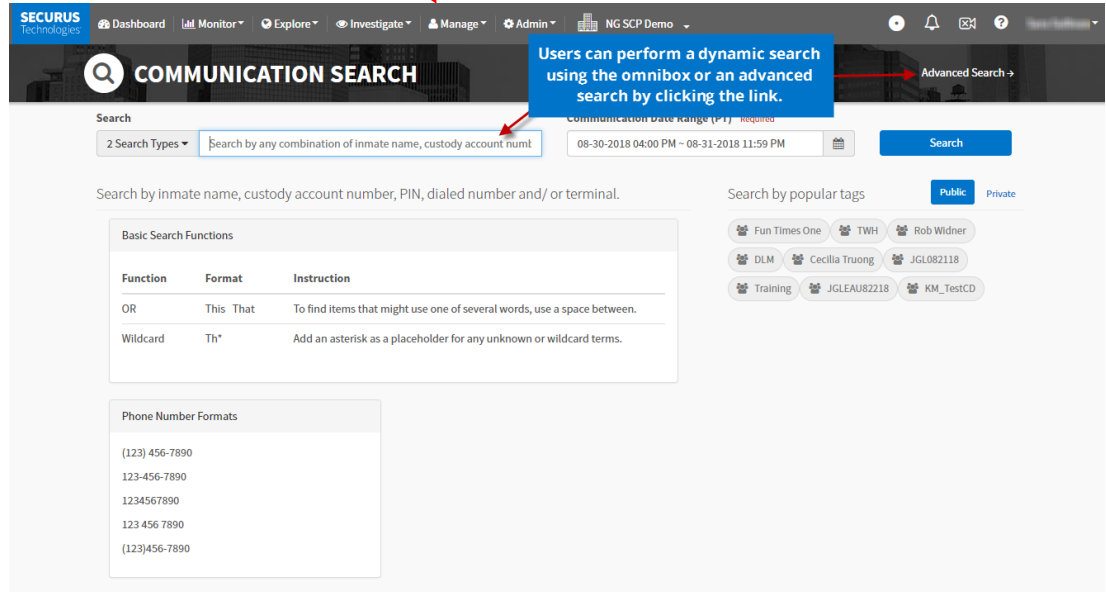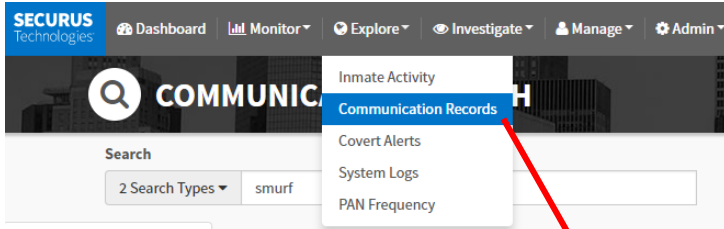
Advanced Search for SVV Communication Records

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 Visitation Communication Detail Report

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

Exporting Results

System provides a way to display scheduled visits to Staff so they know where and when an inmate needs to be available for pending video visits.	**Y**	Please see comments below.
Authorized Dallas County personnel can easily review all upcoming appointments within a specified time frame and can cancel visitations, with an email or SMS text message notification. There is full administrative control, such as create/edit/delete users, scheduled visits, view usage reports, and audit reports		
System shall allow for visitation recording. **i. Visits will be recorded ad-hoc, by user type, or selected when scheduling the visit** **ii. Recorded visits will be searchable and viewable** **iii.Recorded visits will be stored for 90 days** **iv. Dallas County can lock certain recordings such that they will not be purged as part of the standard retention duration**	**Y**	Please see comments below.
Securus Video Visitation allows for visitation recording, including the following abilities: i. Visits will be recorded ad-hoc, by user type, or selected when scheduling the visit ii. Recorded visits will be searchable and viewable iii.Recorded visits will be stored for 90 days iv. Dallas County can lock certain recordings such that they will not be purged as part of the standard retention duration		
System provides for a Visitation Rules Server that allows for configurable rules to be established in order to encourage usage and minimize the number of people in the lobby. Visitation rules are configurable for both detailed and promotional rules that will automate subscriber promotions such as discounted/free visits (i.e., one free visit per new subscriber, one free visit per inmate, etc.).	**Y**	Please see comments below.
Visit Rules allow Dallas County to set up rules that determine the frequency of visitation by user, terminal, location, user group, and site. This feature allows authorized facility personnel to create and enforce rules, such as allowing the inmate user group to have a maximum of two on-site visits per week. Visitation Rules do not apply to Emergency calls. Visitation Rules are accessed through the "Admin" menu. Select "Visit Rules" from the drop-down menu.		

Visitation Rules

Creating New Visitation Rules

While in the Visit Rules section, click on "Create Visit Rule" to create a new Visitation Rule.

Create a New Rule

From here, you will define a rule name, and configure the following fields:

- **Status:** Active or inactive
- **Visit Rule Settings**: select the date for the rule to start and stop.
- **Visitor Types:** Home user, attorney, unregistered visitor, visitor
- **Visit Type**:
  - Onsite: Standard on-site visit
  - Remote: Applies to both friends & family home user and attorney home user
- **Rule Reset**: Daily, weekly, or monthly
- **Rule Applied On**: Apply the rule to a specific location

During the creation of a rule, the rule can be associated with a user, terminal, location, user group, or site. Users can create a new rule without an initial association. However, new rules will not be in effect until there is, at least, one entity associated. Associations, in order of priority, are as follows:

- **User Association**: Rule applies only to a specific Inmate or user
- **Terminal Association**: Rule applies to a specific terminal. This is a cumulative rule applied to the Terminal only – NOT the users under the Terminal*
- **Location Association**: Rule applies to a specific location such as a pod. This is a cumulative rule applied to the Location only – NOT the users under the Location*
- **User Group Association**: Rule applies to every member of the user group to which the rule is associated
- **Site Association**: Rule applies holistically to the Site. This is a cumulative rule applied to the site only – NOT the users under the Site*

The behavior of cumulative rules will soon change such that the rule will apply to all users at the association level.

Rules are also prioritized based on the association level in which they are applied. For example, a visitation rule applied to a User (highest priority) takes higher priority than a rule associated with a Site. This means that if there is a Site level rule that allows inmates to have one on-site visit per 1 month and a User level rule for a specific inmate to have five on-site visits per 1 month, the User level rule take priority.

Example Visitation Rule:

- Rule Name: 2 Visits per Week
- Visitation Type: Onsite
- Quantity: 2
- Frequency: 1
- Duration: Week

Reads: 2 onsite visits per 1 week

If two rules with the same priority conflict, both rules will need to pass to schedule and appointment. An example of this conflict is an Inmate User Group visitation rule to allow one on-site visit per week and an Attorney User Group visitation rule that allows five on-site visits per week. Both rules must pass to schedule a visit.

Associating Visit Rules

Enforcement of a Visit Rule requires association with a user, terminal, location, user group, or site. There are two ways to associate a rule:

- From the Manage > Visits or Visitors menus
- From the Inmate profile page

Editing Visitation Rules

Editing or deleting a visit rule can be accomplished from several different pages, including:

- Admin > Visit Rules
- Manage > Inmates > Visit Settings
- Manage > Visitors

When editing a visitation rule, you can modify all components of the rule as well as add and delete associations. A popup showing the number of impacted sessions displays before saving a rule change. This prevents the unintentional cancellation of previously scheduled visits.

If the rule change does not impact scheduled appointments, a confirmation popup will appear.

Logging

Then NextGen Secure Communications Platform™ (NextGen SCP™) logs all changes to Visit Rules, and this log is accessible from the Explore > System Logs menu.

Logging Changes

Example log outputs include:

Example Log Output

Bypass Visitation Rules and Buffer

NextGen SCP allows authorized facility administrative users to bypass visitation rules and visitation buffers when scheduling appointments for the public.

Bypass Visitation Rules

Example: Facility requires 24 hours visitation buffer and has an active visitation rule that allows inmates to have two on-site visits per week. The facility can choose to override both the buffer policy and visitation rule by choosing "Overrides" and the type of bypass while scheduling the visit.

Appointments scheduled in "Bypass" mode are NOT counted towards visitation rules but will be logged in the system log.

Security Permissions

NextGen SCP security permissions have been modified to accommodate the Visit Rules feature. Facilities that have multiple administrator groups will not be automatically updated.

System is able to communicate with the video hardware at the time of a scheduled visit so that the visitation session will automatically begin without staff involvement.	**Y**	Please see comments below.
Visitation will begin automatically at the scheduled time without any intervention required from facility staff.		
System allows for visitation recording.	**Y**	Please see comments below.
All non-privileged visits are recorded.		

Live Monitoring and Recording

One of the primary advantages of implementing video visitation is the ability to live monitor and record video visitation sessions. This capability creates new investigative opportunities and also reduces violence within jail walls. In addition, the Securus Video Visitation interface enables jail staff to download visits for later investigative review and lock recordings from being purged after the standard retention window expires

System allows for configurable settings for screen resolution and bandwidth requirements.	**Y**	Please see comments below.

The SVV system automatically accounts for available bandwidth and scales the quality accordingly. It offers high quality video using low bandwidth as well as a wide range of video resolutions and bit rates, including: CIF (352 x 288 pixels), SIF (352 x 240 pixels), QCIF (176 x 144 pixels).

Scheduling of video visitation sessions is performed on the Contractors website.	**Y**	Please see comments below.

Securus Video Visitation (SVV) is a web-based visitation system that allows friends, family members, attorneys, and public officials to schedule and participate in video visitation sessions with an inmate—from anywhere with internet access—using a smartphone, tablet or PC. Remote video visitation provides family and friends limitless opportunities to connect with an inmate by sharing everyday events like birthdays, reviewing homework, watching cartoons with their kids, attending a concert, and opening presents on Christmas. Many studies have shown a link between inmates maintaining relationships with their loved ones reduces recidivism.

The SVV service enables safe, secure visitations with fewer burdens on facility staff. This advanced solution provides multiple benefits, including:

- Enhanced facility security by reducing the possibility of inmate confrontation
- Reduction in inmate and visitor movement through a facility
- Improved inmate communication with legal representation, bail-bondsmen, family, and any other persons authorized by Dallas County administration
- Reduction in contraband infiltration
- Increased security for visitors
- Increased inmate and visitor morale with increased opportunities to visit
- Reduced man-hours needed to escort inmates and visitors to visiting areas
- New revenue stream for the facility through paid visitation sessions

Anywhere Video Visitation

This method allows remote visitors, such as family and friends, bail bondsmen, probation officers, and attorneys secure communication with inmates from outside the facility via a broadband internet connection on any device, including both Android and Apple mobile devices.

Remote visitors access SVV services through the Securus mobile application or the www.videovisitanywhere.net website. Remote users need only a tablet, computer, or mobile phone with a built-in or external webcam and a microphone and speakers, or a headset.

Family and friends can obtain an approved account profile *remotely* by sending their picture and driver's license. *Securus is the only company that offers this feature*.

From the mobile app or website, visitors select the facility and inmate with whom they would like to visit and then can:

- Create, reschedule, and/or cancel a scheduled video visit session
- Pay for the scheduled session with a credit or debit card
- Apply for remote video visitation privileges from the facility
- Join a visitation session with inmates—no officer intervention is required

How It Works: Anywhere Video Visitation

An inmate's family, friends, and others—such as attorneys—can access SVV services 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 visitation session, and view account activity.

When a user logs on to the video visitation website or mobile app, they select the facility and inmate they wish to visit. 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 visits according to the inmate's housing location, available terminals at that location, and available visitation time slots. Remote video visitation sessions are charged on a per-session rate, and friend and family can pay using a debit or credit card.

How It Works: On-Site Video Visitation

Onsite visitation allows visitors to arrive at the facility to video visit at a touch-screen terminal with an inmate. When a visitor arrives at the facility, he/she is directed to the designated terminal area after passing through security. Once at the terminal, visitors enter a PIN unique to that visit as validation of the visitor's appointment with the inmate. The PIN is provided to the visitor after scheduling the onsite visit. Visitors can schedule their onsite visitation in three easy ways:

- Securus mobile app: Visitors can schedule an onsite visit by downloading the Securus mobile app to schedule the next onsite visit
- Onsite terminal: Visitors can schedule using one of the touch-screen terminals configured for scheduling the next onsite visit
- Visiting www.videovisitanywhere.com through a mobile device or computer

The facility's needs dictate the scheduling process. By default, onsite visitation is subject to the same scheduling rules as anywhere/remote video visitation.

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

System provides for commissary ordering via touch screen inputs.	**Y**	Please see comments below.
Commissary ordering can occur with touch screen inputs on both the video visitation kiosk and the SecureView inmate tablets. (Learn more about our tablet program at **EXHIBIT E**.)		
The system provides for sick call reporting via touch screen inputs.	**Y**	Please see comments below.
Sick call reporting can occur with touch screen inputs on both the video visitation kiosk and the SecureView inmate tablets (Learn more about our tablet program at **EXHIBIT E.)**		

System provides for the ability for the electronic mail to be fully automated. NOTE: Staff should be able to review messages and, if approved, allow them to be delivered to the terminal screen.	**Y**	Please see comments below.

Securus eMessaging provides facilities with a secure, fully digital two-way messaging solution to help keep constituents and inmates connected during incarceration. eMessaging is provided at no cost to Dallas County and uses existing inmate terminals and community SecureView tablets.

All eMessages are channeled through the secure facility eMessaging web-based portal for message review, analysis, and processing.

eMessaging

Constituents use Securus' free mobile app or family and friend website to purchase 'stamps' and send eMessages. Photos and eCards can be attached for an additional stamp and the family and friend can purchase a text-based reply for the inmate. A family and friend do not require approval to send an eMessage, although it is Dallas County's discretion to approve and allow the delivery based on Dallas County facility standards and policies.

eMessaging Facility Portal

Leveraging the most widely used messaging platform in the corrections industry, Securus eMessaging provides facilities with an intuitive, easy to use system that provides total control over content assessment. The centralized, proprietary platform is managed wholly within the US. The flexible platform can be configured to match the review approach of each facility. An 'Auto Release' configuration allows messages to be forwarded automatically when certain conditions are met. The 'Manual Release' configuration will enable staff to review each message and manually release to the recipient or reject. If a facility does not use Securus' inmate terminals or SecureView tablets, a Mailroom version can be implemented for staff to print and hand deliver messages. All messages and photos are retained for future review for the life of the contract, even if they are rejected or deleted by recipients.

When a message is opened for review additional activities can take place within the screen, such as view the mail history on either the family and friend sender or inmate. This helpful feature enables staff to see who else the family and friend sender has sent messages to and received messages from in the facility. A convenient translator converts Spanish messages to English for staff review.

Review tools are integrated into the review portal to simplify and decrease staff time reviewing messages.

Security

Facilities have the flexibility to suspend inmates from participating in eMessaging. Once suspended, family and friends will see a notification before composing message that the inmate is not eligible for eMessaging at this time. Family and friends can also be blocked from participating in eMessaging and will receive a pop-up notification. Each suspension and reactivation action is logged with staff name, date and reason for the status change.

A word watch filter can be used to screen messages and separate those that have a word in the word watch list. Facility users can add or change words and eMessages containing that text will be held in a folder for manual review. These messages display the words on the watch list at the top of the message highlighted in red for easy viewing, allowing staff to quickly determine the context of the communication and decide to approve or reject.

The word watch filter is easy to use and flexible to align with trends in coded speech phrases or buzz words to quickly identify communication that might

cause a security threat or provide context to an ongoing investigation for both incoming and outgoing reply eMessages.

A 'watch list' for inmates and family and friends can be populated by staff to flag messages for people added to the watch list, providing an efficient way to monitor communication of parties of concern. Individuals on the list can be activated and deactivated at any time.

eMessages that are 'clean'—without photos or words on the Dallas County word watch list or inmate/sender watch lists—can be set to automatically be approved and flow to the inmate to view on a ConnectUs terminal or SecureView tablet. Each eMessage that is rejected by the facility generates an automatic, free message to the sender advising that their message was not forwarded with a stated reason. Rejection reasons can be modified to suit each unique environment.

eCards are like greeting cards and are selected by family and friends from our online catalog. The eCards are pre-worded and are not editable, so there is no need for staff to review these.

Photos can be quickly reviewed with our Photo Review folder. Multiple photos are presented and can be individually rejected or all approved for faster visual assessment.

All eMessage photos and eCards from the public are retained for analysis, even when rejected due to offensive, dangerous, or out of policy content.

Investigations and Reporting

Facility staff can identify someone from the public who is communicating with multiple inmates easily and take action to suspend the inmate and or sender or further investigate.

Intuitive reporting and views provide a complete message history by inmate, and ability to search messages by inmate, family and friend, date, specific message and word on word filter list.

eMessages, providing valuable investigative opportunities, contain up to 4,000 characters when sent by the public and up to 2,000 characters when an inmate replies. Subject lines can contain up to 40 characters.

eMessaging family and friend portals

For the utmost security, eMessages may only be sent and received by family and friends using the Securus Mobile app for smartphones and mobile devices, as well as the Securus Online family and friend website at www.securustech.net. These convenient user interfaces are also used by the public to deposit money into prepaid calling accounts and to enroll, schedule, and participate in a remote video visit. eMessaging is added to their free Securus Online account; the user can purchase a book of stamps used to pay for eMessages by searching for an inmate by name or inmate ID and selecting the state and facility name. Stamps can be purchased using a Visa or MasterCard credit or debit card and the user can save the card for future stamp purchases.
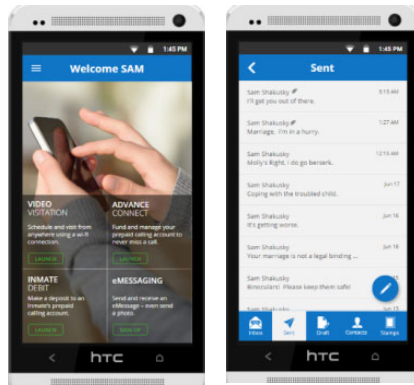
Family and friends can send a text-only message for one stamp and add photos from their photo gallery or take a photo on their mobile device for an additional stamp each. With our Snap n' Send™ service, constituents using the Securus app can snap a photo or select from their gallery and send just the photo for one stamp, helping inmates and the public stay connected through familiar social media capabilities.

Family and friends can also prepay for an inmate text-only reply for an additional stamp. The stamp balance is always shown in the app or website inbox and all stamp purchases clearly state the stamp pricing and any associated fees and taxes. A stamp history can be viewed to show stamp purchase transactions.

If the message is rejected by the facility the sender will receive a free eMessage notification advising that the message was not delivered and the reason. If a reply was prepaid for the inmate and the inmate message is approved, the family and friend will receive the inmate text based reply message in their eMessaging inbox.

eMessaging Inmate portal

The inmate can access the eMessaging module in the ConnectUs inmate terminal or a SecureView tablet after authentication. All eMessages, photos and eCards are displayed on the terminal or tablet in an eMessage inbox with no paper distribution. The inmate will see an indication that they have an eMessage in their inbox and once the eMessage is opened they will clearly see if photos or eCards are attached or if a pre-purchased inmate reply is included. The inmate can reply with a text only eMessage to the sender who issued the prepaid reply stamp.

If the inmate reply message is rejected the inmate and sender of prepaid stamp will receive a free eMessage notification advising that the message was not delivered and a reason.
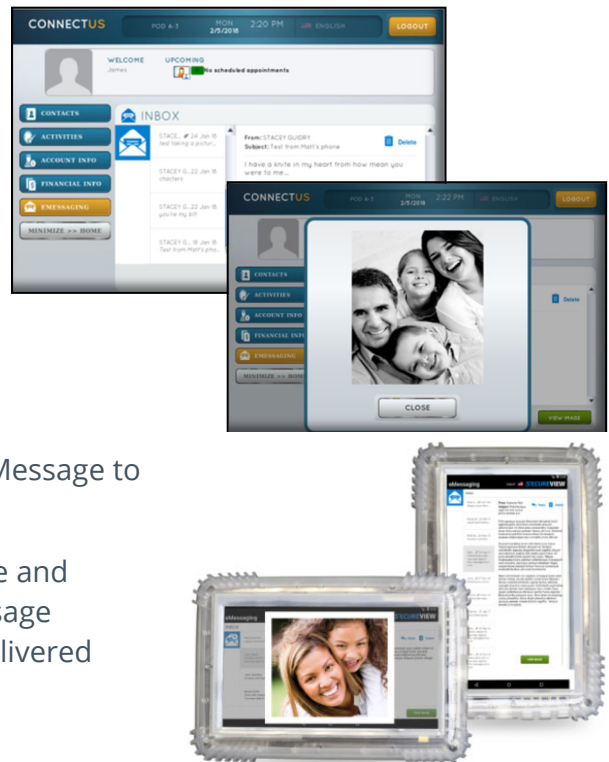
Hosted Video Visitation – Technical Requirements

System is a complete TCP/IP-based system. All video and audio streams between the terminals, visitors, and management equipment (servers) is transmitted over TCP/IP Ethernet.	Y	Please see comments below.
The Securus Video Visitation system is a complete TCP/IP-based system. All video and audio streams between the terminals, visitors, and management equipment (servers) is transmitted over TCP/IP Ethernet		
System consists of inmate terminals connected over a 100 Mbps dedicated Ethernet network so that any terminal can be connected to any other terminal.	Y	Please see comments below.
The Securus Video Visitation system consists of inmate terminals connected over a 100 Mbps dedicated Ethernet network so that any terminal can be connected to any other terminal.		
Terminals are able to access the video visitation solution via local area network (LAN) or via a broadband internet connection (DSL, cable, etc.) using a computer, laptop or tablet that is web camera and headset enabled.	Y	Please see comments below.

Securus Video Visitation terminals are able to access the video visitation solution via local area network (LAN) or via a broadband internet connection (DSL, cable, etc.) using a computer, laptop or tablet that is web camera and headset enabled

System utilizes: **i. High quality video using low bandwidth.** **ii. Recorded visits are searchable and viewable and can be downloaded to external media.** **iii. Video Transmission Speeds: 64 Kbps – 2 Mbps** **iv. Wide range of video resolutions and bit rates: CIF (352 x 288 pixels), SIF (352 x 240 pixels), QCIF (176 x 144 pixels)**	**Y**	Please see comments below.

The Video Visitation system utilizes:

i. High quality video using low bandwidth.

ii. Recorded visits are searchable and viewable and can be downloaded to external media.

iii. Video Transmission Speeds: 64 Kbps – 2 Mbps

iv. Wide range of video resolutions and bit rates: CIF (352 x 288 pixels), SIF (352 x 240 pixels), QCIF (176 x 144 pixels)

System is designed for: **i. Up to 30 frames per second of high quality video at 384+ Kbps** **ii. Up to 15 frames per second of high quality video at 64 – 320 Kbps** **iii. Constant or variable bit rate and frame rate** **iv. System provides encryption for all visits**	**Y**	Please see comments below.

The Video Visitation system is designed for:

i. Up to 30 frames per second of high quality video at 384+ Kbps

ii. Up to 15 frames per second of high quality video at 64 – 320 Kbps

iii. Constant or variable bit rate and frame rate

iv. System provides encryption for all visits

Hosted Video Visitation – Service, Support, Installation, Testing and Training Requirements.		
A. Contractor will work with Dallas County to determine the exact times when Hosted Video Visitation equipment can be replaced to reduce "down time". Video Service, Support, Installation, and Training.	**Y**	Please see comments below.
Securus shall work with Dallas County to determine the exact times when Hosted Video Visitation equipment can be replaced to reduce "down time". Video Service, Support, Installation, and Training.		
Contractor provides support for video visitation system that includes a 24/7/365 US based call center fully owned and operated by the proposer.	**Y**	Please see comments below.
Securus provides support for video visitation system that includes a 24/7/365 US-based call center fully owned and operated by Securus.		
B. Bidder will provide system testing which simulates normal operating conditions of the installed Hosted Video Visitation Solution to ensure proper performance after hardware and software configuration is complete. This simulation must include full traffic load representing high traffic situations for visitation traffic.	**Y**	Please see comments below.
Securus will provide system testing which simulates normal operating conditions of the installed Hosted Video Visitation Solution to ensure proper performance after hardware and software configuration is complete. This simulation will include full traffic load representing high traffic situations for visitation traffic.		
C. Bidder agrees to Dallas County's right to require the replacement of any network service or system component whose failure to meet required performance levels during testing has risen to a chronic problem level.	**Y**	Please see comments below.
Securus agrees to Dallas County's right to require the replacement of any network service or system component whose failure to meet required performance levels during testing has risen to a chronic problem level.		
Contractor provides all end-user training to Dallas County at no cost.	**Y**	Please see comments below.
Securus provides all end user training to Dallas County at no cost.		
Contractor provides all end-user training on site at the various Dallas County facilities.	**Y**	Please see comments below.
Securus shall provide all end-user training on site at the various Dallas County facilities.		

Contractor provides full training for all system users including full-time system administrators, part-time system administrators, special investigators, and data entry specialists, etc.	**Y**	Please see comments below.
Securus shall provide full training for all system users including full-time system administrators, part-time system administrators, special investigators, and data entry specialists, etc.		
Contractor provides ongoing system training for existing Dallas County personnel when required by Dallas County at no cost.	**Y**	Please see comments below.
Securus will provides ongoing system training for existing Dallas County personnel when required by Dallas County at no cost.		
Contractor provides additional training for new Dallas County personnel when required by the Dallas County at no cost.	**Y**	Please see comments below.
Securus shall provide additional training for new Dallas County personnel when required by the Dallas County at no cost. Securus headquarters is located only miles away and available to provide onsite products and services training for new personnel, new products and refresher trainings		
System includes an integrated help function for system operation, administration, reporting and management functions.	**Y**	Please see comments below.
NextGen SCP has an integrated help function for system operation, administration, reporting and management.		
Contractor will provide a "live" Help Desk support function to Dallas County at no cost to the Dallas County during the term of this contract. This Help Desk function will be capable of providing support via telephone to the Dallas County Hosted Video Visitation Solution personnel for the functions of the Hosted Video Visitation Solution and is available 24 hours a day, 7 days a week, 365 days per year.	**Y**	Please see comments below.
Securus shall provide a "live" Help Desk support function to Dallas County at no cost to the Dallas County during the term of this contract. This Help Desk function will be capable of providing support via telephone to the Dallas County Hosted Video Visitation Solution personnel for the functions of the Hosted Video Visitation Solution and is available 24 hours a day, 7 days a week, 365 days per year.		
The "live" Help Desk support function provided by the Contractor is located within the continental United States.	**Y**	Please see comments below.
Securus maintains a live Help Desk in Carrollton, Texas.		

Contractor warrants that the system installed for Dallas County facilities shall be free of defects, irregularities, unprofessional installation, code violations and shall operate as designed and proposed. Should the system not operate as designed and proposed or violate any local, state or federal code, the Bidder will immediately correct the defect or irregularity or bring the system within code and performance specifications at no cost to Dallas County.	Y	Please see comments below.

Securus warrants that the system installed for Dallas County facilities shall be free of defects, irregularities, unprofessional installation, code violations and shall operate as designed and proposed. Should the system not operate as designed and proposed or violate any local, state or federal code, the Bidder will immediately correct the defect or irregularity or bring the system within code and performance specifications at no cost to Dallas County.

Contractor will provide all post installation system programming and maintenance services at no cost to the Dallas County.	Y	Please see comments below.

Securus shall provide all post installation system programming and maintenance services at no cost to the Dallas County.

D. Maintenance service is available on its Hosted Video Visitation Solution seven days per week, twenty-four (24) hours a day, 365 days per year.	Y	Please see comments below.

Maintenance service is available on its Hosted Video Visitation Solution seven days per week, twenty-four (24) hours a day, 365 days per year.

System provides remote diagnostics and maintenance capabilities.	Y	Please see comments below.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services 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 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.

E. Contractor will replace the system in its entirety or its individual components regardless of cause including, but not limited to, normal wear/use, inmate abuse, natural disaster, or inmate unrest. This system or component replacement will be performed at no cost to Dallas County and will occur immediately upon notification to the Bidder of the system problem by the Dallas County facility.	**Y**	Please see comments below.

Securus shall replace the system in its entirety or its individual components regardless of cause including, but not limited to, normal wear/use, inmate abuse, natural disaster, or inmate unrest. This system or component replacement will be performed at no cost to Dallas County and will occur immediately upon notification to Securus of the system problem by the Dallas County facility. As we have shown over the last 5 years, we have added multiple mobile kiosks, law library kiosks, phone handsets, additional phones and kiosks as needed at no cost.

All maintenance calls from the Dallas County will be answered by a "live" operator/service representative located within the United States at all times. Preferably a dedicated "live" operator/service representative	**Y**	Please see comments below.

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 system allows for integration with or data retrieval from Dallas County Jail/Offender/Inmate Management System and uses the same inmate identification number as created by the Jail Management System to identify the inmate on the video visitation system.	Y	Please see comments below.

Securus has proven experience with Integration. Securus currently integrates with more than 110 different vendors, including your current JMS provider, AIS.

Securus has a dedicated integration department that integrates various systems and products in the corrections environment. This dedicated integration department allows Securus to deliver fast and flexible solutions for our customers. The Securus technology has the flexibility to work with facility-owned systems, jail management system (JMS), commissary, banking, and kiosk vendors. Securus will fully cooperate with your facility and your vendors to automate systems.

Securus can modify your data format for migration into our platform, without costly code modifications. Securus integration engineers consult with facilities' IT departments or system providers to determine the best integration strategy for each specific application.

Securus Integration Process

Securus' dedicated integration team designs, develops, tests, and implements all custom integrations with corrections industry vendors and banking systems to deliver fast and flexible solutions for our customers. This process is part of the overall project plan for the installation of the NextGen Secure Communications Platform™ (NextGen SCP™). Major milestones include:

- Collect preliminary needs/requirements
- Contract signed
- Finalized requirements document
- Approved scope statement
- Finalize design document
- Schedule customer implementation
- Develop custom integration solution
- Test custom integration solution
- Implement custom integration solution
- Customer approval and sign-off

PIN Generation

The Securus NextGen SCP enables a facility to set up personal identification numbers (PINs) for each inmate. The system can be configured to require inmates to enter their PIN before making a phone call or joining a video visitation session.

PIN generation can be uploaded from a JMS or commissary provider using the Securus E-Imports application, Web Services, or a custom integration. PINs can also be entered through the NextGen SCP user interface.

PINs can be linked an inmate's custody account for all inmate information, including allowed calling schedule, call durations, visitations, and more. The number can be configured as a number from 4 to 16 digits in length. Each inmate can be issued a unique PIN. A common practice for PINs is using a combination of fields, such as the last four digits of the jacket ID and the birth month and day of the inmate.

Also, some JMS platforms can generate a random 4- to 16-digit PIN and send it to NextGen SCP via an integration. This option is beneficial because it enables the booking officer to give an inmate their PIN, so they can begin using the calling and video services immediately.

PIN Operations

PIN operations through NextGen SCP are highly flexible. Facilities can enable or disable PIN operations at the facility, inmate 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. NextGen SCP has no limit on the number of PIN or non-PIN inmate telephones or kiosks operating at the facility.

For phones and kiosks programmed for PIN operations, each inmate must enter their PIN before making a telephone call or joining a visitation session. By using their PIN, they create an audit trail that that identifies the inmate who placed the call or joined a visitation session, the date and time of the call/visitation, and the number that called or the visitor in the visitation session. PINs also enable facility staff to authorize or restrict specific inmates from calling specific numbers or participating in video visitations.

PIN Restrictions

PINs can be used to restrict inmate calls at the facility, phone/kiosk, or inmate account level. For example, facilities can identify and lock PINs to a phone/kiosk or group of phones/kiosks within a facility. Site administrators also have the ability to transfer PINS, or a single PIN, when inmates change housing units. Transferring PINs can also be automated through the Securus E-Imports application, Web Services, or a custom integration.

JMS Integration

The Securus NextGen SCP can be integrated with a facility's JMS or commissary system so that the inmate PINs are automatically transferred, activated, and deactivated based on the inmate's status. If an inmate is released, the inmate's PIN is stored and can be reactivated along with call detail or visitation records and inmate call or visitation recordings if the inmate returns to the facility.

The following list identifies fields that can be automatically populated in NextGen SCP from a JMS or commissary integration:

- **First Name** – Inmate's first name
- **Middle Name** – Inmate's middle name
- **Last Name** – Inmate's last name
- **Birth Date** – Inmate's date of birth
- **Social Security Number (SSN)** – Inmate social security number
- **Account Number** – Inmate's jail ID, jacket ID, or docket number, to be used as the NextGen SCP inmate custody account number. Any number permanently assigned to an inmate that does not change if they are released and booked back into the facility.
- **PIN** – 4- to16-digit code used by the inmate to place phone calls.
- **Activate Date** – Date in which the inmate account became active in the system
- **Book Date** – Date that the inmate entered the facility
- **Gender** – Inmate's gender
- **Housing** – Location of the inmate
- **Race** – Inmate's 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 inmate
- **Three-Way Detection** – Setting to enable or disable three-way call detection for this inmate
- **Language Preference** – Language in which the inmate speaks for reporting purposes (does not dictate the language of phone prompts)
- **Suspended** – Allows or prevents the inmate from placing calls
- **Suspend Start Date** – Start date of calling privileges suspension
- **Suspend End Date** – End date of calling privileges suspension

Investigative Software		
The system offers investigative software for law enforcement.	**Y**	Please see comments below.
Securus is pleased to offer Dallas County our ICER, IPro and Threads investigative software programs.		
Investigation software is wholly owned by the proposer and does not use another contractor or vendor.	**Y**	Please see comments below.
Securus wholly owns the THREADS investigative tools described herein, including ICER and IPro.		
Investigation software is completely integrated with the calling platform and does not require the export and import of inmate call records, inmate account information, or called party billing name and address information related with Dallas County. Please describe your solution and related features.	**Y**	Please see comments below.
All of our proposed investigative tools are fully owned by Securus and fully integrated into NextGen SCP.		

ICER™—Uncovering Intra-and Inter-Facility Inmate-to-Inmate Telephone Communications

Inmate-to-inmate communication (ITIC) 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: **inmate-to-inmate 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 inmate phone calls, we offer cutting-edge technology based on state-of-the-art, patent-pending, call-matching technology that identifies ITIC even when it's between two different correctional facilities across the country.

Although illegal ITIC 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.

Inmates are continually finding creative ways to speak to each other using the inmate phone system, and ICER listens to and identifies all of these illegal communication events. Whether

two inmates 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—SCP. Please refer to **Exhibit F** for more details.

THREADS

Securus understands that during an investigation, the law enforcement community is inundated with tasks and gathering intelligence. Identifying relevant data can be a challenge at times when new data are identified. This results from numerous different sources, formats, and potential leads that require identification. 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 can be managed remotely at any time through an assigned web-based portal. This means that Dallas County can access data remotely from any location that provides internet access. Please refer to **Exhibit C** for detailed information information on Threads.

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 was initially developed by JLG Technologies, which Securus acquired in 2014.

IPRO includes a wide range of tools that identify voices by name, deter inmate PIN abuse, and provide leads for investigators pursuing illicit activity carried out over the inmate telephone system.

Investigator Pro is a Securus solution and Securus manages the solution roadmap. It is fully integrated with the Securus call platform and is hosted in Securus' data centers. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.

Please refer to **Exhibit G** for more information.

The investigation software provides a way to import data from public phone records and cell phones, including contacts, emails, text messages, call records, and pictures. Please describe your solution and related features.	**Y**	Please see comments below.

The Securus THREADS investigation application accepts imported public phone records.

THREADS was designed to help investigators quickly retrieve, manage, and analyze large volumes of data to discover connections and patterns. Investigators can use data automatically imported from the NextGen Secure Communications Platform™ (NextGen SCP™) system and/or any other set of records imported for a specified target.

Sources of Information

Corrections Data	External Data
• Inmate call records • Inmate personal information (such as name, account number, PIN, DOB, and SSN) • Individuals the inmate is allowed to call versus who they actually called • Called party BNA information • Corrections facility information in proximity to calling behaviors	• Confiscated cell phones (such as calls, text messages, emails, videos, and contacts) • Public phone records • Events and places of interest • Mail • LexisNexis • SS7 information

THREADS integrates all corrections data—such as call records, phone numbers, and billing number address—the moment it is enabled. THREADS analyses external, imported data together with corrections data to aid an investigation.

In addition, THREADS can import data from cell phones, including contacts, emails, text messages, call records, and pictures. A Cellebrite UFED device or similar technology retrieves data from cell phones and this data can then be uploaded to the THREADS application for further analysis. THREADS combines this imported data with the facility's communication records and all other available data to identify and analyze connections and patterns.

Investigation software analyzes data between multiple correctional facilities, so as not to limit the investigation to only Dallas County. Please describe your solution and related features.	**Y**	Please see comments below.

Securus' THREADS investigative software is designed to allow investigators with appropriate permissions to analyze data across multiple customers and correctional facilities, and to share reports and analyses between investigators--including relevant information imported into the system.

THREADS provides a community model allowing investigators and correctional facilities to subscribe to the national THREADS investigative community while still providing security for

the information they import. The community model is facilitated through the Securus centralized database which stores all customer data. Users can choose either to share imported data with the community or to keep data private to themselves or other specified users.

In a community where investigative data is shared, the investigator can use THREADS to uncover correlating intelligence across othersites/faciltiies from the extensive national community data set including, but not limited to:

- More than 79 million communication records
- More than 530,000 current and former inmates
- More than 430,000 contacts (non-inmates)

Investigative Data Community Sites
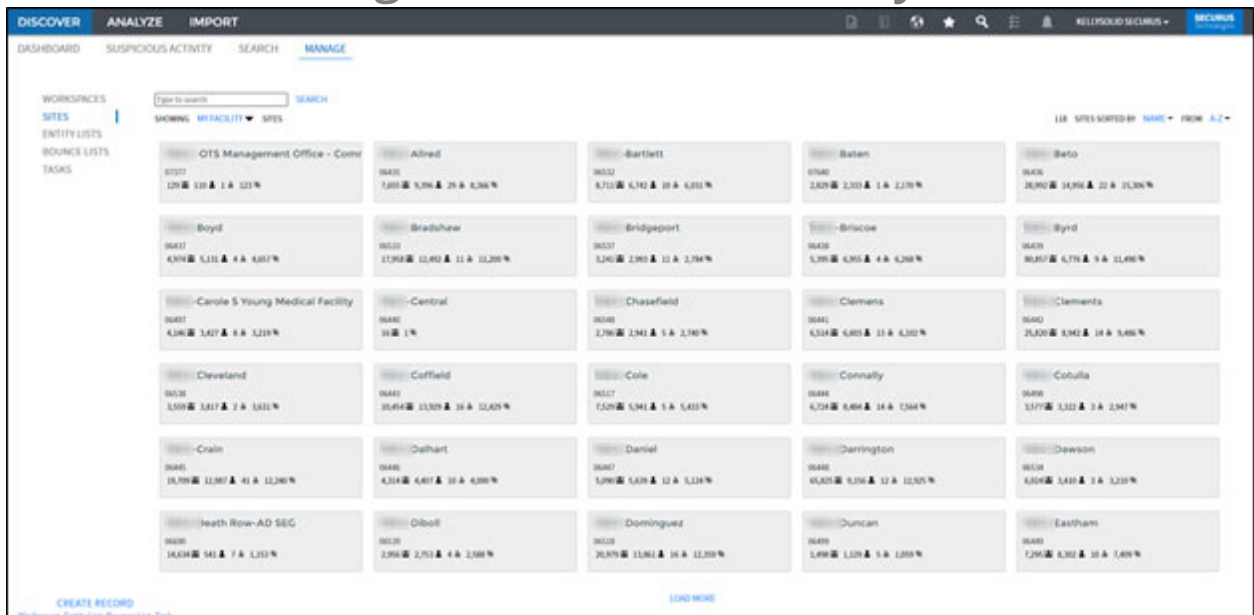
Investigation software is able to notify investigators when information is found related to any report or analysis previously configured. Please describe your solution and related features.	Y	Please see comments below.

The THREADS application supports monitoring and notification of data changes (Alerts).

THREADS notifies users when an analysis is complete or when the analysis identifies specified information.

THREADS users can set up several reports simultaneously, taking full advantage of the application's ability to conduct background analysis. Once complete, the system provides an on-screen alert and a quick-access link to the report.

Investigation software provides investigators with the ability to share information with other investigators. Please describe your solution and related features.	Y	Please see comments below.

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 read-only reports.

THREADS Shared Reports Screen

In addition to specifying report-sharing parameters while setting up the report, THREADS also allows users to share any report after it has been completed.

Investigation software allows investigators to schedule reports and analysis. Please describe your solution and related features.	Y	Please see comments below.

THREADS provides the most flexible scheduling tool in the industry, increasing investigators' efficiency. Each THREADS analysis includes a scheduling agent that allows users to specify data to analyze, report frequency, and more.

Users can elect to run or schedule a specific report within each analysis/report option.

THREADS Report Scheduling Screens

Investigation software must be able to identify an inmate's closest associates (Inner Circle) and show changes that may occur.	Y	Please see comments below.

The THREADS application is a powerful, accurate, and intuitive investigative tool that automatically analyzes data such as inmate communication records, public phone records, data from confiscated cell phones, and more. Investigators can use this data to identify suspicious calling patterns, inner circles, associations between multiple inmates, and correlations to called external parties and more. THREADS' easy-to-use interface provides investigators interactive visualization tools, analytical reports, charts, graphs, and maps. THREADS will also build a case and provide a presentation view to use as evidence in a criminal trial.

THREADS offers investigative benefits, such as:

- Cell phone forensics analysis
- Accomplice identification
- Indirect contact identification (see who is really contacted)
- Linkage identification
- Inner circle identification
- Associated gang member identification
- Internal communication identification within jail walls
- Unique patterns identification
- Single system analysis of all combined data
- Enhanced reporting tools to harvest all of this information

System identifies called party billing name and address and includes these called parties as entities in the investigation software. Please describe your solution, related features, and how many billing name and addresses are in your system today.	Y	Please see comments below.

THREADS identifies billing name and addresses (BNA) for contacts outside of the correctional facility. At present, THREADS includes billing names and addresses for more than 1 million contacts and more than 170 million communication records related to more than 1.4 million inmates.

THREADS uses contacts' billing name and address and also provides full, interactive mapping capabilities to easily identify:

- Called party name and address
- Phonebook contacts
- Geo coordinates obtained on calls from inmates to cell phones
- Correctional site/facilities

Inmate's BNA and Site Location
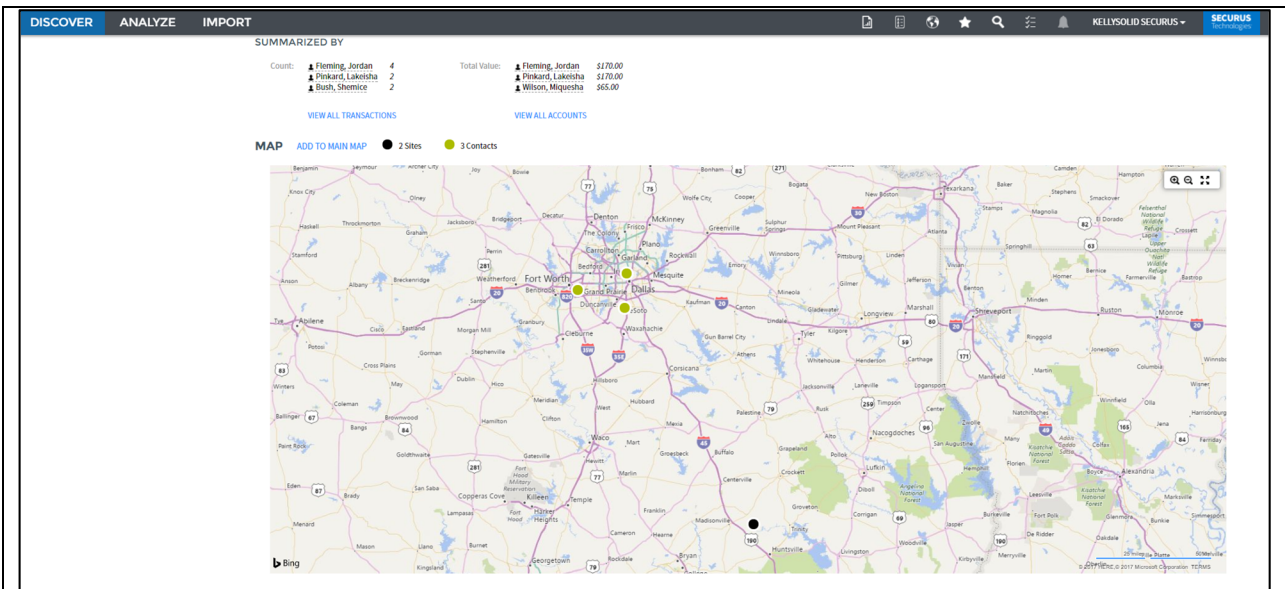
Investigation software provides calling frequency and statistics.	**Y**	Please see comments below.

THREADS provides several ways to analyze information, including communication activity reporting, calling frequency and statistics, and contact listings. THREADS groups common reporting and analysis into categories for ease of use. The various reports include linkage charts, scatter diagrams, star charts, text outputs, conspiracy indexes, timelines, PDF exports, and much more.

Investigation software provides a contact listing for called party information.	**Y**	Please see comments below.

THREADS provides several ways to analyze information, including communication activity reporting, calling frequency and statistics, and contact listings. THREADS groups common reporting and analysis into categories for ease of use. The various reports include linkage charts, scatter diagrams, star charts, text outputs, conspiracy indexes, timelines, PDF exports, and much more.

The THREADS application provides several categories for analyzing communication activity:

- Communication Statistics
  - Communication activity

- o Frequency and statistics
- o Contact listing
- o Communication listing
- Communication Behavior
  - o Sequence analysis
  - o Pattern analysis
  - o Chain analysis
- Common Communication
  - o Common contact
  - o Concurrent common contact

Other available categories include:

- Organization Analysis
  - o Inner circle identification
  - o Inner circle delta
  - o Who's the boss (most likely leader of criminal ring)
- Subscription Usage Analysis
  - o Hole detection (identifies holes in communications)
  - o Concurrent phone usage
  - o Contact swap (Identify PIN theft/PIN sharing and contacts on the outside switching phone numbers)
- Linkages
  - o Entity linkages
  - o Interconnected linkages
  - o Intercommunications
- Timelines
  - o Graphical timelines
  - o Trends
  - o Interactive
  - o Includes communications and events
- Correlations
  - o Cross-site analysis
  - o Cross-case analysis

Investigation software provides capability to import cell tower information obtained from public phone companies such as AT&T and Verizon.	**Y**	Please see comments below.

While our system is developed with these capabilities, we are not currently offering the products dependent upon location-based data from cellular providers. All of the major cellular carriers have publicly announced that due to consumer privacy discussions with Congress and the FCC they are not making such data available. This applies to all corporations and no one in the industry should be able to provide this service until such time as Congress and the carriers finalize discussions to maintain consumer privacy.

Investigation software provides analysis based on pattern dialing.	**Y**	Please see comments below.

The Securus THREADS application allows investigators to identify communication sequences that occur multiple times for a selected target and to generate a timeline of the sequences and conspiracy analysis. Investigators can identify contacts who may be related using data automatically imported from NextGen Secure Communications Platform™ data and/or any other set of records imported for a specified target.

Investigation software identifies gaps in inmate calling behaviors.	**Y**	Please see comments below.

The Securus THREADS platform allows investigators to identify gaps in communication activity that are greater than a specified minimum time for a selected target. This can be shown through a Hole Detection analysis. This report output is a timeline that shows high/low calling activity as well as "holes" or gaps where the inmate is not using the calling service (Holes are designated with a black color).

Hole Detection Analysis Report
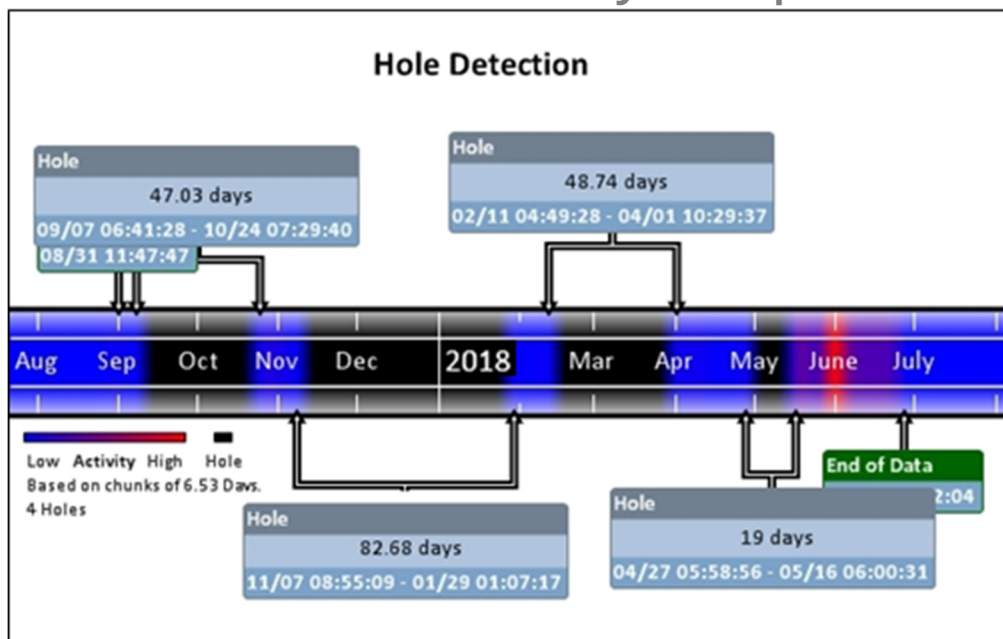
Investigators can use data, such as inmate phone calls, automatically imported from the NextGen Secure Communication Platform™ (NextGen SCP™) and/or any other set of communication records imported for a specified target. Gaps in communication could indicate, but is not limited to, PIN sharing, use of a contraband cell phone, lack of funds to make calls or incidents that cause an inmate stop using the NextGen SCP calling service.

Investigation software identifies linkages between multiple parties, whether those parties are inmates or constituents to include two entity linkage analyses.	Y	Please see comments below.

The Securus THREADS application provides linkage reports that identify all known connections between any target, whether an inmate or not. The system generates a graphical linkage chart that shows the known connections to a selected set of targets. Connection types are configurable and can consist of communications, mail covers, associations, events, phone book records, and more.

THREADS also produces supporting details related to the linkage chart, such as:

- A list of all entities included in the chart

- Linkage paths (showing the shortest path between each entity)

- Connection reasons (showing why there is a connection)

THREADS Entity Linkage Reporting
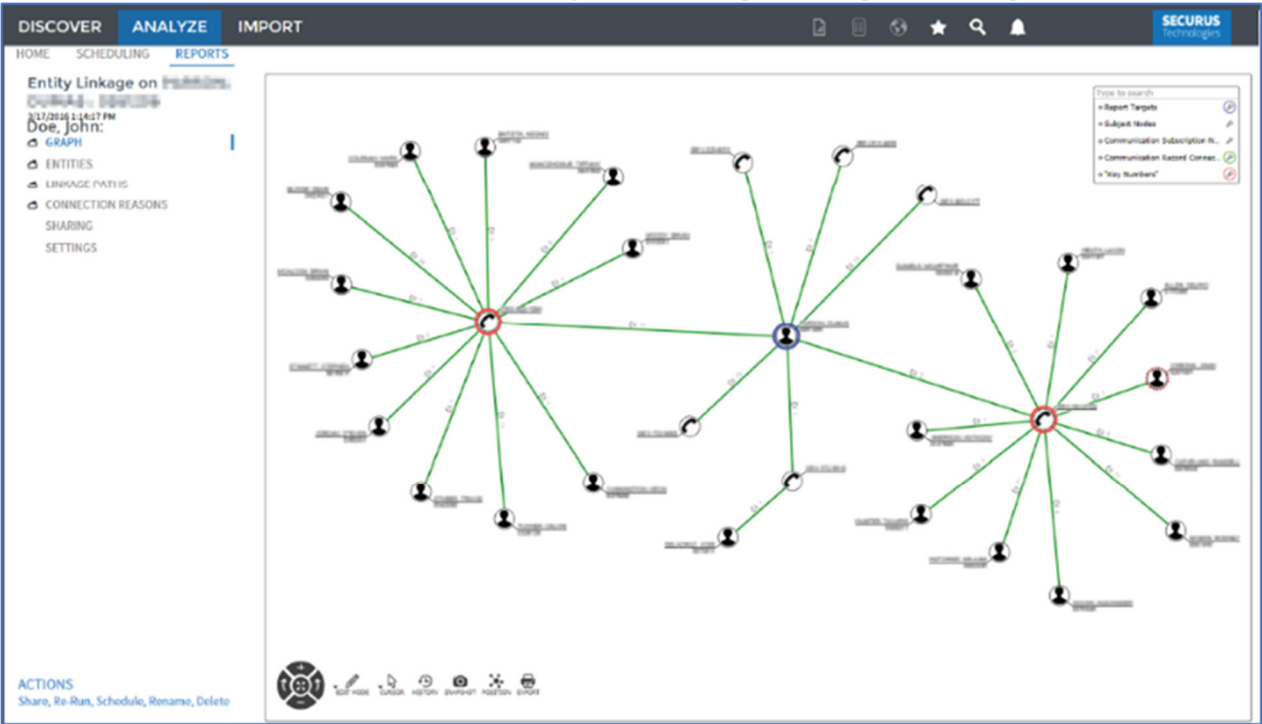
The investigation software shows information on a map that allows investigators to add or remove information from the map as it may suit their investigation. Please describe your solution and related features.	Y	Please see comments below.

THREADS uses the Microsoft Bing map utilities for standard and advanced mapping functions like no other investigative software tool. THREADS also has advanced customization mapping tools built around Bing. These tools allow investigators to interact with the map, add new locations to the map, add more information to the existing locations, drop pins, and draw circles, polygons, and trajectories on the map. THREADS allows the customization of the colors, descriptions, and comments shown.

Communication events from a facility and terminated at a specified billed number address or geographic location are automatically displayed on the map. THREADS generates maps from NextGen Secure Communications Platform™ data, as well as imported and/or manually added data; investigators can add and remove information from the map in real time. THREADS will also export map images for external use.

Investigation software identifies changes in inmate contact phone numbers (contact swap).	**Y**	Please see comments below.

The Securus THREADS application allows investigators to identify subscriptions that may be changing hands between multiple inmates or people outside of the facility. THREADS can identify PIN stealing, PIN sharing, and even phone swapping (people using different phones/phone numbers). Investigators can use data automatically imported from the NextGen Secure Communications Platform™ or any other set of records imported for a specified target.

Investigation software with link analyst capability (phone and video visitation.	**Y**	Please see comments below.

The THREADS application does not limit the number of data sources or types that may be incorporated; THREADS supports the import and link analysis of call detail records, offender demographic data, visitation data, offender banking data, and security threat group information. THREADS provides easy-to-use importers that allow the user to set up templates to import similarly formatted files quickly.

Call Monitoring & Recording

The system maintains all call recordings centrally on SAN storage technology and does not use tape drives for primary storage of call recordings.	**Y**	Please see comments below.

The integrated calling services recording application works independently, so there is never a need for integration of a third-party manufacturer's product. This allows the facility to deal with a single vendor if any issues arise.

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.

The stored call recordings are maintained at the vendor's central depository and remain for a period of time as requested by Dallas County.	**Y**	Please see comments below.
All recordings created on the platform reside in at least two of our Data Centers. Recordings are stored online for immediate access for at least six months. NextGen SCP can also be used to burn the information to a digital file that can be transferred to CD or DVD for additional back up, if necessary.		

	All call recordings are stored online and available through the online user interface for a minimum period of six months.	**Y**	Please see comments below.

All call recordings shall be stored online and available through the online user interface for a minimum period of six months.

	Facility personnel are able to search call recordings by dialed number, date, time, inmate account, or site name.	**Y**	Please see comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) provides authorized personnel and investigators single-point access to research Dallas County communication records and recordings.

Users can specify search criteria, such as called party, calling telephone, date, time, PIN, custody account number, duration, and location, and search across a site or group of sites based on their security authorization. NextGen SCP searches communication 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 communication 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 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.

	Facility personnel are able to simultaneously live monitor conversations while the system is recording the conversations.	**Y**	Please see comments below.

The NextGen Secure Communications Platform™ (NextGen SCP™) allows authorized users to live monitor calls in progress via a browser on an internet-connected device. The feature provides users selectable scanning of all live calls in progress in specific locations, so the user does not have to scan all phones in use.

The feature's integrated media player has a time-shifting capability allowing the investigator to pause, rewind, and replay even as 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 to the dialed number or phone in use.

Facility personnel can monitor, disconnect, and / or barge into a live call.	**Y**	Please see comments below.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) has an integrated recording and monitoring system. The automated system is designed to be a cost-effective solution for all correctional facilities of any size. Multiple levels of security provide that only authorized personnel can access and monitor the inmate 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. Facility personnel (with appropriate privileges) can monitor live calls by highlighting the call in progress and clicking on the handset icon (). This process is undetectable by the inmate or the called party and does not disrupt the recording process.

Authorized personnel can monitor, disconnect and barge into live calls.

Concise descriptions of activity appear for each phone in use. For example, the system shows the inmate name and ID, dialed number, start date/time, and duration. NextGen SCP also shows whether the call was accessed, call notes that may be available, or whether the call is flagged. Clicking on a call opens a side-bar with additional details of 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 language of the call prompts. This side-bar also provides an easy method to download the call recording, extend the expiration date of the call recording retention period, add a note to the CDR, or view the recording access history—all with a single mouse click.

NextGen SCP does not record visits with entities the facility has designated as private, such as visits with legal counsel or clergy. NextGen SCP prevents all unauthorized attempts to listen to private calls—Additionally, the system does not provide a way to monitor these private calls. The communication record will clearly indicate the visit as "private" in the user interface and will contain no recording.

The system has the ability to have a selectable scan of all live calls in progress	**Y**	Please see comments below.

While on the NextGen Secure Communications Platform™ (NextGen SCP™) calling services' Monitor Calls page, Dallas County personnel can use the Scan Patrol feature to automatically cycle through live calls at a brief interval, allowing the user to listen to brief portions of each call to determine whether it's a call that they might be interested in for a more detailed analysis.

Users can enter a specific amount of time the system will play each call before moving to the next active call, similar to the scan function on an automobile radio. The scanning begins on the first active call on the first active post and continues to the next active call, looping back to the first active call when reaching the end.

The following figure presents an example the calling services Scan Patrol page.

Scanning Live Calls
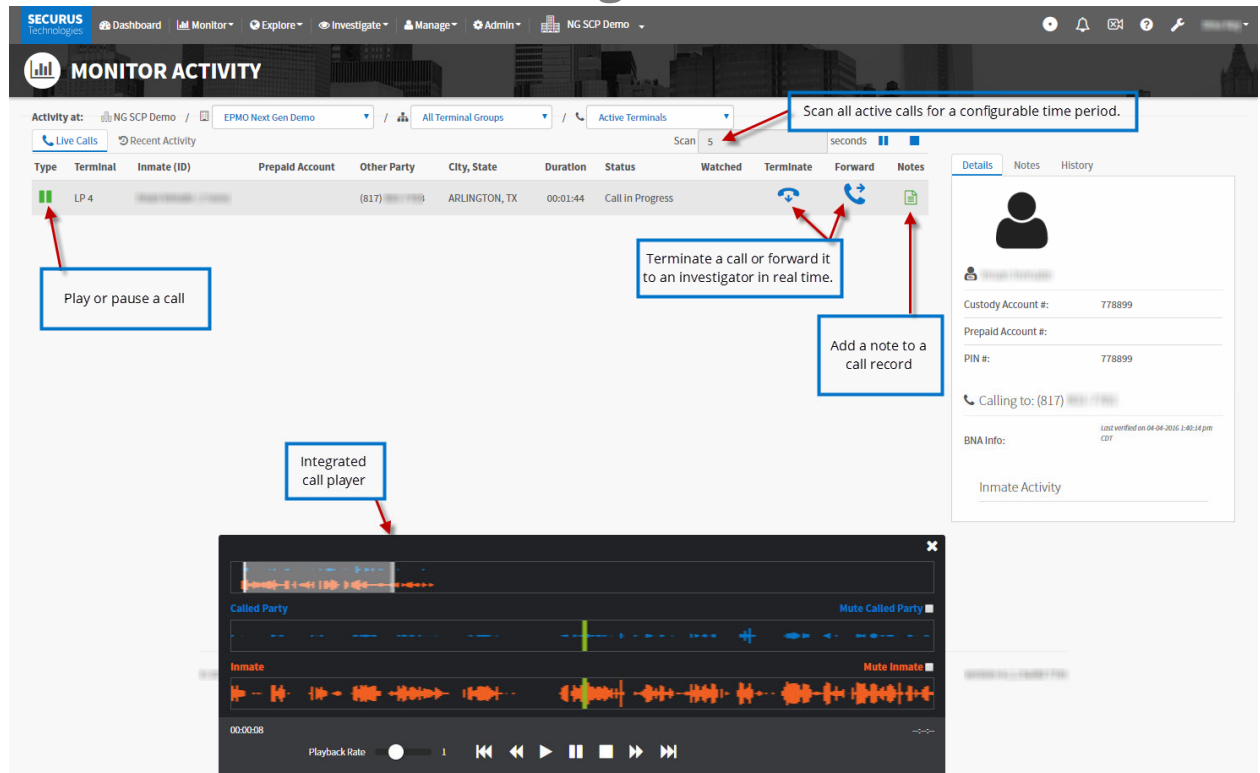
The system provides a call history through live monitoring to allow personnel to see recent activity for phone numbers and phones without navigating away from live monitoring.	Y	Please see comments below.

The NextGen SCP Monitor Activity function allows for real-time monitoring of calls in progress via a multi-media PC workstation. Facility personnel (with appropriate privileges) can monitor live calls by highlighting the call in progress and clicking on the

handset icon ( ). This process is undetectable by the inmate or the called party and does not disrupt the recording process. Concise descriptions of activity appear for each phone in use. For example, the system shows the inmate name and ID, dialed number, start date/time, and duration. NextGen SCP also shows whether the call was accessed, call notes that may be available, or whether the call is flagged. Clicking on a call opens a side-bar with additional details of 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 language of the call prompts. This side-bar also provides an easy method to download the call recording, extend the expiration date of the call recording retention period, add a note to the CDR, or view the recording access history—all with a single mouse click.

Inmate Multi-Function Kiosk Software and Applications

Automated Information System. The ability for an inmate to look up court dates, sentences, attorneys and any related court information	**Y**	Please see comments below.

Automated Information Services (AIS) is the industry's first and only hosted, interactive voice response (IVR) system that provides general facility and inmate-specific information to detainees and outside callers over the phone. AIS also can be configured to enable inmate family members and friends to open or fund a prepaid calling account or an inmate's trust using their phone. These additional funding options make it easier for family members and friends to contribute funds, increasing a facility's potential commissionable revenue.

All functionality is available around the clock, allowing constituents to access the system whenever they need it. AIS can be configured to provide callers with the following information:

- Criminal charges
- Bond amounts and types
- Court dates, times, and locations
- Projected release date
- Commissary balance
- Visitation eligibility
- General facility information
    - Facility location
    - Directions
    - Hours
    - Mailing policies
    - Visitation policies
    - Money deposit policies

AIS retrieves information from a facility's various management information systems, including jail management and court systems, every 15 minutes. The service offers an English and Spanish interface, text-to-speech playback of inmate names, and a touchtone and speech recognition

AIS Facts
For the year-ending 2018:

- AIS is installed at 220+ facilities
- 180,000+ funding transactions were processed
- Nearly 10 million calls were accepted by AIS
- Average call duration with AIS shortens call times by almost 70%

interface. Family members and friends access AIS by calling the facility's normal telephone number. Inmates access their information by dialing a speed-dial code from any inmate telephone.

Additional AIS benefits include:

- Improved efficiency – quickly answering inmates, family members, and friends while freeing staff to focus on other responsibilities
- Use of phone system already installed – no need for additional hardware or wiring
- Answer 90 percent of inmate questions currently answered by corrections officers
- Reduce calls answered by staff by 80 to 90 percent – AIS provides 24-hour access and eliminates most common calls
- Realize a 200 percent increase in answered calls – able to assist callers who might otherwise hang up
- because of extended wait times
- Reliable system – 99.9 percent uptime service level agreement
- Usage summary emailed to the facility every month
- Increase commissionable revenue by allowing another funding method

AIS Return on Investment

Most facilities find incoming phone calls to be an administrative burden. Securus estimates that an average facility receives one half telephone call per day, per inmate, with each call averaging four minutes. Inmates ask facility personnel an additional one half question per day. These activities consume administrative resources and take personnel away from their primary responsibilities.

Monthly Time Consumption per Inmate

1 inmate X ½ call X 4 min X 30 days = 60 minutes

<div style="background-color:#1f6fc0; color:white;">

AIS Value Automation

Incoming Requests:	AIS automates 80 percent of administration requests, which results in a savings of 48 minutes per ADP per month
Inmate Requests:	AIS automates 90 percent of inmate requests, which results in a savings of 54 minutes per month per ADP

</div>

Automated Information System. The ability for outside party (inmate representative/family) to look up court dates, sentences, attorneys and any related court information	**Y**	Please see comments below.

Securus AIS shall provide the ability for an outside party (inmate representative/family) to look up court dates, sentences, attorneys and any related court information.

Kiosk applications shall include time stamping for tracking inmate grievances/kites/other applications. (grievance aging report required to meet TX Commission on Jail Standards Mandate)	**Y**	Please see comments below.

Securus continues to lead the corrections industry with ever-improving technology and solutions. The ConnectUs Inmate Forms/Grievance Application will have a significant impact to facility operational process. It is a custom workflow tool that makes your grievance process completely paperless and allows for grievances to easily be processed by your staff. This application not only creates staff efficiencies but also saves your correctional facility money.

Functional Overview

The Inmate Forms/Grievance Application is used to electronically process a wide variety of forms submitted by inmates. At a summary level, it performs these functions:

- Provides form creation and management tools to create and manage multiple form types, each with its own customized workflow
- Provides a user interface for inmates to
  - View a list of available form types for completion
  - Complete and submit a form type
  - View a list of their submitted forms and their statuses

- - - o View the resolution provided to a specific form and either Accept or Appeal the resolution
    - ▪ Provides a user interface for facility staff to
        - o View forms awaiting their action
        - o Read and assign a form to another staff member for resolution
        - o Request more information from the inmate about a form
        - o Provide a resolution to a submitted form back to the inmate
    - ▪ Provides option to provide one or more Appeal levels to the workflow
    - ▪ Provides staff supervisors ability to
        - o See reports of the volumes and progress of forms through the workflow
        - o See pie charts representing age of forms currently in the workflow
        - o Assign staff members to process specific forms
    - ▪ Provides an audit trail of all staff actions in the workflow
    - ▪ Provides storage and retention of all forms
    - ▪ Secures access to forms to inmate and only staff assigned to form type

Forms Overview

The Inmate Forms/Grievance Application allows customers to emulate their existing paper forms in an electronic format. Examples of Uses of Forms:

- ▪ General Grievance
- ▪ General Request
- ▪ Request medications
- ▪ Request Law Library Access

Form Capabilities

Key form capabilities include:

- ▪ Fixed text labels for titles, labels and instructions
- ▪ Text fields that are automatically filled from the NextGen Secure Communications Platform™ data. e.g. Custody Account Number
- ▪ Text fields entered by the inmate
- ▪ Text fields entered by facility staff that can be configured to be hidden or viewable by inmate
- ▪ Check boxes
- ▪ Customizable graphic for facility logo at top of form

- Work-flow unique to the form type. A General Grievance could have a workflow with multiple Appeal Levels, while a request for Law Library Access could have no Appeal level.

Authenticated and Anonymous Forms

Forms are configured to be either Authenticated or Anonymous

Authenticated Forms

Authenticated Forms require an inmate to login (authenticate) prior to completing the form. The Grievance application attaches the inmate's identity to the form for the visibility of facility staff. Optionally, inmates can be required to re-authenticate to submit forms. The re-authenticate option is set in IFD Provisioning and applies to all authenticated forms.

Anonymous Forms

An "anonymous form" does not require the inmate to login to the Inmate Forms/Grievance Application. The Inmate Forms/Grievance application does not attach the inmate's identity to the form to protect inmate from possible recrimination. Anonymous forms have no means by which the inmate may protest (escalate) the resolution of the form. Therefore, anonymous forms cannot have escalation levels.

Since anonymous forms have a simpler workflow than authenticated forms, they can be used as a light-weight processing of forms. Anonymous forms could be used to capture and process simple requests that do not need a response to be sent back to the inmate.

Just because the Inmate Forms/Grievance Application does not track the identity of the inmate submitting an Anonymous form, the form can ask the inmate to provide their name &/or custody account number.

Anonymous forms can be accessed by inmates whose PIN numbers are inactive and are restricted from using the phone system.

Forms Processing Workflow

The Inmate Forms/Grievance Application provides a configurable work flow for processing inmate form submissions. It is based on a form workflow layer template that is configured for each level of each form type.

The workflow for Anonymous forms is a simpler subset of that for Authenticated forms since anonymous forms cannot be returned to the inmate.

The Anonymous work flow is:

1. The inmate accesses the Inmate Forms/Grievance Application on ConnectUs

2. The inmate selects an Anonymous form type, completes it and submits it.

3. The form is routed to the Assigner who reviews and assigns the form to a Processor or Group of Processors. The assignment step can be automated if there is only one Processor for a form type

4. The Processor reviews the form and either

   o Assigns it to another Processor, or
   o Enters a resolution to the inmate request/grievance.

The basic work flow provided by the Inmate Forms/Grievance Application is:

1. The inmate accesses the Inmate Forms/Grievance Application on ConnectUs

2. The inmate selects a form type, then if not already logged in, is prompted to authenticate to the Inmate Forms/Grievance application.

3. Inmate completes input fields of form and submits it.

4. The form is routed to the Assigner who reviews and assigns the form to a Processor or Group of Processors.

   a. The assignment step can be automated if there is only one Processor for the form type.

5. The Processor reviews the form and either

   o Assigns it to another Processor
   o Requests more information from the inmate, or
   o Enters a resolution to the inmate request/grievance.

6. The form is routed back to the inmate for the inmate to

   a. Provide requested information, or

   b. Respond to the resolution provided. The inmate can

      i. Actively accept it

      ii. Passively accept it by doing nothing, or

      iii. Appeal it to the next level

Appeal Levels

One or more Appeal Levels can be configured for each form. Simple requests typically do not have appeal levels configured. Formal grievance forms can have one or more appeal levels depending on the facility's existing grievance process. The Appeal Level work flow similar to the initial (Level 0) workflow.

Please note that we also offer Forms and Grievances on our SecureView tablet. Please see **Exhibit E** for details.

Kiosk application for medical request shall work directly with current medical applications/staff, with the ability to track request (time stamping) throughout the workflow. (grievance aging report required to meet TX Commission on Jail Standards Mandate)	**Y**	Please see comments below.

The Securus Sick Call application allows an inmate to report an ailment to facility staff by selecting from a predetermined list. The Sick Call application delivers the following benefits to your facility:

- Automates manual processes
- Enables staff to focus on security
- Eliminates the unnecessary movement of inmates within the facility
- Allows authorized infirmary staff to access calls anytime/anywhere
- Provides a higher quality of service to inmates, reducing grievances

The following depicts the steps to place a sick call using Securus' Sick Call application.

Sick Call Application

1. Select the "Sick Call" application from the SVV terminal

2. Add symptoms

3. Click "Submit"
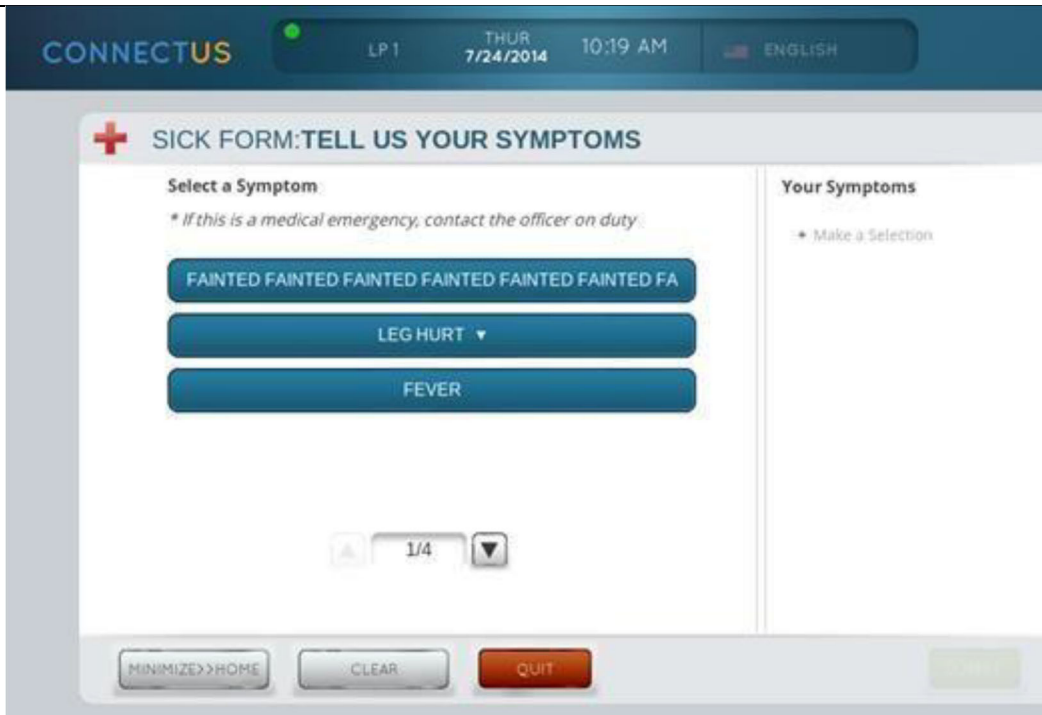
4. Review the call by clicking on "Calls"
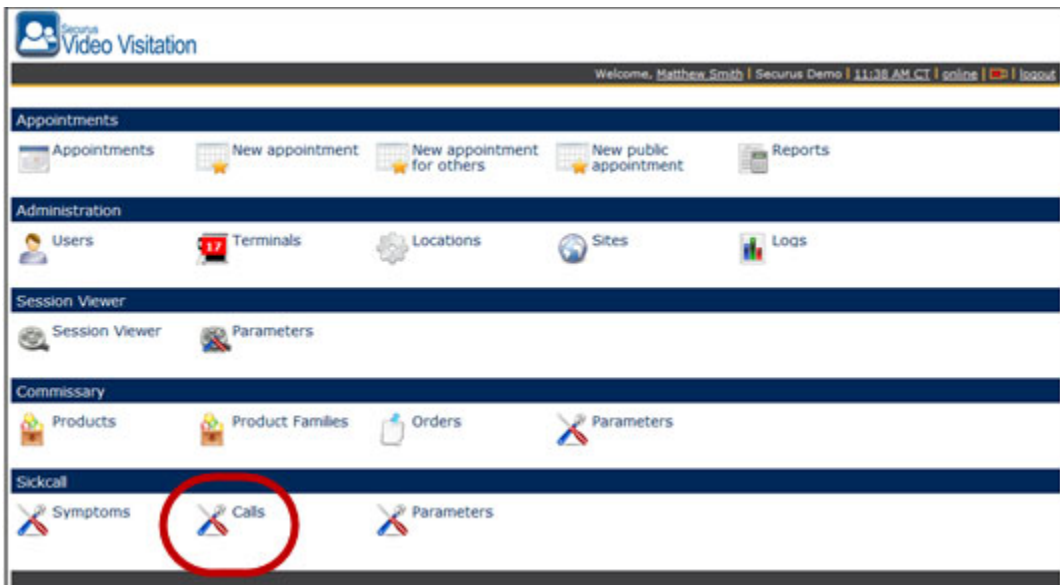
5. Review and/or export calls
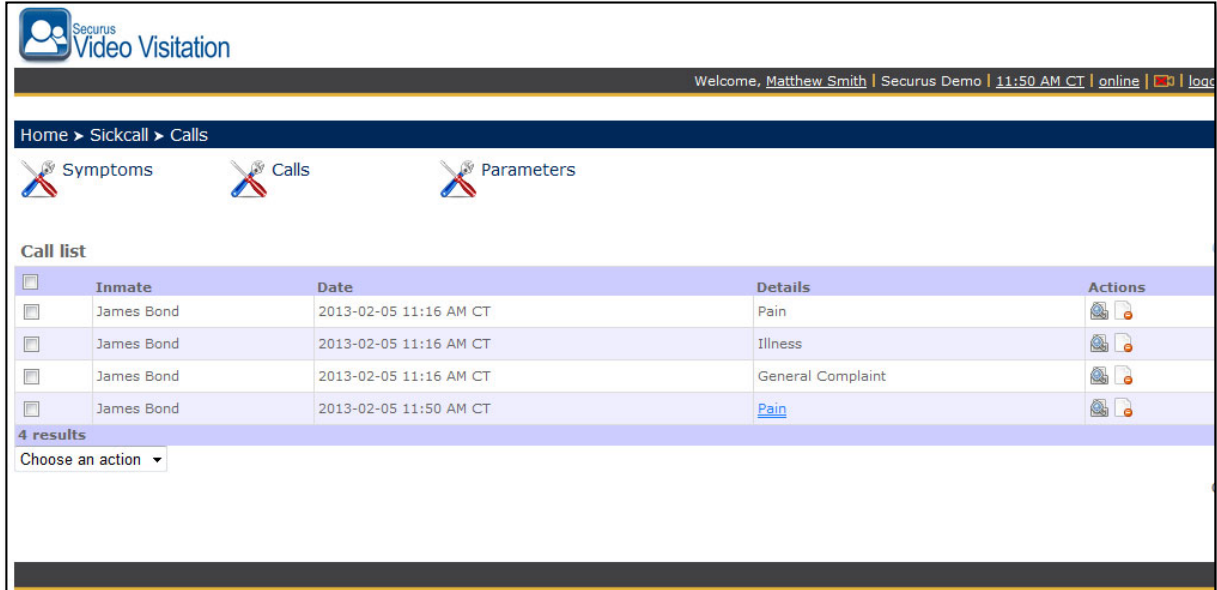
Please note that we also offer this application on our SecureView Inmate Tablets.

Kiosk shall have the ability to have a scrolling banner across the screen (information approved by the Sheriff's Department).	**Y**	Please see comments below.

ConnectUs™ allows you to easily publish notifications that are always displayed on the ConnectUs™ terminal. In addition to providing pertinent facility-related information, these messages can be used to promote new products, services, and promotions such as Video Visitation.

See examples of the banner at the bottom of the kiosk screen below.
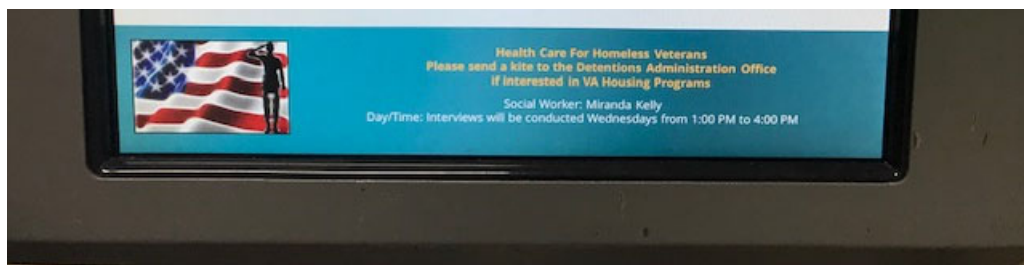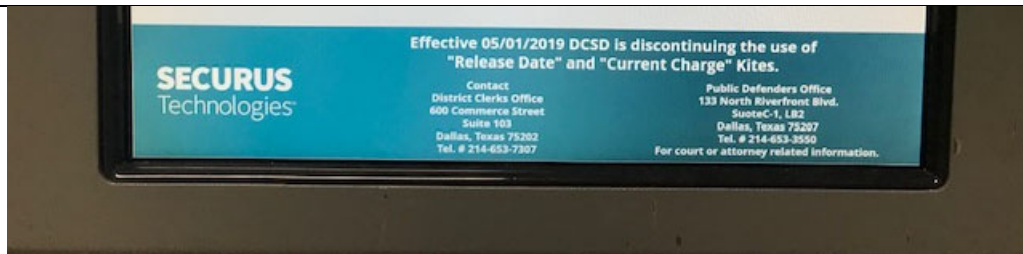
Kiosk (and other optional technology) shall have the ability of additional applications as approved and agreed upon by the Sheriff dept. representative.	Y	Please see comments below.

A decade ago, it was hard to imagine that your correctional facility would need anything more than a telephone on the wall for inmate communications. Today, there are a wide variety of communications options and the device on the wall can be used for so much more than telephone calls.

ConnectUs™ is Securus' vision for the future of inmate communication and self-help services. ConnectUs™ includes an integrated video terminal that facilitates access to Securus and third-party services through a common interface. Your facility can completely manage what an inmate can or cannot do through the ConnectUs™ software.

The ConnectUs™ software enables users to perform multiple operations, similar to a smartphone. Inmates can place a telephone call or join a video visitation session, read a digital inmate handbook, submit a grievance, watch a tutorial video or place a commissary order.

ConnectUs™ also manages which applications are available to inmates and when. It ensures that a scheduled visit is not interrupted by another inmate placing a telephone call or using the device to place a commissary order. Moreover, other vendors easily create and publish an application for use by your inmates through ConnectUs™.

Imagine turning your existing hardware into multi-purpose inmate communication devices…

Which present a familiar interface that completely controls **_everything_** an inmate is presented with…

Yet provides unprecedented communication access within the facility and beyond…

Providing automated reporting compliance, and conflict management…

With an infinite ability to scale—allowing quick implementation of whatever the "next" app might be…

Inspired Design

ConnectUs™ is a collection of intentional details that add up to an impressively powerful inmate communication platform that consolidates all inmate activities into a single unified interface. With a customized mix of applications, your facility can deliver an experience that keeps pace with today's technology while making life better for your inmates and staff.

Multi-language   Digital Bulletin Board   BIG Buttons

Multi-task   Conflict Resolution   Touch Screen

1. Conflict Resolution

ConnectUs™ manages available applications by the time of the day or day of the week. This allows for information applications, such as an inmate handbook, to be available during non-calling hours. ConnectUs™ automatically prioritizes scheduled communication events higher than non-scheduled communication events. If a video visitation is scheduled and another inmate wants to use the same terminal for a telephone call, ConnectUs™ will limit the call duration to avoid conflict with the video visitation session. Similarly, the Telephone Calling Application is disabled when a video visit is scheduled to begin. We manage usage conflicts, so your staff does not have to.

2. Applications

ConnectUs™ provides an "app store" environment where new functionality can quickly and easily be developed and delivered to the inmate.

3. Date/Time

ConnectUs™ continually displays date and time so inmates can manage their schedules and not miss or late to scheduled communication events.

be

4. Multi-Language

ConnectUs™ supports the ability to display applications in multiple languages – allowing inmates to use the system in their preferred language and enhancing your facility's support of non-English speaking inmates.

5. Digital Bulletin Board

ConnectUs™ allows you to easily publish notifications that are always displayed on the ConnectUs™ terminal. In addition to providing pertinent facility-related information, these messages can be used to promote new products, services, and promotions such as Video Visitation.

6. Multi-Tasking

ConnectUs™ allows an inmate to use multiple applications at the same time. They can be on telephone call while reading the inmate handbook, or placing a commissary order, or submitting a grievance. The ability to multi-task allows inmates to accomplish tasks quickly instead of unnecessarily preventing other inmates from using the terminal.

System/Kiosk shall have the ability to accommodate inmates needing to communicate using American Sign Language (ASL). A basic Video Relay Services (VRS) feature are required.	**Y**	Please see comments below.

Securus' NextGen Secure Communications Platform™ (NextGen SCP™) provides support for hearing-impaired inmates 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 inmate call controls, management, and investigative abilities expected for inmate 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 Dallas County 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 inmates with "equal access" to communication services while allowing Dallas County to provide, manage, and investigate inmate VRS calls in a manner consistent with traditional inmate calls.

Securus VRS provides equal access by allowing Dallas County to:

- Provide VRS-capable inmate 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 inmate calls
- Record VRS calls in accordance with the same recording controls that govern whether or not to record traditional inmate 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 inmate call for both the inmate and the other end of the video portion of the VRS call. The other end of the VRS call might be the inmate'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 inmate call management control structures as for traditional inmate 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 inmate PAN lists
- Call recording
- Collecting VRS calls in inmate calls for investigations and evidence

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

Inmate access to Securus VRS is provided as an application available through ConnectUs—the controlled inmate interface provided on inmate kiosks. ConnectUs can be configured to present numerous applications to Dallas County inmates, which allows inmates to use the same multi-function terminal for Securus VRS calls as for standard inmate calling, Securus Video Visitation, Inmate Forms, and more.

Because VRS calls are required by the FCC to be free, all inmate VRS calls will be provided at no cost to the inmate. To ensure Dallas County can prevent the unauthorized use of Securus VRS to place free calls, the Securus VRS is also integrated with NextGen SCP to allow Dallas County to designate which inmates are allowed to place VRS calls. The Securus VRS ConnectUs application requires inmates to enter their designated inmate 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, Dallas County 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.

C | TRANSITION/ IMPLEMENTATION PLAN AND TIMELINE

C.   TRANSITION/IMPLEMENTATION PLAN AND TIMELINE. (15 points).

Respondents are to submit an estimated implementation plan and transition date schedule. The plan shall be designed to provide seamless transition with minimal interruption of telephone services to inmates. The plan/schedule shall include a detailed explanation of the following items:

1)   Procedures for transition of service/equipment from the existing IPS to the new IPS to include assignment of PINS and updating of calling lists for current inmates.
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

> **Selecting Securus ensures no disruption in service for Dallas County inmates—even as we upgrade and expand service functionality.**

As the incumbent provider of services at Dallas County, Securus is uniquely positioned to upgrade the County to our NextGen Secure Communication Platform™ (NextGen SCP™) without any downtime, and with no impact to inmates or friends and family members. Securus is proud of our five-year association with Dallas County. We believe our longtime partnership has proven we bring technology capabilities that set Securus apart from any other vendor. We have worked closely with Dallas County to deploy new and existing technologies to meet the needs of the county and its constituents.

We know this RFP is about the future and choosing a supplier that will meet your needs over the next 5 years. We believe our track record and our response to this RFP demonstrate that we will continue to bring value to the partnership going forward. We also ask that you consider the following additional advantages of continuing to work with Securus versus selecting another provider:

1. **Immediate Transitioning to RFP Offer.** If you choose Securus as your future vendor, we can immediately transition you to our offer—no need to wait for project plans and installation schedules.

2. **No Impact on Inmates or Their Family Members and Friends.** No need to establish new accounts, no need to arrange for refunds of existing accounts, no need to work through call blocking problems or answer questions about how to set up new accounts from confused end-users. No two competitors have the same rules or programs in place for completing calls—stay with Securus and avoid inmate frustration and called party complaints.

3. **Eliminate Unnecessary Work By Staff.** Staying with Securus means your staff does not need to learn to work with a new vendor. No new contacts to establish. Your staff will continue to work with the same account team and field service technicians who already know your operation and already have security clearances for your facility.

4. **Our knowledge of your needs gained from working together for over past five years.** Through our experience in working together, we understand your operation. You know our employees, and we know you. We understand your internal operating procedures and how things get done within your facility. There is no substitute for the experience we've both gained in working together.

5. **Integration with existing processes and vendors.** Through our partnership, we've developed specific ways to handle day-to-day issues. We've integrated processes, systems, and applications. We know how to work with your existing vendors and equipment. By selecting Securus, you will avoid the difficult process of re-mapping, re-engineering, re-developing, and re-training integration links. Vendor continuity prevents system interoperability issues during the transition.

6. **Avoid Having to Work With Multiple Systems and Recordings For Investigative Work.** Staying with Securus, you gain continuity between current and stored recordings. You avoid losing existing investigative history the need to re-train investigators and do not adversely impact open cases.

7. **Eliminate Risk of Performance.** Does your RFP address all your needs? Are you sure? Could a potential new provider misinterpret what you are asking for in your requirements? Can they deliver what they promise? Do they have the proper licenses to provide you the technology they claim they can provide—what will happen if they get shut down? Your experience with Securus provides greater certainty that you are going to get what you need—from a company that you know can deliver.

2) Times when telephone instruments will be operational identifying possible "down time"

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

As the incumbent provider of services, Securus is uniquely positioned to transfer Dallas County to our NextGen SCP system without downtime.

Please see our charts below.

Service/Functionality	Number of Days to Install
Automated Information Service (AIS)	**60 days**
THREADS Investigative Platform	**Currently Installed**
ICER (Inmate Intercommunication Evaluation and Reporting System)	**Currently Installed**

IPRO (Investigator Pro)	**30 days**
Tablet Installation and Activation	**90 days**

Implementation Time Based on Delivery System[1]

Service/Application	Delivery System	
	Multi-Function Kiosk	**Tablets**
Telephone Calls	**Currently Installed**	90 days
Video Visits	**Currently Installed**	90 days
Video Relay Service	**2 days**	N/A
JobView	**Currently Installed**	90 days
Law Library	**Currently Installed**	90 days
eMessaging	**10 days**	90 days
Digital Mail	**10 days**	90 days
Document and Video Viewer	**Currently Installed**	90 days
Grievances and Inmate Forms	**Currently Installed**	90 days
Religious Materials	**N/A**	90 days
Books	**N/A**	90 days
Education/Classes	**N/A**	90 days

[1] Timelines are contingent upon the availability of jail staff

3)   Service coordination requirements between the Contractor and Local Exchange Companies (LEC's)

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

As the incumbent inmate communications provider for Dallas County, Securus has already worked with the local exchange carriers to coordinate service. Securus will maintain the service currently in place through the LECs for the duration of the next contract, if awarded.

4)   Any software programming and preparation for installation of system and equipment, as required.

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

Only the incumbent provider for Dallas County can seamlessly upgrade the system in place without requiring additional software programming.

As your current vendor, and with the history supporting inmate communications at Dallas County, Securus is positioned to support your objectives in a manner that no other vendor can provide, such as:

1. **Our knowledge of your needs gained from working together over the past five years.** We understand your internal operating procedures and how things get done within your facility.   There is no substitute for the experience both of our organizations have gained by working together over an extended period of time.

2. **Integration with existing processes and vendors.** There will be no need to start over and go through the difficult process of re-mapping, re-engineering, re-developing, and re-training integration links.

3. **Immediate transitioning to RFP Offer.** With our Centralized Platform and deployed integrations at DallasCounty, Securus can immediately transition you to the new technologies and avoid disruptive installation schedules.

4. **No impact on inmates or their friends or family members.** There will be no need to establish new accounts, arrange for refunds of existing accounts, work through call blocking problems, or answer questions about how to set up new accounts from confused end-users. By staying with Securus, you avoid inmate frustration and called party complaints.

5. **Eliminate unnecessary work by staff.** With Securus, your officers will not have to learn a new system or work through new integrations. Your staff will continue to work with the same state-of-the-art software solutions with dedicated account team and field service technicians who already know your operation.

6.   **Eliminate risk of performance.** With Securus, Dallas County has seen first- hand our ability to meet and exceed our commitments.

By continuing our partnership, Dallas County and the Dallas County Sheriff's Office has a vendor that has the **proven qualifications, experience, technology, equipment, financial stability, and response times to meet your expectations.** Securus couples its industry-leading technologies with exceptional service and a robust revenue stream to the County to deliver an inmate communications solution that is second to none.

5)   **Responsibilities required of Dallas County during implementation**
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

As previously stated, as your current vendor, there will be no disruption in inmate to community communication as your inmate phones and visitation are in place.

- There will be no need to start over and go through the difficult process of re-mapping, re-engineering, re-developing, and re-training integration links.

- There will be no need to establish new accounts, arrange for refunds of existing accounts, work through call blocking problems, or answer questions about how to set up new accounts from confused end-users. By staying with Securus, you avoid inmate frustration and called party complaints.

- **Eliminate unnecessary work by staff.** With Securus, your officers will not have to learn a new system or work through new integrations. Your staff will continue to work with the same state-of-the-art software solutions with dedicated account team and field service technicians who already know your operation.

- **Eliminate risk of performance.** With Securus, Dallas County has seen first- hand our ability to meet and exceed our commitments.

At the beginning of the implementation project, the Securus project management team will work with the Dallas County 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 Dallas County 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 Dallas County team. The automated email notifications the communication of updates and status changes for major milestones and other tasks.

D| COST – LOWEST OVERALL INMATE/FAMILY COSTS

Pursuant to RFP Instructions, this section has been bound and placed in a separate sealed envelope for Dallas County.

E | SMALL BUSINESS ENTERPRISE

E.   Small Business Enterprise (15 points)

     Submit all Mandatory Forms found in the attachment section of this solicitation.
SECURUS HAS READ, UNDERSTANDS AND WILL COMPLY WITH THIS REQUIREMENT.

Please find the mandatory forms (Attachments 1 through 4) on the following pages.

Deleted pursuant to Addendum #3.

EXHIBITS

EXHIBIT A: Audited Financial Reports
EXHIBIT B: Dun & Bradstreet Report
EXHIBIT C: THREADS Overview
EXHIBIT D: SecureView Tablet Program
EXHIBIT E: ICER Overview
EXHIBIT F: Investigator Pro Overview
Exhibit G: Public Telephone Rates
Exhibit H: Addendum
Acknowledgements

A: AUDITED FINANCIAL REPORTS

Securus Technologies Holdings, LLC (formerly Securus Technologies Holdings, Inc.)

Consolidated Financial Statements
December 31, 2018 and 2017

Contents

pwc

Report of Independent Auditors

To the Management and the Board of
Directors of Securus Technologies Holdings, LLC

We have audited the accompanying consolidated financial statements of Securus Technologies Holdings, LLC and its subsidiaries ("the Company"), which comprise the consolidated balance sheets as of December 31, 2018 and 2017, and the related consolidated statements of operations, stockholder's/member's equity and cash flows for the year ended December 31, 2018 and for the period from November 1, 2017 through December 31, 2017.

Management's Responsibility for the Consolidated Financial Statements

Management is responsible for the preparation and fair presentation of the consolidated financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on the consolidated financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on our judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, we consider internal control relevant to the Company's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of Securus Technologies Holdings, LLC and its subsidiaries as of December 31, 2018 and 2017, and the results of their operations and their cash flows for the year ended December 31, 2018 and for the period from November 1, 2017 through December 31, 2017 in accordance with accounting principles generally accepted in the United States of America.

Emphasis of Matter

As discussed in Note 1 to the consolidated financial statements, the Company changed the manner in which it accounts for revenue from contracts with customers in 2018. Our opinion is not modified with respect to this matter.

Other Matter

The consolidated financial statements of the Company for the period from January 1, 2017 to October 31, 2017 were audited by other auditors whose report, dated February 28, 2018, expressed an unmodified opinion on those financial statements and included a paragraph describing the acquisition of Securus Holdings, Inc. and Subsidiaries by SCRS Acquisition Corporation on November 1, 2017.

PricewaterhouseCoopers LLP

April 11, 2019

2

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Consolidated Balance Sheets
(dollars in thousands)

	Successor	
	December 31, 2018	December 31, 2017
Assets		
Current assets:		
Cash and cash equivalents	$ 12,890	$ 53,954
Restricted cash	6,923	8,236
Accounts and other receivables, net	35,916	41,701
Inventory	11,466	5,896
Prepaid expenses and other current assets	18,222	19,210
Total current assets	85,417	128,997
Property and equipment, net	155,450	131,975
Intangibles and other assets, net	783,741	776,675
Goodwill	1,018,119	987,778
Total assets	$ 2,042,727	$ 2,025,425
Liabilities and Member's Equity		
Current liabilities:		
Accounts payable	$ 26,556	$ 19,421
Accrued liabilities	63,359	90,858
Deferred revenue and customer advances	35,339	27,052
Current portion of long-term debt	10,202	9,450
Total current liabilities	135,456	146,781
Deferred income taxes	129,029	140,163
Long-term debt	1,294,791	1,218,336
Other long-term liabilities	3,555	6,945
Total liabilities	1,562,831	1,512,225
Commitments and contingencies (see Note 10)		
Member's equity:		
Member's capital	445,501	445,501
Retained earnings	34,395	67,699
Total member's equity	479,896	513,200
Total liabilities and member's equity	$ 2,042,727	$ 2,025,425

The accompanying notes are an integral part of these consolidated financial statements.

3

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Consolidated Statements of Operations
(dollars in thousands)

	Successor		Predecessor
	December 31, 2018	For the Period From November 1 to December 31, 2017	For the Period From January 1 to October 31, 2017
Revenue:			
Inmate telecommunications and investigative products	$ 419,913	$ 69,872	$ 351,698
Media and communications services	88,944	11,910	50,060
Payment services	143,746	20,272	93,261
Electronic monitoring services	31,085	5,348	25,579
Total revenue	683,688	107,402	520,598
Operating costs and expenses:			
Cost of service	311,843	47,621	225,341
Selling, general and administrative expenses	195,606	36,562	155,668
Depreciation and amortization expense	91,836	11,282	83,978
Goodwill impairment	11,628	-	
Transaction expenses	18,370	220	55,043
Total operating costs and expenses	629,283	95,685	520,030
Operating income	54,405	11,717	568
Interest and other expenses, net	104,494	14,165	44,631
Impairment of deferred loan costs	-	-	12,380
Loss before income taxes	(50,089)	(2,448)	(56,443)
Income tax benefit	(14,972)	(70,147)	(14,588)
Net income (loss)	$ (35,117)	$ 67,699	$ (41,855)

The accompanying notes are an integral part of these consolidated financial statements.

4

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Consolidated Statements of Stockholder's / Member's Equity
(dollars in thousands)

	Common Stock		Additional Paid-in Capital	Member's Capital	Retained Earnings (Accumulated Deficit)	Total Stockholder's / Member's Equity
	Shares	Amount				
Predecessor:						
Balance, December 31, 2016	1,000	$ -	$ 256,657	$ -	$ 9,123	$ 265,780
Share-based compensation	-	-	4,095	-	-	4,095
Net loss	-	-	-	-	(41,855)	(41,855)
Balance, October 31, 2017	1,000	$ -	$ 260,752	$ -	$ (32,732)	$ 228,020
Successor:						
Balance, November 01, 2017	1,000	$ -	$ 445,501	$ -	$ -	$ 445,501
Net income		-	-	-	67,699	67,699
Conversion to LLC	(1,000)	-	(445,501)	445,501	-	-
Balance, December 31, 2017	-	-	-	445,501	67,699	513,200
Cumulative effect of accounting change	-	-	-	-	1,813	1,813
Net loss	-	-	-	-	(35,117)	(35,117)
Balance, December 31, 2018	-	$ -	$ -	$ 445,501	$ 34,395	$ 479,896

The accompanying notes are an integral part of these consolidated financial statements.

5

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Consolidated Statements of Cash Flows
(dollars in thousands)

| | Successor | | Predecessor |
	December 31, 2018	For the Period From November 1 to December 31, 2017	For the Period From January 1 to October 31, 2017
Cash flows from operating activities:			
Net income (loss)	$ (35,117)	$ 67,699	$ (41,855)
Adjustments to reconcile net income (loss) to net cash provided by operating activities:			
Depreciation and amortization	91,836	11,282	83,978
Goodwill impairment	11,628	–	–
Deferred income taxes	(16,030)	(70,338)	(14,703)
Share-based compensation	–	–	4,095
Amortization of deferred financing costs and discounts	4,744	470	5,880
Acceleration of deferred loan cost amortization	–	–	12,380
Change in fair value of derivatives	1,957	–	(6,040)
Payment of and change in fair value of contingent consideration	(14,873)	–	24,745
Other operating activities, net	(98)	(550)	(153)
Changes in operating assets and liabilities, net of acquisitions:			
Accounts receivables	8,367	(8,640)	3,473
Prepaid expenses and other current assets	397	1,410	(10,295)
Inventory	(5,570)	(2,355)	286
Other assets	(10,955)	210	4,346
Accounts payable	7,210	1,212	(1,345)
Accrued and other liabilities	6,859	(9,787)	24,232
Net cash provided by (used in) operating activities	50,355	(9,387)	89,024
Cash flows from investing activities:			
Purchase of property and equipment	(64,748)	(11,116)	(38,742)
Additions to intangible assets	(21,735)	(3,987)	(24,291)
Business acquisitions, net of cash acquired	(69,136)	(5,819)	–
Net cash used in investing activities	(155,619)	(20,922)	(63,033)
Cash flows from financing activities:			
Net activity on revolver	8,500	12,000	2,000
Long-term debt borrowings, net of issuance costs	73,976	70,000	–
Payments on long-term debt	(10,014)	–	(10,963)
Payment of contingent consideration	(5,670)	(4,547)	(19,525)
Repayment of capital lease obligations	(3,905)	(497)	(3,055)
Net cash provided by (used in) financing activities	62,887	76,956	(31,543)
Increase (decrease) in cash, cash equivalents, and restricted cash	(42,377)	46,647	(5,552)
Cash, cash equivalents, and restricted cash:			
Beginning of period	62,190	15,543	16,511
End of period	$ 19,813	$ 62,190	$ 10,959
Supplemental disclosures of cash flow information:			
Cash paid during the period for:			
Interest	$ 97,978	$ 13,128	$ 39,411
Income taxes, net of refunds	1,846	526	1,123
Noncash investing and financing activities:			
Additions to capital leases	$ –	$ –	$ 5,795

The accompanying notes are an integral part of these consolidated financial statements.

6

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Note 1.   Business and Summary of Significant Accounting Policies

Securus Technologies Holdings, LLC, (Securus, and together with its subsidiaries, collectively, the Company), formerly known as Securus Technologies Holdings, Inc., is based in Dallas, Texas and is a leading provider of civil and criminal justice technology solutions that improve public safety and modernize the incarceration experience for approximately 3,500 correctional facilities and over 1,200,000 inmates across North America. As one of the largest inmate communications providers in the corrections industry, the Company's product and service combinations deliver unique, full criminal lifecycle solutions from pre-incarceration incident management through post-incarceration monitoring.

On November 1, 2017 (the Acquisition Date), SCRS Acquisition Corporation (SCRS) acquired 100% of the issued and outstanding capital stock of Connect Acquisition Corp., the indirect parent of Securus, in a business combination accounted for as an acquisition (the Securus Acquisition, see Note 2). As a result, the Company's Consolidated Statements of Operations, Consolidated Statement of Stockholder's Equity, and Consolidated Statement of Cash Flows for the period from January 1, 2017 to October 31, 2017 (the period ended October 31, 2017) are referenced herein as the predecessor financial statements (the Predecessor or the Predecessor Company). The Company's Consolidated Balance Sheets as of December 31, 2018 and 2017 and the related Consolidated Statements of Operations, Consolidated Statements of Member's Equity, and Consolidated Statements of Cash Flows for the period from November 1, 2017 to December 31, 2017 (the period ended December 31, 2017) and the period from January 1, 2018 to December 31, 2018 (the period ended December 31, 2018) are referenced herein as the successor financial statements (the Successor or the Successor Company). Furthermore, the consolidated financial information for the period after the Securus Acquisition is presented on a different basis of accounting than that for the period before the Securus Acquisition, and therefore is not comparable.

Principles of consolidation and basis of presentation: The accompanying consolidated financial statements include the accounts of Securus and its wholly owned subsidiaries. All intercompany accounts and transactions have been eliminated in consolidation. In 2018, the Company revised its reported revenue categories within the Consolidated Statement of Operations, as compared to previous years, to present revenues in better accordance with the types of products and services offered in its business operations.

Accounting estimates: The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America (GAAP) requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosures of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenue and expenses during the reporting period. Significant items subject to such estimates include the purchase price allocation associated with business combinations, valuation allowances for receivables, the recoverability of property and equipment, contingent consideration, and deferred income taxes.

Management evaluates its estimates and assumptions on an ongoing basis using historical experience and other factors, including the current economic environment. Management believes this approach to be reasonable under the circumstances. Management adjusts such estimates and assumptions when facts and circumstances dictate. As future events and their effects cannot be determined with precision, actual results could differ significantly from these estimates. Changes in estimates will be accounted for prospectively.

**Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)**

Notes to Consolidated Financial Statements

Cash and cash equivalents and restricted cash: Cash equivalents consist of highly liquid investments, such as certificates of deposits, money market funds and short term treasury instruments, with original maturities of 90 days or less. Restricted cash accounts hold amounts established for regulatory requirements or for the benefit of certain customers in the event the Company does not perform under the provisions of the respective underlying contracts with these customers.

Trade accounts receivable: Trade accounts receivable are recorded at the invoice amount and do not bear interest. The majority of trade accounts receivable represents amounts collected by credit card processors and third party billing agents for calls placed or to be placed through the Company's telephone platforms. Additionally, the Company holds receivables from various government agencies for prepaid calling plans, software sales, offender monitoring services, online payment services, communications and media services, and investigative analysis. The Company's trade receivables are analyzed for collectability based on the age of individual accounts or types of customers, and an allowance for doubtful accounts is maintained based on the age of those receivables. The allowance for doubtful accounts is the Company's best estimate of the amount of probable credit losses in its existing accounts receivable. The Company's policy is to write-off accounts after 90–180 days from invoice date, depending on the type of customer, or after all collection efforts have failed.

Fair value of financial instruments: The Company's financial instruments consist of cash and cash equivalents, restricted cash, accounts receivable, accounts payable, and long-term debt (including the current portion) as of December 31, 2018 and December 31, 2017. The Company's financial instruments also included interest rate caps as of December 31, 2018, which are recorded in Intangibles and other assets, net on the Consolidated Balance Sheet at fair value in accordance with market interest rates. In accordance with the Company's adoption of a recent accounting pronouncement (see 'Recently issued accounting pronouncements' within Note 1), the Company is not required to disclose the fair value of financial instruments carried at amortized cost, including long-term debt.

Concentrations of credit risk: Financial instruments, which potentially expose the Company to concentrations of credit risk, consist primarily of cash and cash equivalents and accounts receivable. The Company's revenues are concentrated in the United States in the corrections industry. At December 31, 2018, one billing agent comprised approximately 10.5% of total trade accounts receivable. There were no customers or agents that comprised more than 10% of total trade accounts receivable at December 31, 2017. The Company does not require collateral on accounts receivable balances and provides allowances for potential credit losses.

Inventory: The Company's inventory consists of media players. Inventory is stated at the lower of cost (first-in, first-out basis) or net realizable value. Inventory is fully comprised of finished goods.

Property and equipment: All purchases of property and equipment are stated at cost and include costs necessary to place such property and equipment in service. Property and equipment acquired through mergers and acquisitions are recorded at fair value as of their acquisition date. Major renewals and improvements that extend an asset's useful life are capitalized, while repairs and maintenance are charged to operations as incurred. Construction in progress represents the cost of material purchases and construction costs for telecommunications hardware systems and offender tracking devices in various stages of completion.

Depreciation is computed on a straight-line basis using estimated useful lives of 2 to 8 years and of 3 to 5 years during the Successor and Predecessor periods, respectively, for telecommunications equipment, video visitation equipment, offender tracking devices, and office equipment. During the Successor and Predeccessor periods, inmate media kiosks and tablets are depreciated on a straight-line basis using an estimated useful life of 5 to 7 years, and leased inmate media tablets are depreciated on a straight-line basis using an estimated useful life of 18 months. Leasehold improvements and equipment acquired through capital lease arrangements are depreciated over the lesser of their useful life or lease term.

8

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Goodwill, intangibles, and other assets: Goodwill represents the excess of the purchase price over the fair value of identifiable net assets acquired in business combinations accounted for as acquisitions. Intangible and other assets include patents and trademarks, capitalized software development costs, acquired technology rights, acquired contract rights, an equity investment, and deposits and other long-term assets.

In connection with the Securus Acquisition and other business acquisitions, management assessed the value of the Company's additions to goodwill and intangible assets with the assistance of an independent appraiser based on a discounted cash flow model and multiple of earnings. Assumptions critical to the Company's fair value estimates under the discounted cash flow model include the discount rate using the weighted average cost of capital approach, royalty rate, projected average revenue growth, and projected long-term growth rates in the determination of terminal values.

There were no changes to goodwill in the Predecessor period. The changes in the carrying amount of goodwill, including the measurement period adjustments primarily related to the working capital finalization from the Securus Acquisition (see Note 2), during the Successor period were as follows (in thousands):

Goodwill pushed down through Securus Acquisition	$	982,746
Goodwill acquired through business acquisition		5,032
Balance, December 31, 2017		987,778
Measurement period adjustments		(8,917)
Goodwill acquired through GovPay Acquisition (see Note 3)		50,886
Impairment		(11,628)
Balance, December 31, 2018	$	1,018,119

Amortization of acquired technology is computed over useful asset lives, which range from 6 to 17 years and from 3 to 12 years for the Successor period and Predecessor period, respectively, in accordance with the pattern of the projected economic benefit of the asset. Amortization of acquired contracts is computed over useful asset lives, which range from 3 to 20 years and from 3 to 25 years for the Successor period and Predecessor period, respectively, in accordance with the pattern in which the economic benefit is projected to be earned each year over the life of the contract. As of December 31, 2018 and December 31, 2017, acquired contracts included customer relationships, customer license agreements, non-compete agreements, and upfront customer incentives. Amortization of capitalized software development costs is computed on a straight-line basis over 3 to 5 years for the Successor and Predecessor periods. As of December 31, 2018 and December 31, 2017, the weighted average amortization period for all intangible assets subject to amortization was approximately 16.5 and 16.9 years, respectively.

The Company performs an annual qualitative assessment of goodwill as of the last day of each fiscal year, or whenever events or circumstances indicate the fair value of the reporting unit is less than the carrying amount, to determine whether quantitative impairment testing is necessary. In accordance with the adopted Update as referenced in the 'Recently issued accounting pronouncements' section of this Note, the Company has eliminated the second step of the two-step goodwill impairment process and instead performs its annual goodwill impairment test by comparing the fair value of a reporting unit to its carrying amount and recognizes an impairment charge for the amount by which the carrying amount exceeds the reporting unit's fair value. The Company determined no goodwill impairment existed as of the period ended December 31, 2017. However, as result of the Company's testing of goodwill as of December 31, 2018, it was determined that goodwill was impaired in relation to the Company's electronic monitoring reporting unit and, therefore, an impairment loss of $11.6 million was recorded in the

9

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Company's Consolidated Statement of Operations. This impairment loss was primarily attributed to a reduction in forecasted sales and earnings for the reporting unit. The method used in the calculation of the reporting unit's fair value was comprised of the determination of the present value of the future debt-free net cash flows in accordance with observed market prices realized in actual arm's length transactions of similar, publicly traded entities.

Other intangible assets with indefinite useful lives, primarily certain trademarks and tradenames, are reviewed quantitatively annually and tested for impairment annually or more frequently if events or changes in circumstances indicate that the asset may be impaired. For this impairment test, the carrying value of the intangible asset is compared to its fair value. If the carrying value exceeds the fair value, an impairment loss is recognized by reducing the carrying value of the intangible asset to its fair value. The Company determined no impairment existed for other intangible assets with indefinite useful lives as of the periods ended December 31, 2018, December 31, 2017 and October 31, 2017.

Long-lived assets, such as property, equipment and purchased intangibles subject to amortization, are grouped with other assets at the lowest level of identifiable cash flow streams and are reviewed for impairment as a group whenever events or changes in circumstances indicate that the carrying amount of an asset may not be recoverable. Recoverability of assets to be held and used is measured by a comparison of the carrying value of the assets to the estimated undiscounted future cash flows expected to be generated by the assets. If the carrying value of the assets exceeds their estimated future cash flows, an impairment charge is recognized by the amount by which the carrying value of the assets exceeds the fair value of the assets. The Company determined that no significant impairment existed as of the periods ended December 31, 2018, December 31, 2017 and October 31, 2017.

The Company capitalizes labor and other costs associated with software developed for internal use. Software is considered for internal use if acquired, internally developed, or modified solely to meet the entity's internal needs and if during the software's development or modification, no plan exists to market the software externally. Costs incurred during the application development stage are capitalized, which includes costs to design the software configuration and interfaces, coding, installation, and testing. Capitalization of cost begins when the preliminary project stage is completed and management with the relevant authority authorizes and commits to funding a computer software project and believes that it is probable that the project will be completed and the software will be used to perform the function intended. Capitalization ceases when the project is complete or it is no longer probable that the project will be completed. Costs related to training and maintenance are expensed as incurred.

The Company capitalizes interest costs associated with internally developed software based on the effective interest rate on aggregate borrowings. The Company capitalized interest in the amount of $0.4 million, $0.1 million, and $0.1 million during the periods ended December 31, 2018, December 31, 2017, and October 31, 2017, respectively.

Effective January 1, 2018, in accordance with the adoption of the new standard related to revenue recognition (see Recently issued accounting pronouncements within this Note), the Company capitalizes costs incurred to obtain and costs incurred to fulfill a customer contract. Capitalized costs to obtain are comprised of sales commissions related to new contracts and up-front payments required by facility customers as part of the competitive process to award a contract, which are referred to in the industry as signing bonuses. Capitalized costs to fulfill are comprised of personnel and contractor costs incurred for the setup of new customers subsequent to the signing of the contract. The long-term and short-term portions of these costs are included within Intangibles and other assets, net and within Prepaid expenses and other current assets on the Consolidated Balance Sheet, respectively. These contract costs are amortized over the contractual periods to which they pertain, including expected renewals. The costs comprised of sales commissions and customer setup are amortized into Selling, general and administrative expenses in the Consolidated Statement of Operations, while the costs related to the Company's signing bonuses are amortized into Cost of Service. The weighted average amortization

period for the Company's costs to obtain and costs to fulfill was approximately 8.1 years and 9.2 years, respectively, as of December 31, 2018.

Revenue recognition: In January 2014, the Financial Accounting Standards Board (FASB) issued a new standard related to revenue recognition, to which it has subsequently released several amendments as of this report date (see Recently issued accounting pronouncements in Note 1). Under the standard, revenue is recognized when a customer obtains control of promised goods or services in an amount that reflects the consideration the entity expects to receive in exchange for those goods or services. In addition, the standard requires disclosure of the nature, amount, timing, and uncertainty of revenue and cash flows arising from contracts with customers.

The guidance permits two methods of adoption: retrospectively to each prior reporting period presented (full retrospective method), or retrospectively with the cumulative effect of initially applying the guidance recognized at the date of initial application (modified retrospective method). The Company utilized the modified retrospective method by which the reporting periods prior to the period ended December 31, 2018 are not adjusted for this new standard, and the cumulative effect of this adoption is reported as an adjustment to the Company's retained earnings as of January 1, 2018 in the Consolidated Statement of Members' Equity.

The adoption of this standard impacted the accounting of only one of the Company's revenue streams: software licensing revenues on its public safety software, which are reported within Inmate telecommunications and investigative products (ITS) revenues in the Consolidated Statement of Operations. Specifically, the Company now recognizes these software licensing revenues at the point of billing and delivery of the license rather than ratably over the maintenance and support period, as the license is a functional license, not a symbolic one, that is a distinct deliverable from the support and maintenance provided to the customer. Further, vendor-specific objective evidence, or VSOE, is no longer required for the determination of the fair value price of separate and distinct deliverables.

Adoption of this standard resulted in an increase to retained earnings as of January 1, 2018 of approximately $1.8 million, comprised of $1.4 million reduction in software licensing deferred revenues and $0.4 million in capitalized contract costs. Revenue recognition related to hardware, professional services, and maintenance services, as well as all other revenue streams of the Company, remained substantially unchanged.

Revenues related to collect and prepaid calling services generated by ITS contracts are recognized during the period in which the calls are made or upon expiration of customer accounts, which generally is six months after last usage. Revenues related to convenience fees are recorded as incurred. Revenues related to automated interactive voice response systems, investigative call analysis, and live call monitoring are recognized during the period in which the service is used based on call volume. Advance payments received to fund customer accounts are deferred until the services are delivered. The Company records the related telecommunications costs for validating, transmitting, billing and collection, and line and long distance charges, along with commissions payable to the facilities and allowances for uncollectible calls, based on historical experience, during the same period in which revenue is recognized. Regulatory fees and taxes billed to customers are recorded on a net basis.

Revenues related to media and communications services are generated through the provision of electronic communications solutions, music and other media content services, and media devices. These goods and services are provided in accordance with multi-year contracts entered into between the Company and the facilities, and revenue is recognized upon delivery of the goods and services to the inmate, or upon passage of time wherein future redemption is unlikely. The determination of the likelihood of redemption is based on an analysis of the Company's historical redemption trends, which is within approximately six months from the original transaction date. Deferred revenue is recorded for payments received in advance for the sales of these services.

11

Revenues related to payment services are generated through the provision of secure online payment solutions to both friends and families of inmates and to governmental agencies. Similar to the Company's media and communications services, payment services are provided in accordance with multi-year contracts entered into between the Company and the facility or governmental agency. Revenue is recognized upon delivery of the service.

Revenues related to offender monitoring systems and services are comprised of a subscription-based model. A flat, daily fee is charged by the Company to its customers in accordance with the number of offender monitoring devices used by the customer, and the revenue is recognized as the services are performed.

401(k) plan: The Company sponsors a 401(k) savings plan for the benefit of eligible full-time employees. The plan is a qualified benefit plan in accordance with the Employee Retirement Income Security Act of 1974. Employees participating in the plan can generally contribute a portion of annual earnings not to exceed $18,500, or $24,500 for employees 50 years of age or older. The 401(k) plan provides for the Company to make discretionary matching contributions of 50% of an eligible employee's contribution for up to 6% of their salary. Matching contributions and plan expenses were $2.4 million, $0.5 million, and $1.8 million during the periods ended December 31, 2018, December 31, 2017, and October 31, 2017, respectively.

Transaction expenses: The Company recorded approximately $18.4 million, $0.2 million, and $55.0 million of transaction expenses during the periods ended December 31, 2018, December 31, 2017, and October 31, 2017, respectively. The expenses recorded during the period ended December 31, 2018 are comprised of approximately $14.9 million of costs incurred for due diligence services for the potential acquisition of Inmate Calling Solutions, LLC (see Note 11), $2.8 million of costs incurred for the Company's acquisition of Government Payment Services, Inc. (see Note 3), $0.4 million of transaction costs incurred in the Securus Acquisition (see Note 2), and $0.2 million of other miscellaneous costs. The expenses recorded during the period ended October 31, 2017 are comprised of $29.5 million of seller's transaction costs incurred in the Securus Acquisition (see Note 2), $24.7 million of change in fair value of the Company's contingent consideration (see Note 10), and $0.1 million of transaction costs related to other business acquisitions.

Income taxes: The Company records deferred tax assets and liabilities at an amount equal to the expected future tax consequences of transactions and events. Deferred tax assets and liabilities are determined based on the future tax consequences attributable to the differences between the financial statement carrying amounts of existing assets and liabilities and their respective tax bases and operating loss and tax credit carryforwards. Deferred tax assets and liabilities are measured using enacted income tax rates expected to apply to taxable income in the years in which those differences are expected to be recovered or settled. The effect on deferred tax assets and liabilities of a change in income tax rates is recognized in the results of operations in the period that includes the enactment date.

Equity-based compensation: During the Predecessor period, the Company offered equity-based awards to executives and certain key management personnel in a long-term equity incentive plan of Securus Investment Holdings, LLC (the Predecessor Plan). The Company accounted for the Predecessor Plan based on the grant date estimated fair value of each award, net of estimated forfeitures or cancellations, over the vesting period of the equity grant.

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Incentive Compensation Plan: On April 30, 2018, SCRS Holding Corporation implemented a long term incentive compensation plan pursuant to which certain employees of the Company may be entitled to receive compensation in the event of certain qualifying events as described, and pursuant to certain conditions set forth, in the plan. Compensation costs are recognized for an award based on the award's fair value remeasured at each reporting date until the date of settlement. Change in the fair value of a liability that occur during the requisite service period is recognized as compensation cost over that period. Any difference between the amount for which a liability award is settled and its fair value at the settlement date is an adjustment of compensation cost in the period of settlement.

Commitments and contingencies: Liabilities for loss contingencies arising from claims, assessments, litigation, fines, and penalties and other sources are recorded when it is probable that a liability has been incurred and the amount of the assessment and/or remediation can be reasonably estimated. Legal fees related to loss contingencies are expensed as services are rendered.

Acquisition accounting: Business acquisitions are accounted for under the acquisition method of accounting. Allocating the purchase price requires the Company to estimate the fair value of various assets and liabilities as well as contingent consideration. Management is responsible for determining the appropriate valuation model and estimated fair values, and in doing so, considers a number of factors, including information provided by an outside valuation advisor. The Company primarily establishes fair value using the income approach based upon a discounted cash flow model. The income approach requires the use of many assumptions and estimates including future revenues and expenses, as well as discount factors and income tax rates.

Recently issued accounting pronouncements: In August 2015, the FASB released an amendment to their January 2014 update regarding the implementation of Accounting Standards Codification (ASC) 606, Revenue from Contracts with Customers. ASC 606 has superseded ASC 605, Revenue Recognition, and most industry-specific guidance throughout the Industry Topics of the Codification. Non-public companies are required to adopt the new revenue guidance for annual reporting periods beginning after December 15, 2018, with early adoption permitted. The Company elected to early adopt and thereby implemented this new accounting treatment for the reporting of its fiscal period beginning January 1, 2018 under a modified retrospective approach. The adoption of this standard resulted in a change in accounting for the Company's software licensing revenues (see Revenue recognition in Note 1), and it resulted in both a change in capitalization of contract-related costs and a change in the useful lives over which certain capitalized contract costs are amortized (see Note 4).

In February 2016, the FASB issued ASC 842, Leases, that supersedes the leasing guidance in ASC 840, Leases. Under the new guidance, lessees are required to recognize lease assets and lease liabilities on the balance sheet for all leases with terms longer than 12 months. Leases will be classified as either finance or operating, with classification affecting the pattern of expense recognition in the income statement. This update is effective for fiscal years beginning after December 15, 2019 and entities are required to adopt using a modified retrospective transition method, as full retrospective transition method is prohibited. The Company will apply this transition at the beginning of the period of adoption, January 1, 2019, and is evaluating the impact of this update on its consolidated financial statements.

13

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

In March 2016, the FASB issued an update that requires liabilities related to the sale of prepaid stored-value products to be accounted for consistently with breakage guidance in ASC 606, Revenue from Contracts with Customers, and addresses the current diversity in practice regarding the de-recognition of a prepaid stored-value product liability. Under the new guidance, an entity shall derecognize the amount related to expected breakage in proportion to the pattern of rights expected to be exercised by the product holder only to the extent that it is probable that a significant reversal of the recognized breakage amount will not subsequently occur. This update is effective for non-public entities for annual reporting periods beginning after December 15, 2018, with early adoption permitted. The Company elected early adoption as of January 1, 2018. This update does not have a material impact on the Company's consolidated financial statements.

In August 2016, the FASB issued an update to clarify the classification of various types of transactions within the statement of cash flows. Cash payments up to the amount of the contingent consideration liability recognized at the acquisition date (including measurement-period adjustments) shall be classified as financing activities; any excess shall be classified as operating activities. Cash payments made soon after the acquisition date of a business combination by an acquirer to settle a contingent consideration liability shall be classified as cash outflows for investing activities.

This update also includes a change to the classification of debt prepayments or debt extinguishment costs, which shall be classified as cash outflows in financing activities, not in operating activities. For non-public entities, this update is effective for annual reporting periods beginning after December 15, 2018, with early adoption permitted. Further, this update is to be applied using a retrospective transition method to each period presented. The Company has elected early adoption and thereby implemented this new accounting treatment for the reporting of its fiscal period beginning January 1, 2018 using the retrospective approach. This update does not have a material impact on the Company's consolidated financial statements.

In November 2016, the FASB issued an update to the presentation of transactions involving restricted cash within the statement of cash flows. In this update, amounts generally described as restricted cash and restricted cash equivalents should be included with cash and cash equivalents when reconciling the beginning-of-period and end-of-period total amounts shown on the statement of cash flows. This update does not provide a definition of restricted cash or restricted cash equivalents. This update is effective for non-public entities for annual reporting periods beginning after December 15, 2018, and early adoption is permitted. The Company elected early adoption and thereby implemented this new accounting treatment for the reporting of its fiscal period beginning January 1, 2018. This update does not have a material impact on the Company's consolidated financial statements.

In January 2017, the FASB issued an update to clarify the definition of a business for purposes of classifying whether a transaction should be accounted for as an acquisition or disposal of a business or of an asset. This update rules that even if a group of assets acquired has both inputs and processes, if those assets are concentrated in a single identifiable asset or a group of similar identifiable assets, they do not constitute a business. This update is effective for non-public entities for annual reporting periods beginning after December 15, 2018, and early adoption is permitted under certain conditions. The Company is evaluating the impact of this update on its consolidated financial statements.

14

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

In January 2017, the FASB issued an update to simplify the subsequent measurement of goodwill by eliminating Step 2 from the goodwill impairment test. In computing the implied fair value of goodwill under Step 2, an entity had to perform procedures to determine the fair value at the testing date of its assets and liabilities following the procedure that would be required in determining the fair value of assets acquired and liabilities assumed in a business combination. Instead, under this update, an entity should perform its annual goodwill impairment test by comparing the fair value of a reporting unit to its carrying amount and recognize an impairment charge for the amount by which the carrying amount exceeds the reporting unit's fair value. Any loss recognized should not exceed the total amount of goodwill allocated to that reporting unit, and an entity should consider income tax effects for any tax deductible goodwill on the carrying amount of the reporting unit when measuring the impairment loss, if applicable. This update also eliminated the requirements for any reporting unit with a zero or negative carrying amount to perform a qualitative assessment and, if it fails that qualitative test, to perform Step 2 of the impairment test. Early adoption is permitted for interim or annual goodwill impairment tests performed on testing dates after January 1, 2017, and adoption is required for annual or any interim goodwill impairment tests in fiscal years beginning after December 15, 2019. The Company elected to early adopt and thereby performed its testing of goodwill impairment under this new method by which if the fair value of a reporting unit exceeds its carrying amount, the goodwill of the reporting unit is not considered impaired. See the 'Goodwill and intangible and other assets' section of this Note for further detail on the impact of this update to the Company's consolidated financial statements.

Note 2.   Securus Acquisition

Funding for the Securus Acquisition totaled approximately $1.6 billion and consisted of $1.15 billion in net debt proceeds, including $29.5 million drawn on the revolving credit facility, used to repay the existing indebtedness of the Predecessor Company and to partially fund the acquisition, and of $446 million in equity proceeds. Under the acquisition method, the total purchase price for the Securus Acquisition was allocated on a preliminary basis to tangible and identifiable intangible assets acquired and liabilities assumed based upon their estimated fair values as of the Acquisition Date.

During the year ended December 31, 2018, the Company finalized the purchase price accounting for the Securus Acquisition and made revisions to the preliminary estimates primarily from the finalization of the working capital adjustment subsequent to the Acquisition Date. The purchase price for the Securus Acquisition was allocated as follows (in thousands):

	Preliminary	Adjustments	Final
Current assets	$ 72,787	$ -	$ 72,787
Property and equipment	126,996	-	126,996
Identifiable intangible assets:			
Acquired contract rights	477,090	-	477,090
Tradenames	109,400	-	109,400
Acquired technology rights	170,990	-	170,990
Goodwill	982,746	(8,725)	974,021
Other assets	18,854	-	18,854
Deferred income taxes	(210,501)	2,416	(208,085)
Other liabilities	(157,544)	6,309	(151,235)
Total purchase price	$ 1,590,818	$ -	$ 1,590,818

15

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

As a result of the change in control, the Company's financial statements have been presented on the basis of pushdown accounting in accordance with applicable accounting guidance. Pushdown accounting entails establishing a new basis for the assets and liabilities of an acquired company based on a "push down" of the acquirer's stepped-up basis to the acquired company in connection with a change-in-control event. Accordingly, the related accounting adjustments based on the purchase price paid by the parent company have been recorded in the financial statements of the Company. The purchase price for the Securus Acquisition was determined based on the Company's expectations of future earnings and cash flows, resulting in the recognition of goodwill. Total gross contractual receivables at the Acquisition Date were approximately $33.0 million, all of which were expected to be collected. Carryover basis accounting applies for tax purposes and goodwill arising from the transaction is not deductible for income tax purposes. All financial information presented prior to November 1, 2017 represents the Predecessor basis of accounting.

Note 3.   GovPay Acquisition

On January 1, 2018, Securus J Holdings, Inc., an indirect wholly owned subsidiary of Securus, acquired 100% of the issued and outstanding capital stock of Government Payment Services, Inc. (GovPay), a processor of electronic payments for government entities, in order to expand its customer base in the government payment processing market, for total consideration of approximately $69.3 million, all of which was paid at closing. This acquisition was funded through the Company's incremental borrowing in December 2017 under the Deutsche Bank Agreements (see Note 5). Under the acquisition method, the total purchase price of GovPay was allocated to tangible and identifiable intangible assets acquired and liabilities assumed based upon their estimated fair values as of the January 1, 2018 closing date.

The purchase price of GovPay on January 1, 2018 was allocated as follows (in thousands):

Current assets	$	2,794
Property and equipment		209
Identifiable intangible assets:		
Acquired contract rights		17,795
Tradenames		3,620
Acquired technology rights		3,960
Goodwill		50,886
Other assets		11
Deferred income taxes		(6,166)
Other liabilities		(3,824)
Total purchase price	$	69,285

GovPay's total gross contractual receivables at the acquisition date were approximately $2.7 million, of which all were expected to be collected. Transaction expenses in relation to the GovPay acquisition of approximately $2.8 million were included in the Company's Consolidated Statement of Operations for the year ended December 21, 2018. The goodwill generated in this transaction represents the synergies expected to be gained in the government payment processing market because of the complementary technology acquired and future product offerings. Carryover basis accounting applies for tax purposes and goodwill arising from the transaction is not deductible for income tax purposes.

16

**Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)**

Notes to Consolidated Financial Statements

Note 4.   Balance Sheet Components

Accounts and other receivables, net consist of the following at December 31 (in thousands):

	2018	2017
Trade accounts receivable	$ 36,649	$ 39,469
Current portion of notes receivable	317	579
Income tax receivable	1,748	1,744
	38,714	41,792
Less allowance for doubtful accounts	(2,798)	(91)
	$ 35,916	$ 41,701

Property and equipment, net consists of the following at December 31 (in thousands):

	2018	2017
Telecommunications equipment	$ 44,563	$ 29,567
Inmate media kiosks and tablets	62,765	37,276
Video visitation equipment	21,100	14,928
Offender tracking devices	11,405	8,774
Construction in progress	17,114	14,941
Office furniture and equipment	25,417	20,126
Leasehold improvements	13,170	12,410
	195,534	138,022
Less accumulated depreciation and amortization	(40,084)	(6,047)
	$ 155,450	$ 131,975

Depreciation expense for each of the periods ended December 31, 2018, December 31, 2017, and October 31, 2017 was approximately $41.9 million, $6.3 million, and $27.1 million, respectively. Property and equipment acquired through capital lease (See Note 10) equaled $7.7 million and $9.8 million, net of accumulated depreciation of $2.5 million and $0.4 million, during the periods ended December 31, 2018 and December 31, 2017, respectively.

17

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Intangibles and other assets, net consist of the following at December 31 (in thousands):

	Gross Carrying Value	Accumulated Amortization	Net	Weighted Average Life
2018				
Indefinite-lived tradenames	$ 111,690	$ -	$ 111,690	
Patents and trademarks	3,566	(340)	3,226	12.1
Capitalized software development costs	36,024	(3,195)	32,829	3.9
Acquired technology rights	173,272	(30,598)	142,674	9.4
Acquired contract rights	494,905	(16,806)	478,099	20.0
Costs to obtain customer contracts	4,417	(612)	3,805	8.1
Costs to fulfill customer contracts	4,882	(282)	4,600	9.2
Deposits and other long-term assets	6,134	-	6,134	
Equity investment	684	-	684	
	$ 835,574	$ (51,833)	$ 783,741	
2017:				
Indefinite-lived tradenames	$ 108,070	$ -	108,070	
Patents and trademarks	3,065	(75)	2,990	11.5
Capitalized software development costs	16,632	(54)	16,578	3.7
Acquired technology rights	171,462	(4,487)	166,975	9.5
Acquired contract rights	477,757	(393)	477,364	20.0
Deposits and other long-term assets	3,946	-	3,946	
Equity investment	752	-	752	
	$ 781,684	$ (5,009)	$ 776,675	

Amortization of intangibles and other assets for the periods ended December 31, 2018, December 31, 2017, and October 31, 2017 was $49.9 million, $5.7 million, and $56.9 million, respectively. Estimated amortization expense related to intangibles, excluding costs to obtain and fulfill customer contracts, deposits and other long-term assets and equity investment, for each of the next five years through December 31, 2023 and thereafter is summarized as follows (in thousands):

2019	$	58,441
2020		57,891
2021		55,285
2022		52,928
2023		48,621
Thereafter		383,662
	$	656,828

18

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Accrued liabilities consist of the following at December 31 (in thousands):

	2018		2017	
Accrued expenses	$	35,217	$	42,907
Contingent consideration		-		20,543
Accrued compensation		7,843		11,492
Amounts due to correctional facilities		6,923		3,684
Accrued taxes		3,769		7,890
Short term portion of capital leases		3,179		3,741
Accrued interest and other		6,428		601
	$	63,359	$	90,858

Note 5.   Debt

Debt consists of the following at December 31 (in thousands):

	2018		2017	
Revolving credit facility due November 2022	$	50,000	$	41,500
Secured first lien term loans due November 2024		1,009,986		945,000
Secured second lien loans due November 2025		282,500		282,500
		1,342,486		1,269,000
Less unamortized deferred financing costs		(3,250)		(2,766)
Less unamortized discount		(34,243)		(38,448)
		1,304,993		1,227,786
Less current portion of long-term debt		(10,202)		(9,450)
	$	1,294,791	$	1,218,336

Future maturities of debt for each of the following five years are as follows (in thousands):

2019	$	10,202
2020		10,202
2021		10,202
2022		60,202
2023		10,202
Thereafter		1,241,476
	$	1,342,486

19

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

On November 1, 2017, in connection with the Securus Acquisition (See Note 2), the Successor Company entered into a first lien credit agreement (the Deutsche Bank First Lien Agreement) and a second lien credit agreement (the Deutsche Bank Second Lien Agreement and, together with the Deutsche Bank First Lien Agreement, the Deutsche Bank Agreements). Specifically, the Deutsche Bank Agreements were entered into by SCRS, as the initial borrower, and by Securus when Securus became the ultimate borrower by virtue of an assignment of the debt from SCRS. Net proceeds of $1.15 billion, after deducting approximately $38.9 million of original issue discount and approximately $2.8 million of debt issuance costs, were used to repay all previous indebtedness of the Predecessor Company and to partially fund the Securus Acquisition. In the Predecessor period, a loss of $12.4 million was recorded, which consisted of the accelerated amortization of the total carrying amounts of deferred financing costs and discounts on the Predecessor Company's revolving credit facility, first lien term loans, and second lien term loans.

On May 25, 2018, the Company amended the Deutsche Bank First Lien Agreement to increase its borrowings by $75 million. This additional borrowing was primarily used to pay down approximately $73.5 million of the Company's revolving credit facility and $0.3 million of accrued interest.

The Deutsche Bank First Lien Agreement provides the Company with $1.02 billion first lien term loans, comprised of an $875.0 million first tranche (First Tranche) borrowed on November 1, 2017, a $70.0 million second tranche (Second Tranche) borrowed on December 14, 2017, a $75.0 million additional borrowing on the First Tranche on May 25, 2018, and a $150.0 million revolving credit facility, which provides for a $50.0 million sublimit for the issuance of letters of credit. The Deutsche Bank Second Lien Agreement provides the Company with $282.5 million second lien term loans.

The Deutsche Bank Agreements provide an incremental basket to incur additional secured loans, along with related debt baskets which permit the incurrence of junior and unsecured loans and the issuance of notes, in an aggregate amount which is the greater of $190M and the last 4 quarters of Consolidated EBITDA, plus an unlimited amount so long as in the case of the incurrence of additional *pari passu* loans, the Consolidated First Lien Net Leverage Ratio, determined on a Pro Forma Basis, does not exceed 4.70 to 1.00, and in the case of the incurrence of additional junior lien loans, so long as the Consolidated Senior Secured Net Leverage Ratio (as defined in the Deutsche Bank Agreements) determined on a pro forma basis is no more than 6.10:1.00 or the Fixed Charge Coverage Ratio, determined on a Pro Forma Basis, is not less than the Fixed Charge Coverage Ratio for the most recently ended quarter (less the amount of any previously issued incremental loans and notes allocated to this basket).

The first lien term loans of the Deutsche Bank First Lien Agreement bear interest at an annual rate at the Company's option equal to either: (a) the Base Rate plus the Applicable Margin of 3.5%, or (b) the LIBO Rate plus the Applicable Margin of 4.5%. Advances under the revolving credit facility bear interest at an annual rate of the Base Rate plus Applicable Margin of 2.5%, or the LIBO Rate plus Applicable Margin of 3.5%. The Base Rate is the greatest of: (a) The Federal Funds Rate, as defined in the Deutsche Bank Agreements, plus 0.50%, (b) the Prime Rate, as set by Deutsche Bank New York, in effect on such day, and (c) the LIBO Rate for an Interest Period of one month, plus 1.00%. The LIBO Rate must be at least 1.00%. The letter of credit fees of 3.50% plus a fronting fee of 0.125% per annum are payable on a quarterly basis with respect to outstanding letters of credit, and the unused amount of the revolving credit facility is subject to commitment fees of 0.375% per annum. The first lien term loans mature on November 1, 2024. The effective interest rate at December 31, 2018 was 7.6%, payable quarterly in arrears.

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

The Deutsche Bank First Lien Agreement requires amortization payments of 1.00% per annum of the initial outstanding principal amount of the first lien term loans, increased for the Second Tranche, which are due quarterly, allows for voluntary prepayments of the first lien loans at any time (subject to certain requirement and limitations for voluntary prepayments of first lien term loans), and requires mandatory prepayments of first lien term loans upon the occurrence of certain events, including certain sales of assets and receipt of certain insurance proceeds, subject to reinvestment rights, and the issuance of debt (other than debt permitted to be incurred under the credit agreement). To the extent the Company generates excess cash flow (as defined in the Deutsche Bank Agreements) in any fiscal year, starting with the fiscal year ended December 31, 2018, the Company is required to prepay principal equal to 50% of such excess cash flow less voluntary repayments of the loans (Accelerated Payment) during such fiscal year if, as of the last day of the most recently ended fiscal year, the Consolidated First Lien Net Leverage Ratio (as defined in the Deutsche Bank Agreements) is greater than 4.20:1.00. If the Consolidated First Lien Net Leverage ratio is less than or equal to 4.20:1.00 but greater than 3.70:1.00, the Company is required to prepay principal equal to 25% of such excess cash flow less voluntary repayments of the loans. No payment is required if the Consolidated First Lien Net Leverage ratio is less than or equal to 3.70:1.00.

The obligations under the Deutsche Bank First Lien Agreement are collateralized by a first lien on substantially all of the assets of Securus and its material domestic subsidiaries. The Company draws from the revolving credit facility to cover normal business cash requirements. As of December 31, 2018, the Company had $50 million outstanding on the revolving credit facility, $0.1 million of letters of credit outstanding, and $99.9 million of borrowing availability under the revolving credit facility, which includes $49.9 million of unused letter of credit availability.

The second lien term loans under the Deutsche Bank Second Lien Agreement bear interest at an annual rate at the Company's option equal to either: (a) the Base Rate plus the Applicable Margin of 7.25%, or (b) the LIBO Rate plus the Applicable Margin of 8.25%. The Base Rate is the greatest of: (a) The Federal Funds Rate, as defined in the Agreements, plus 0.50%, (b) the Prime Rate, as set by Deutsche Bank New York, in effect on such day, and (c) the LIBO Rate for an Interest Period of one month, plus 1.00%. The LIBO Rate must be at least 1.00%. The Deutsche Bank Second Lien Agreement does not require principal amortization payments and matures on November 1, 2025. The effective interest rate at December 31, 2018 was 8.5%, payable quarterly in arrears. The Deutsche Bank Second Lien Agreement allows for voluntary prepayments of the second lien term loans, and, subject to application to the first lien loans under the Deutsche Bank First Lien Agreement, requires the same Accelerated Payment of the second lien term loans as the Deutsche Bank First Lien Agreement requires of the first lien term loans.

All of Securus' material domestic subsidiaries (collectively, the Subsidiary Guarantors) are jointly and severally liable for the secured revolving credit facility, first lien term loans and second lien term loans under the Deutsche Bank Agreements.

The Deutsche Bank Agreements contain operating covenants that limit Securus' and its restricted subsidiaries' ability to incur additional indebtedness, make certain payments including dividends to shareholders, divest company assets, make investments, acquisitions and loans, permit liens on their assets, merge, dissolve or engage in other fundamental changes, change the nature of their business and enter into transactions with affiliates, in each case, subject to customary limitations, cure rights and exceptions. In the event that Securus or any restricted subsidiary fails to comply with these covenants and restrictions, the Company may be in default, at which time payment of the long-term debt and unpaid interest may be accelerated by the Company's lenders and become immediately due and payable.

21

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

The Deutsche Bank First Lien Agreement contains a springing financial covenant for the benefit of only the lenders under the revolving credit facility, which covenant requires that the Consolidated First Lien Net Leverage Ratio cannot be greater than 7.00:1.00 only if usage of the revolver exceeds 35% of the amount of the revolving credit facility commitment (excluding letters of credit) on any quarterly test date. Based on the balance outstanding on our revolving credit facility as percentage of total borrowing availability, this covenant was not in effect at December 31, 2018.

Note 6.   Derivative Instruments

The Company used derivatives instruments primarily to manage interest rate risk exposure and to add stability to interest expense, with the primary objective being to minimize interest rate risks associated with the Company's financing activities. These agreements involved the receipt of variable rate amounts from a counterparty if interest rates rise above the strike rate of the contract in exchange for an upfront premium. Upon the effective dates of each of the Company's derivative instruments, management determined that all instruments would be a nondesignated hedge. Therefore, none would be monitored for effectiveness. Derivative financial instruments are recorded in the Consolidated Balance Sheets in intangible and other assets, net and are measured at fair value. Changes in market value of the derivative financial instruments are recorded in Interest and other expenses, net, in the Consolidated Statement of Operations.

Interest rate cap agreements: On October 5, 2018, the Company entered into two interest rate cap agreements: one with Goldman Sachs (GS) and another with Deutsche Bank (DB). Both interest rate caps involve the receipt of variable amounts from a counterparty if interest rates rise above the strike rate of the contract in exchange for an upfront premium. Each of these caps have a notional amount of $350.0 million with a cap rate of 3.5%. The Company paid a premium of $1.36 million and $1.38 million, respectively, to enter into the agreements. The fair value of the GS and DB cap agreements at December 31, 2018 were each $0.4 million, with decreases in fair value during the period ended December 31, 2018 of $1.0 million and $1.0 million, respectively. Both cap agreements terminate on September 30, 2021.

Note 7.   Income Taxes

Income tax expense (benefit) is as follows (in thousands):

| | Successor | | Predecessor |
| | | | |
	December 31, 2018	For the Period From November 1 to December 31, 2017	For the Period From January 1 to October 31, 2017
Current:			
U.S. federal	$ (679)	$ -	$ (93)
U.S. state	1,701	191	174
Foreign	36	-	34
Total current	1,058	191	115
Deferred:			
U.S. federal	(9,670)	(71,045)	(14,945)
U.S. state	(5,805)	702	320
Foreign	(555)	5	(78)
Total deferred	(16,030)	(70,338)	(14,703)
Total income tax benefit	$ (14,972)	$ (70,147)	$ (14,588)

22

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

On December 22, 2017, the U.S. Tax Cuts and Jobs Act (the "TCJA") was signed into law. This act includes, among other items, a permanent reduction to the U.S. corporate income tax rate from 35% to 21% effective January 1, 2018. In 2017, the SEC issued Staff Accounting Bulletin No. 118 which permitted the recording of provisional amounts related to the impact of the TCJA during a measurement period not to exceed one year from the enactment date of the TCJA. As a result, at December 31, 2017, the Company recognized a provisional tax benefit of $70.2 million from revaluing U.S. net deferred tax liabilities. The accounting for these items is now complete and the current period adjustments related to the provisional items were not significant.

Income taxes differ from the expected statutory income tax expense (benefit), by applying the U.S. federal income tax rate of 21% to pre-tax earnings from continuing operations due to the following (in thousands):

	Successor				Predecessor	
	December 31, 2018		For the Period From November 1 to December 31, 2017		For the Period From January 1 to October 31, 2017	
Expected statutory income tax expense (benefit)	$	(10,519)	$	(857)	$	(19,755)
Goodwill impairment		2,005		-		-
Transaction expenses		(993)		-		-
Amounts not deductible for income tax		459		190		4,834
State taxes, net of federal benefit		(2,681)		295		-
Rate change		(3,269)		(69,743)		-
Other		26		(32)		333
Total income tax benefit	$	(14,972)	$	(70,147)	$	(14,588)

The rate change for 2017 in the above table is primarily due to the provisional tax benefit of $70.2 million from revaluing deferred tax liabilities pursuant to TCJA. Also included in this line is state tax expense of $0.5 million from revaluing deferred tax liabilities due to changes in the deferred state tax rate. The rate change for 2018 is state tax benefit of $3.3 million from revaluing deferred tax liabilities due to changes in the deferred state tax rate.

23

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

The tax effects of temporary differences that give rise to significant portions of the deferred income tax assets and deferred income tax liabilities as of December 31, 2018 and 2017 were as follows (in thousands):

	2018	2017
Net current deferred income tax assets (liabilities):		
Deferred income tax assets:		
Allowance for doubtful accounts	$ 703	$ 725
Accrued expenses	2,851	1,494
Deferred revenue	7,362	5,920
Net operating loss and tax credit carryforwards	30,853	27,779
Accrued interest	14,276	-
Transaction expenses	4,888	1,143
Other	348	399
Deferred income tax assets	61,281	37,460
Deferred income tax liabilities:		
Property and equipment principally due to differences in depreciation	(26,616)	(21,301)
Intangible assets due to difference in book/tax basis	(157,545)	(155,354)
Goodwill	(6,149)	(968)
Deferred income tax liabilities	(190,310)	(177,623)
Net deferred income tax liabilities	$ (129,029)	$ (140,163)

At December 31, 2018, the Company had U.S. federal net operating loss carryforwards for tax purposes aggregating approximately $133.5 million, $122.2 million of which, if not utilized to reduce taxable income in future periods, will expire from 2018 through 2038. The remaining $11.3 million in net operating loss carryforwards have an indefinite carryforward period; however, these can only reduce taxable income in a future period by a maximum of 80%. Approximately $122.2 million of these net operating loss carryforwards are subject to certain rules under Internal Revenue Code (IRC) Section 382. The Company believes these IRC Section 382 limitations will not ultimately affect its ability to use substantially all of the net operating loss carryforwards for income tax purposes, with the exception of $7.7 million that remain limited until expiration and are not included in the deferred tax asset as a result of the limitation. The federal net operating loss carryforwards in the income tax returns filed included unrecognized tax benefits taken in prior years. The net operating losses for which a deferred tax asset is recognized for financial statement purposes are presented net of these unrecognized tax benefits. The Company had approximately $56.9 million of interest expense incurred in 2018 that was not deductible for Federal income tax purposes in 2018 but can carried forward indefinitely.

The Company accounts for the uncertainty in income taxes on the determination of whether tax benefits claimed or expected to be claimed on a tax return should be recorded in the financial statements. The tax benefit from an uncertain tax position may be recognized only if it is more likely than not that the tax position will be sustained on examination by the taxing authorities. The determination is based on the technical merits of the position and presumes that each uncertain tax position will be examined by the relevant taxing authority that has full knowledge of all relevant information. As of December 31, 2018 and 2017, the Company had gross unrecognized tax benefits of $2.0 million and nil, respectively. The Company does not believe it is reasonably possible that the total amount of unrecognized tax benefits will

24

materially change in the next twelve months. The majority of the unrecognized tax benefits at December 31, 2018, if recognized, would affect the effective tax rate.

A valuation allowance is provided when it is more likely than not that some portion or the entire net deferred tax asset will not be realized. The Company calculated the deferred tax liability, deferred tax asset, and the related valuation of net deferred tax assets, including net operating loss carryforwards, for the taxable temporary differences on a jurisdiction by jurisdiction basis. The valuation allowance represents the excess deferred tax assets including the net operating loss carryforwards, over the net deferred tax liabilities, excluding deferred liabilities that are not available to offset deferred tax assets. The Company has not offset any of the net deferred tax assets, including net operating loss carryforwards, with a valuation allowance for the tax periods ended December 31, 2018 and 2017, respectively.

The Company's policy with respect to recognition of interest and penalties on uncertain tax position is to assess the likelihood, for each uncertain tax position, that any interest and penalties may be assessed by the relevant taxing authorities and, based on such assessment, record any significant interest and penalties as a component of income tax expense. In relation to the Company's unrecognized tax positions, the Company has recorded an immaterial amount of accrued interest and penalties as of December 31, 2018 and 2017, respectively.

Securus or one of its subsidiaries files income tax returns in the U.S. federal jurisdiction, Canada and various states. As of December 31, 2018, the Company has filed domestic income tax returns as part of a consolidated group at the SCRS Holding Corporation level and has open tax years for the U.S. federal return from 2002 forward with respect to its net operating loss carryforwards, where the IRS may not raise tax for these years, but can reduce net operating loss carryforwards. Otherwise, with few exceptions, the Company is no longer subject to federal, state, or local income tax examinations for years prior to 2014.

Note 8. Member's Equity

Prior to December 31, 2017, Securus' capital structure was comprised of 1,000 authorized shares of capital stock with a par value of $0.01, all of which were issued and held by Securus Holdings, Inc. On December 31, 2017, Securus was converted into a limited liability company with Securus Holdings, LLC retaining 100% of the membership interests of Securus.

Equity-based compensation: During the Predecessor period, Predecessor Company executives and certain key management personnel were awarded equity-based awards pursuant to the Predecessor Plan, which was designed to serve as an incentive to attract and retain qualified and competent employees. Under the Predecessor Plan, 55.9 million Series B Units in Securus Investment Holdings, LLC (the Incentive Units) were set aside to be granted to participants under individual Incentive Unit Agreements. The Incentive Units vested at 20% annually over a 5 year period and were subject to forfeiture pursuant to the terms of the Incentive Unit Agreements. All Incentive Units were to vest immediately upon a change in control. On November 1, 2017, upon change of control arising from the Securus Acquisition, all remaining unvested Incentive Units vested at 100% and the Predecessor Plan was terminated.

Note 9. Related Party Transactions

Effective November 1, 2017, SCRS entered into a Corporate Advisory Services Agreement with Platinum Equity Advisors, LLC (Platinum), an affiliate of SCRS, pursuant to which the Company is provided advisory services for an annual fee of up to $10 million, plus expenses incurred by Platinum in rendering such services. During the periods ended December 31, 2018 and 2017, the Company incurred fees and expenses of $10.3 million and $5.0 million, respectively, under the agreement, together with an additional

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

$1 million fee in 2018 for services related to the GovPay acquisition, all charged to Selling general and administrative expenses.

Note 10.   Commitments and Contingencies

Leases: The Company leases office space and certain office equipment under operating lease agreements. Most of the Company's lease terms have escalation clauses and renewal options, typically equal to the lease term. The Company accounts for escalating rents on a straight-line basis over the life of the lease. Rent expense under operating lease agreements for each of the periods ended December 31, 2018, December 31, 2017, and October 31, 2017, was approximately $12.3 million, $2.0 million, and $8.8 million, respectively.

In February 2017, the Company vacated one of its office locations, for which it recorded a cease-use reserve of $0.2 million and $0.4 million at December 31, 2018 and December 31, 2017, respectively, and began subletting it to another tenant. Rental income earned from the sublet for each of the periods ended December 31, 2018, December 31, 2017 and October 31, 2017 was $1.0 million, $0.2 million and $0.3 million, respectively. Total minimum rental payments to be received over the remainder of the sublease term is approximately $0.8 million.

The Company has also entered into various agreements to rent telecommunications and office equipment and computer software, which are accounted for as capital leases. The current and non-current portions of these capital lease obligations are included in Accrued liabilities and in Other long-term liabilities on the Consolidated Balance Sheet, respectively. Of total future payments for capital lease agreements in effect at December 31, 2018, December 31, 2017, and October 31, 2017, $0.1 million, $0.5 million, and $0.6 million is comprised of interest, respectively.

Future minimum payments under the Company's operating and capital lease agreements for each of the next five years through December 31, 2023 and thereafter are summarized as follows (in thousands):

	Operating Leases		Capital Leases	
2019	$	10,901	$	2,976
2020		9,760		668
2021		8,879		3
2022		6,619		-
2023		5,376		-
Thereafter		24,157		-
Total minimum lease payments	$	65,692	$	3,647

Minimum guaranteed payments: The Company is required to make the following minimum commission payments to certain of its correctional facility customers regardless of the level of revenues generated by the Company on those contracts, as follows (in thousands):

2019	$	41,726
2020		22,550
2021		10,980
2022		8,151
2023		2,048
Thereafter		485
Total minimum commission payments	$	85,940

26

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Contingent consideration: In relation to the Company's acquisition of JPay, Inc. (JPay) in 2015, the purchase included a contingent consideration expected to be paid annually in 2016 through 2018 based on JPay's financial performance as compared to certain metrics as set forth in the stock purchase agreement. Fair value was estimated using the Monte Carlo method as of the acquisition date, and was adjusted under such method each year. The final payment was made by the Company in 2018. At December 31, 2017, the fair value of the contingent consideration equaled approximately $36.5 million.

During the period ended October 31, 2017, a $24.7 million increase in fair value was recorded as Transaction expenses in the Company's Consolidated Statement of Operations, and the Predecessor Company paid $22.6 million in cash. During the period ended December 31, 2017, no change in fair value was recorded, and the Successor Company paid $4.5 million in cash as a prepayment of the contingent consideration earned in 2017. The final payment of $20.5 million, comprised of $25 million owed by the Successor Company less the $4.5 million paid during the period ended December 31, 2017, was made in May 2018, of which $14.9 million and $5.6 million is recorded in the operating section and the financing section of the Consolidated Statement of Cash Flows, respectively. The remainder of the 2018 payment of contingent consideration earned in 2017 was paid by the owners of the Predecessor Company.

Employment agreements: As of December 31, 2018 and December 31, 2017, the Company had employment agreements with certain key management personnel, which provided for minimum compensation levels and incentive bonuses along with provisions for termination of benefits in certain circumstances and for certain severance payments in the event of a change in control (as defined). In addition, executives of the Predecessor Company participated in the Predecessor Plan (see Note 8).

Incentive Compensation Plan: Effective April 30, 2018, Company executives and certain key management employees began participating in a long-term incentive compensation plan as provided for in the SCRS Holding Corporation 2018 Participation Plan (the Plan). The Company's Compensation Committee (the Committee) administers the Plan, which is designed to serve as an incentive to attract and retain qualified and competent employees. Performance units, which are granted to employees under individual grant agreements, generally mature over a 4.5 year period with all granted units fully maturing upon a change of control or initial public offering (IPO). The maximum number of units that may be awarded under the Plan is 30.0 million units. Upon the occurrence of a Qualifying Event, as defined in the Plan, participants may be entitled to receive a cash payment (or stock in the event of an IPO) for their share of the value of the Qualifying Event. The Plan expires and terminates at the earlier of either a change of control or on April 30, 2026. No Qualifying Events occurred and, therefore, no compensation costs were recorded under the Plan during the year ended December 31, 2018.

Litigation and regulatory matters: The Company has been, and expects to continue to be, subject to various legal and administrative proceedings or various claims in the normal course of business. We believe the ultimate disposition of these matters will not have a material effect on our financial condition, liquidity, or results of operations.

27

Securus Technologies Holdings, LLC
(formerly Securus Technologies Holdings, Inc.)

Notes to Consolidated Financial Statements

Note 11.   Subsequent Event

On April 22, 2018, Securus Technologies, Inc. (Securus Technologies), a wholly owned subsidiary of Securus, entered into a unit purchase agreement pursuant to which it intended to acquire 100% of the issued and outstanding membership interests of Inmate Calling Solutions, LLC (ICS). However, on April 2, 2019, Securus Technologies voluntarily withdrew its application to the Federal Communications Commission (FCC) for approval of the purchase after Securus Technologies and ICS were informed by the FCC that it would be unable to support this merger based on competitive concerns. As a result, Securus Technologies and ICS terminated the unit purchase agreement, and all incremental borrowing arrangements to fund the transaction were terminated.

Management evaluated the disclosure of any material subsequent events through April 11, 2019, which was the date the financial statements were issued. As of April 11, 2019, there were no other subsequent events that required recognition or disclosure.

28

B: DUN & BRADSTREET REPORT

dun & bradstreet

SECURUS TECHNOLOGIES, INC.   DUNS: 19-285-8954

Business Information Report

Company Information	

4000 International Pkwy Ste 3000
Carrollton, TX 75007

This is a **headquarters subsidiary** location.

Website	www.securus.net	**Financial Statement**	
Telephone	(972) 241-1535	Sales	NA
Chief Executive:	THE OFFICER(S)	Net Worth	NA
Stock Symbol:	NA	History:	NA
Year Started	2004	Financial Condition:	NA
Employees	787	Financing:	SECURED
		SIC:	4813
		Line of Business:	Telephone communications

Corporate Family:

This business is a headquarters subsidiary of the corporate family.

Scores

PAYDEX ®	

78 ▲

3 days beyond terms

78

| 1   100 |

120 Days Slow   30 Days Slow   Prompt

Based on up to 24 months of trade.
D&B PAYDEX® Key

■ High risk of late payment
(average 30 to 120 days beyond terms)

■ Medium risk of late payment
(average 30 days or less beyond terms)

■ Low risk of late payment
(average prompt to 30+ days sooner)

Credit Limit Recommendation	

Risk Category
Low

Conservative Credit Limit
$1,000k

Aggressive Credit Limit
$1,000k

High   Moderate   Low

D&B Rating ®

Rating

--

The credit rating was assigned based on D&B's assessment of the company's financial ratios and its cash flow. For more information, see the D&B Rating Key.

Below is an overview of the company's rating history since 11/22/2011

D&B Rating	Date Applied
--	2015-11-02
1R3	2015-09-17
--	2015-02-19
1R3	2013-02-14
--	2011-11-22

The Summary Analysis section reflects information in D&B's file as of May 10, 2019

D&B Viability Rating

3	Viability Score	

9 High Risk   5   1 Low Risk

Compared to ALL US Businesses within the D&B Database:

- Level of Risk: **Low Risk**
- Businesses ranked 3 have a probability of becoming no longer viable: **3%**
- Percentage of businesses ranked 3: **15%**
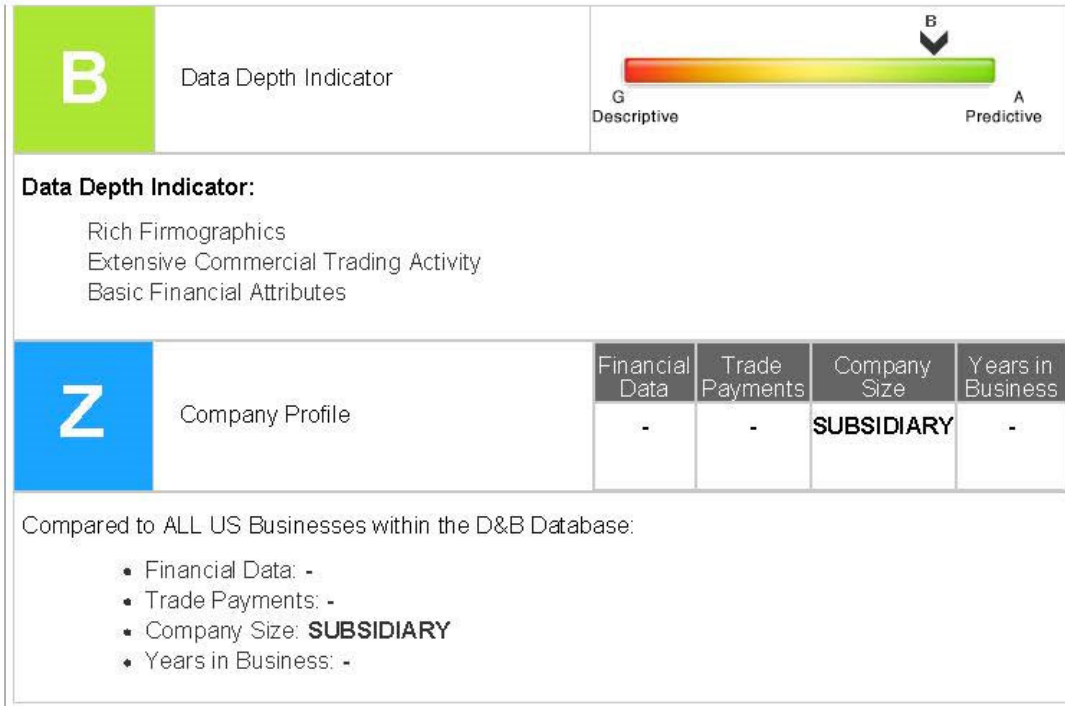- Across all US businesses, the average probability of becoming no longer viable: **14%**

2	Portfolio Comparison	

9 High Risk   5   1 Low Risk
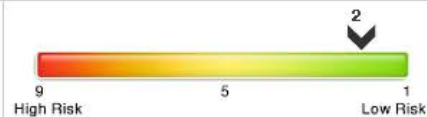
Compared to ALL US Businesses within the D&B Database:

- Model Segment: **Established Trade Payments**
- Level of Risk: **Low Risk**
- Businesses ranked 2 within this model segment have a probability of becoming no longer viable: **3%**
- Percentage of businesses ranked2 within this model segment: **16%**
- Within this model segment, the average probability of becoming no longer viable: **5%**

B	Data Depth Indicator	

Data Depth Indicator:

Rich Firmographics
Extensive Commercial Trading Activity
Basic Financial Attributes

Z	Company Profile	Financial Data	Trade Payments	Company Size	Years in Business
		-	-	**SUBSIDIARY**	-

Compared to ALL US Businesses within the D&B Database:

- Financial Data: -
- Trade Payments: -
- Company Size: **SUBSIDIARY**
- Years in Business: -

History & Operations

History

The following information was reported: **01/19/2018**

Officer(s):
ROBERT E. PICKENS, CEO
RICHARD A SMITH, SR ADVISOR BOARD OF DIR
WILLIAM D MARKERT, CFO
ARLIN B GOLDBERG, CIO
DENNIS REINHOLD, V PRES-GENERAL COUNSEL-SEC

The Delaware Secretary of State's business registrations file showed that Securus Technologies, Inc. was registered as a Corporation on January 12, 2004, under file registration number 3750176.
Business started 2004. Present control succeeded Nov 2011.

CONTROL CHANGE:
On September 17, 2015, sources stated that Abry Partners, Inc., Boston, MA, has acquired 66.9% in Securus Holdings, Inc., Dallas, TX, on June 2013. With the acquisition, Securus Holdings, Inc. will now operate as a subsidiary of Abry Partners, Inc. Securus Holdings, Inc. is the parent company of Securus Technologies, Inc., Dallas, TX. Terms were undisclosed.
On November 21, 2011, sources stated that Castle Harlan Inc., New York, NY, has completed the acquisition of Securus Technologies Inc., Dallas, TX, on November 10, 2011. With this acquisition, Securus Technologies Inc., will operate as an affiliate of Castle Harlan Inc. Terms of the transaction were not disclosed. Further details are not available at this time.

RECENT EVENTS:
On January 18, 2018, sources stated that Securus Technologies, Inc., Carrollton, TX, has acquired Government Payment Service, Inc., d/b/a GovPayNet, Indianapolis, IN, on January 4, 2018. With the acquisition, Government Payment Service, Inc. will now operate as a subsidiary of Securus Technologies, Inc. Employees and management were retained. Terms of the deal were not disclosed. Further details are unavailable.
On December 6, 2017, Robert Bro, President stated that Securus Technologies, Inc., Carrollton, TX, has completed the acquisition of Jobview, LLC, Burnsville, MN, on December 1, 2017. With the acquisition, Jobview, LLC will now operating as a wholly-owned subsidiary of Securus Technologies, Inc. Employees and management were retained. Terms of transactions were not disclosed.
On August 6, 2015, sources stated that Securus Technologies Inc., Dallas, TX, has completed the acquisition of Jpay Inc., Miramar, FL, on July 31, 2015. With the acquisition, Jpay Inc. will now operate as a wholly owned subsidiary of Securus Technologies Inc. Employees and management were retained. Terms of the transaction were not disclosed. Further details are unavailable.
On May 29, 2015, sources stated that Securus Technologies Inc., Dallas, TX, has announced on May 14, 2015, the opening of its industry leading Technology Center near its headquarters in Dallas, Texas. Further details are unavailable.
On February 4, 2015, sources stated that Securus Technologies Inc., Dallas, TX, through its newly formed subsidiary, CellBlox Acquisition, LLC, a Delaware company, has acquired substantially all of the assets of CellBlox, Inc., Huntsville, AL, on January 14, 2015. With the acquisition, CellBlox, Inc. has ceased to exist, and operations have moved to Securus' headquarters.

On August 22, 2014, sources stated that Securus Technologies, Inc., Dallas, TX, has acquired the Alternative Monitoring Services division of General Security Services Corporation, Minneapolis, MN, on August 4, 2014. The Alternative Monitoring Services division will now be part of Satellite Tracking of People LLC, Houston, TX, a subsidiary of Securus Technologies, Inc. Terms were undisclosed.

On July 2, 2014, sources stated that Securus Technologies Inc., Dallas, TX, has acquired JLG Technologies LLC, Framingham, MA, on June 11, 2014. With this acquisition, JLG Technologies LLC will now operate as a subsidiary of Securus Technologies Inc. Terms of the deal were not disclosed. Further details are unavailable.

On March 13, 2014, sources stated that Securus Technologies Inc., Dallas, TX, has completed the acquisition of Telerus, Inc., Denver, CO, on March 3, 2014. With the acquisition, Telerus, Inc. will now operate as a subsidiary of Securus Technologies, Inc. Terms were undisclosed. Further details are unavailable.

On January 9, 2014, sources stated that Securus Technologies Inc., Dallas, TX, has acquired Satellite Tracking Of People LLC, Houston, TX, on December 20, 2013. With this acquisition, Satellite Tracking Of People LLC will now operate as a subsidiary of Securus Technologies Inc. Terms of the deal were not disclosed. Further details are unavailable.

On November 26, 2013, Denise Straub, Operations Manager, stated that Securus Technologies Inc., Dallas, TX, has completed the acquisition of Archonix Systems LLC, Marlton, NJ, on November 12, 2013. With the acquisition, Archonix Systems LLC will now operate as a wholly owned subsidiary of Securus Technologies Inc. Financial terms were not disclosed. Further details are unavailable.

On July 17, 2012, sources stated that Securus Technologies Inc., Dallas, TX, an affiliate of Castle Harlan Inc., New York, NY, has acquired Direct Hit Systems Inc., Melbourne, FL, on July 3, 2012. With the acquisition, Direct Hit Systems Inc. will now be a wholly owned subsidiary of Securus Technologies Inc. Further details are unavailable.

On March 23, 2012, sources stated that Securus Technologies Inc., Dallas, TX, announced the acquisition of Primonics Inc., Montreal, Canada, on March 19, 2012. Further details are unavailable.

On July 6, 2007, an inside source at the company stated that Securus acquired Syscon Holding Ltd, Richmond, British Columbia, Canada.

RECENT EVENT:
On November 18, 2015, sources stated that Securus Technologies, Inc., Dallas, TX, has completed the acquisition of Guarded Exchange, L.L.C., Jefferson City, MO, on October 30, 2015. With the acquisition, Guarded Exchange, L.L.C. will now operate as a subsidiary of Securus Technologies, Inc. Employees and management were retained. Terms of the transaction were not disclosed.

On August 14, 2015, sources stated that Securus Technologies, Inc., Dallas, TX, has acquired Cara Clinicals Inc., Saint Paul, MN on July 31, 2015. With the acquisition, Cara Clinicals Inc. will now operate as a subsidiary of Securus Technologies, Inc. Employees and the management were retained. Terms are undetermined. Further details are unavailable.

ROBERT E PICKENS. He has served as the company's CMO since September 2008. He has over 18 years of Senior level telecommunications experience. Before joining the company, he was COO of Eschelon Telecom. He has a Bachelor of Science in Business degree in Marketing and Management from the University of Minnesota Carlson School Of Management.

RICHARD A SMITH. He has served as the company's President and CEO since June 2008. He served as the CEO of Eschelon Telecom Inc., a publicly traded local exchange carrier, from August 2003 through August 2007. He holds an Associate Degree of Applied Science in Electrical Engineering from the Rochester Institute of Technology, a Bachelor of Science in Electrical Engineering from the state University of New York at Buffalo, a Masters in Mathematics from the state University of New York at Brockport, and a Masters in Business Administration from the University of Rochesters Simon School.

WILLIAM D MARKERT. He has served as the company's CFO since June 2008. From December 1999 to November 2007, he held Executive level finance positions at Eschelon Telecom, Inc., with his most recent position being Executive Vice President of Network Finance. He holds a Baccalaureate in Business Administration from the University of Wisconsin-Whitewater and a Masters in Business Administration from the University of St. Thomas in St. Paul, Minnesota.

ARLIN B GOLDBERG. He has served as the company's CIO since September 2008. He has over 30 years of telecommunication industry experience. Previously, he served as the Executive Vice President of Information Technology for Eschelon Telecom from October 1996 until July 2007. He received his Bachelor of Science in Business degree in Accounting from the University of Minnesota Carlson School of Management.

DENNIS REINHOLD. He has served as the company's Vice President, General Counsel and Secretary since he joined in August 2005. Prior to joining the company in August 2005, he served as the Associate General Counsel of SOURCECORP, Inc. (NASDAQ: SRCP), a public company with approximately 7,000 employees worldwide that specialized in business process outsourcing of critical data and documents. He has a J.D. from St. Louis University, a B.S. in Marketing and Business Administration from the University of Illinois and he completed the Advanced Management Program at The Wharton School, University of Pennsylvania.

AFFILIATES:

AFFILIATES:

MERGER/ACQUISITION:
Business address has changed from 14651 Dallas Pkwy Ste 600, Dallas, TX, 75254 to 4000 International Pkwy Ste 3000, Carrollton, TX, 75007.

Operations

01/19/2018

Description:
Subsidiary of SECURUS HOLDINGS, INC., DALLAS, TX started 2010 which operates as a holding company.

As noted, this company is a subsidiary of Securus Holdings, Inc., DUNS number 966860665, and reference is made to that report for background information on the parent company and its management.

Provides telephone communications.

Terms are Net 30 days. Sells to general public and goverment agencies. Territory : International.

Nonseasonal.

Employees: 787 which includes officer(s). 360 employed here.

Facilities: Leases premises in building.

Subsidiaries: This business has multiple subsidiaries, detailed subsidiary information is available in D&B's linkage or family tree products.

SIC & NAICS

SIC:
Based on information in our file, D&B has assigned this company an extended 8-digit SIC. D&B's use of 8-digit SICs enables us to be more specific to a company's operations that if we use the standard 4-digit code.The 4-digit SIC numbers link to the description on the Occupational Safety & Health Administration (OSHA) Web site. Links open in a new browser window.

4813 0000 Telephone communication, except radio

NAICS:
517911 Telecommunications Resellers

Payments

PAYDEX® ®

The D&B PAYDEX® is a unique, dollar weighted indicator of payment performance based on up to 114 payment experiences as reported to D&B by trade references.

3 Month PAYDEX®	24 Month PAYDEX®
77 ▲	78 ▲
When weighted by dollar amount, payments to suppliers average 5 days beyond terms terms.	When weighted by dollar amount, payments to suppliers average 3 days beyond terms terms.
Based on payments collected over the last 3 months	Based on payments collected over the last 24 months
	When dollar amounts are not considered, then approximately 88 of the company's payments are within terms.

🟥 **High risk of late payment (average 30 to 120 days beyond terms)**

🟨 **Medium risk of late payment (average 30 days or less beyond terms)**

🟩 **Low risk of late payment (average prompt to 30+ days sooner)**

Payments Summary

Total (Last 24 Months): 114

C: THREADS FREQUENTLY USED FEATURES

- **creation of a centralized database which shall contain all data elements necessary for provision of monitoring services, reporting and historical call transaction information;**

Frequently Used THREADS Features

Workspaces

Within THREADS, Securus provides online workspaces where investigative cases can be built. These workspaces allow users to compile data and build an investigation. Pictures, locations, devices, organizations, and known associates can be inserted and attached within the workspaces to organize in-progress investigations while investigators add additional data points. Investigators can update the permissions for each workspace to allow only the active investigator, only Dallas County facilities, or your full shared community to have access to individual workspaces. Through these settings, users filter editing privileges for those assigned with viewing access.

THREADS Workspace
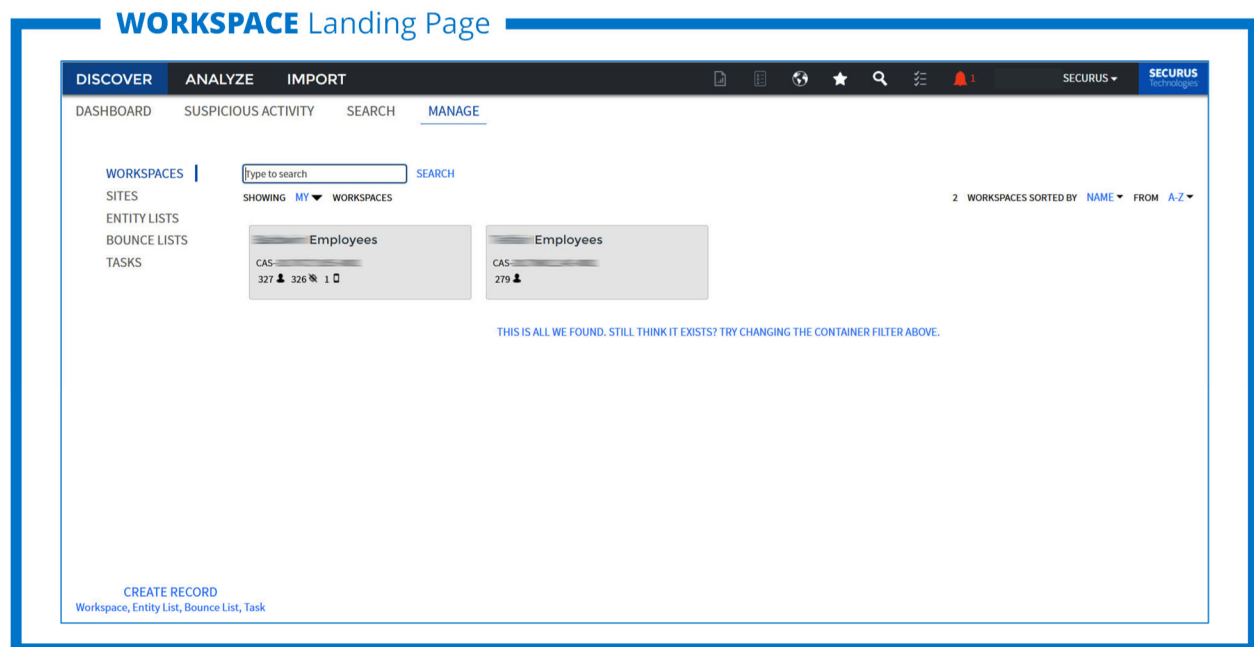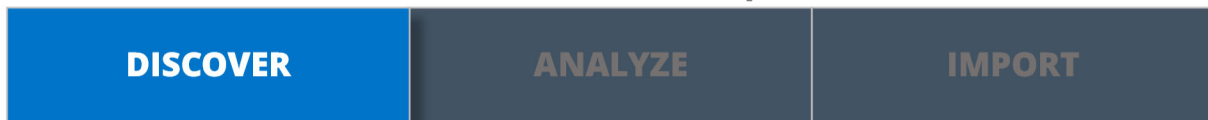
Graphic and Textual Information

All information is presented graphically as well as textually. Timeline charts and graphical analysis make it easy to reveal periods of high-intensity calling and other calling patterns on a graphical and interactive timeline.

Textual and Graphical Data Presentations

Inmate Identification and Automatic Notifications

This technology identifies the inmate—even if the calls are masked by another inmate's PIN—and **eliminates human intervention by receiving actionable intelligence at the push of a button**. THREADS also provides **automated notifications** that can alert an investigator when information is found.

THREADS Reports

Reports are accessed on the Analyze page as shown below:

(1) DISCOVER | **ANALYZE** | IMPORT

(2) HOME

THREADS provides the following types of reports:

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

These report types are described in the following pages.
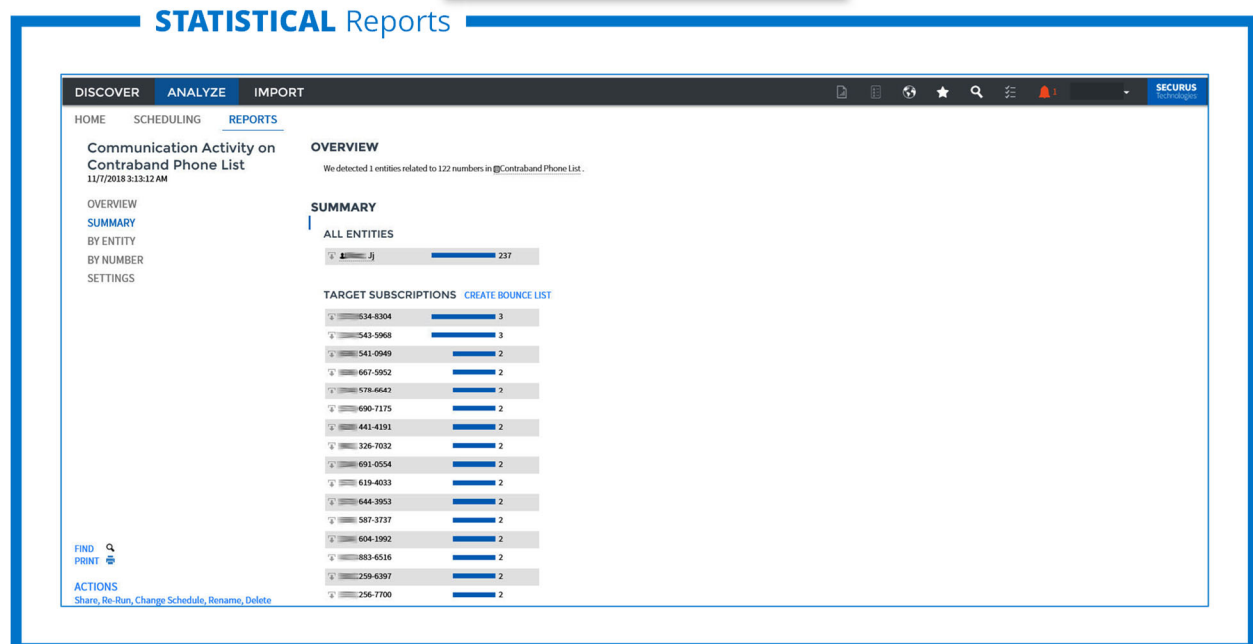
Statistical Reports

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 inmate or person.

Investigators can:

- 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 inmate as a potential owner of a device.
- Identify the phone numbers that an inmate or person calls with the highest frequency.
- Identify all phone numbers associated with an inmate 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 two or more targets or groups of targets. This report produces a CSV file for download.

Sample Statisical Reports

Linkage Reports

Linkage analysis shows how inmates 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 inmates are talking to and how the calls are related to other known numbers or inmates.

Users can generate a linkage chart that identifies the following information based on user-selected connection types, such as calls, financials, visitation, etc:

- A target(s) relationships
- Connections between two selected targets or two sets of targets
- Connections between two or more targets

In addition, users can generate a linkage chart that identifies direct relationships between selected targets based solely on phone calls.


Sample Linkage Analysis
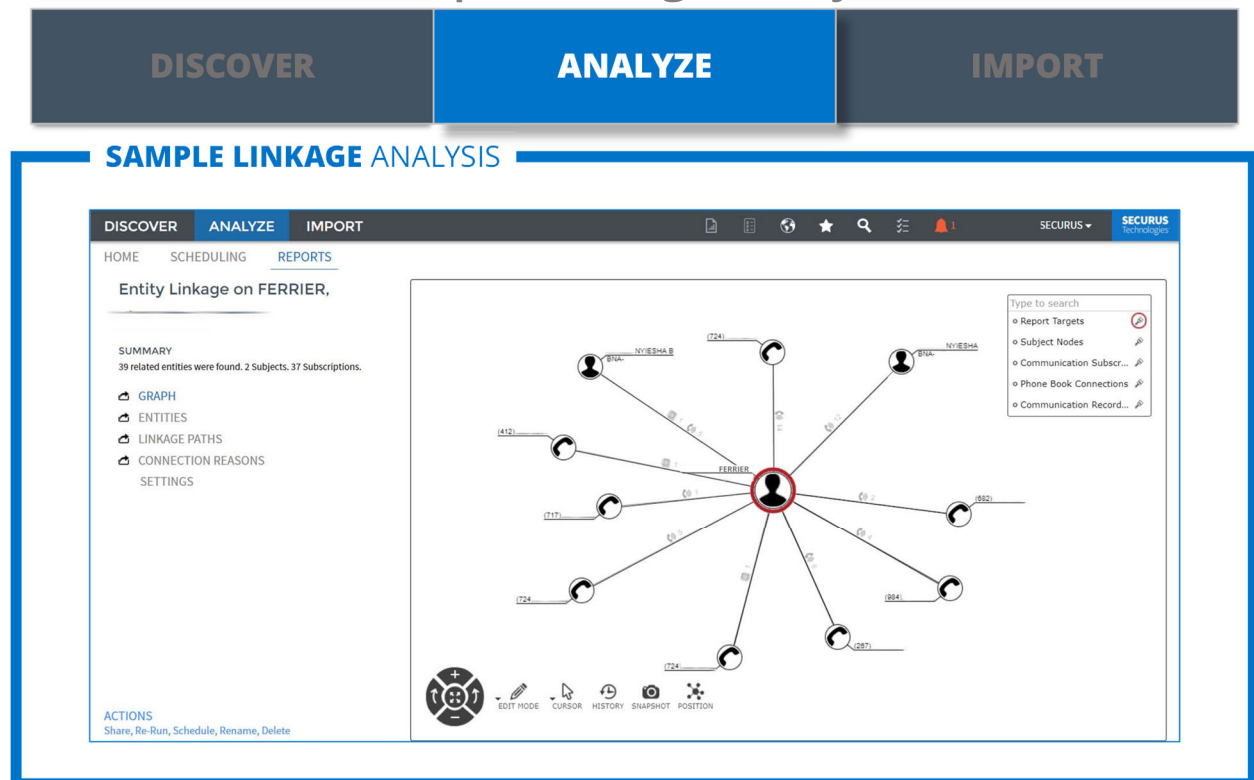
Working Group / Inner Circle Reports

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 links 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. Knowledge of organized groups and gangs can aid staff in monitoring member activity or take preventive measures against illicit activities.

Investigators can:

- 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.

Sample Inner Circle Report
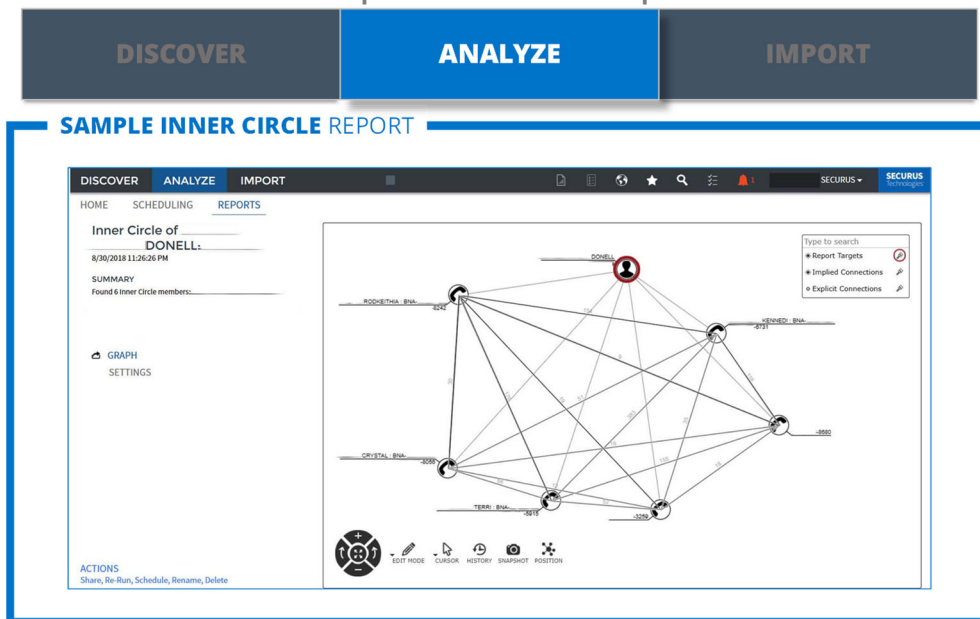
Correlation Reports

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

Investigators can:

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

Sample Workplace Correlation Report

Time-Based / Hole Detection Reports

Time-based analysis provides reports based on the timing and frequency of an inmate's or other person's communications. The investigator can 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.

Investigators can:

- Identify holes or gaps in an inmate's or person's communication activity.

- Display a set of phone numbers that a person called where communications stop with one phone number and communications start 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.

Sample Hole Detection Report

Financial Reports

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

Investigators can:

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

Sample Financial Report

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.

D: SECUREVIEW TABLET PROGRAM

- **any value-added service features not specifically outlined within:**

Securus Inmate Tablet Program: SecureView

The SecureView Tablet Program is the industry's only comprehensive design built on 6 fundamental beliefs:

- **Tablets should be affordable**: Securus provides free applications and content that is available to all inmates through the Community Tablets. Inmates subscribing for the low $5 one-day fee will have unlimited access to their purchased media for the next 29 (or 30) days.

- **Tablets should be used**: The SecureView Tablet Program offers applications and content that is beneficial and accessible to all inmates. These applications provide inmate betterment, keep inmates occupied and streamline facility processes.

- **Tablets should be easy to administer**: The SecureView Tablet Program was designed with ease of use in mind, while still allowing staff to maintain complete control over tablets in the hands of inmates. The Officer Tablet puts tools like Availability Restrictions and Behavior Modification directly in the hands of staff.

- **Tablets should be educational**: Securus makes several educational applications and programs available for inmates through the SecureView Tablet. By offering a vast range of educational opportunities through tablets, the SecureView Tablet meets the needs of inmates.

- **Tablets should offer inexpensive purchases**: The SecureView Media Store offers inexpensive premium content delivering inmates with a large variety of affordable entertainment options through their tablet.

- **Tablets should not be one-size-fits-all**: Securus developed the SecureView Tablet Program to be flexible to meet the needs of multiple agencies.

Our solution is "turnkey," requiring minimal facility administration and will allow for the expansion and customization of content and capabilities without risking security. Best of all, the SecureView tablet offers full control by your approved staff over what each tablet may access using the SecureView Command & Control Officer tablet.

The SecureView tablets are provided to the facility with each of the applications already on the tablet and ready for use.

On the Community Tablets, inmates can read books, access educational and self-improvement information and programs, play games, listen and watch pod casts, research the law library and even look for a job, all without incurring any additional costs. For a small fee, an inmate can use the "Make Mine" feature to convert the Community Tablet into a Personal Tablet, which gives the inmate access to premium content as well as the free and critical content available on all Community Tablets.

The SecureView tablet offers facilities the flexibility of a safe and secure personal device for inmates to assist in re-entry programs, job search, law library requirements, communication with family, and education. All these applications, plus books, music, religion, games, and podcasts, will promote positive inmate productivity - keeping your facility staff safer to focus on real security issues - while saving your staff time by not conducting risky, expensive inmate movement to get inmates to these costly services.

> " Before the tablets, I would walk past a unit and there would be 5-6 guys acting up; yelling, spitting, and pushing each other around.
>
> After the tablets, I walked past the same unit and it was so quiet I didn't think anyone was in there. Everyone was quietly sitting around with the tablets.
>
> They are doing very well in my facility. "
>
> *Major – Fort Bend County, TX*

One of many benefits of our SecureView Tablet program is to streamline how inmates communicate not only with friends and family but also with detention officers. Many of the inmate applications available on SecureView tablets – such as Education, Forms & Grievances, Commissary Ordering, eBooks, Law Library, Document Viewer, etc. – are capable of replacing many traditional manual paper processes. These features reduce the need to use paper to submit grievances, make requests, order commissary, or even to read such items as the inmate handbook or religious materials.

SecureView Tablets software, network, servers and content have the highest levels or security and have even been field tested by cybercrime experts to ensure your protection.

Types of Tablets

The SecureView Tablet Program is flexible and combines the accessibility of free Community Tablets with an ability to maximize premium content and usage through Personal Tablets. Securus is the only provider that offers Command & Control Officer Tablets that allow facility staff to control inmate tablets.

Our new lithium batteries ensure 65 hours of usage between charges.

Community Tablet

With a free Community Tablet, inmates have equal access to essential applications such as phone, education, mental health, commissary ordering, inmate forms and grievances and much more. Inmates simply log in and begin using the tablets at no cost. Unlimited usage of these critical applications drives operational efficiencies, safety, and user betterment. Community Tablets are wiped of all downloaded content each night.

FREE COMMUNITY TABLETS

THE PURPOSE OF FREE TABLETS

Free Community Tablets allow all inmates equal access to essential applications. Simply log in and begin using the tablets at no cost.

- Education
- Communication
- Mental Health
- Religion
- Handbooks and Videos
- Forms and Grievances
- Commissary Access

ALL *for* FREE

Assigned/Unassigned Community Tablets

Community Tablets can be assigned or unassigned:

- Unassigned Community Tablet: Any inmate can log in to an Unassigned Community Tablet. The wallpaper will be green.

- Assigned Community Tablet: Only an assigned inmate will be able to log in to an Assigned Community Tablet. The wallpaper updates to orange to indicate the tablet is assigned to a specific inmate.

Colored wallpaper is useful for easy identification.

Maintaining Tablet Inventory

Securus automatically maintains inventory levels of Community Tablets. With just in time shipping, Securus ensures there are always enough Community Tablets on site to supply inmates with equal access to critical applications and content, with no need to store a large amount of tablets. When the threshold of Community Tablets goes below a predefined amount, Securus automatically will ship additional Community Tablets to the site.

Community Tablets stored in charging location

Securus System maintains inventory levels and automatically provides tablets when you need them

Facility Powers Up Screen will display tablet's destination

Place tablet in final location
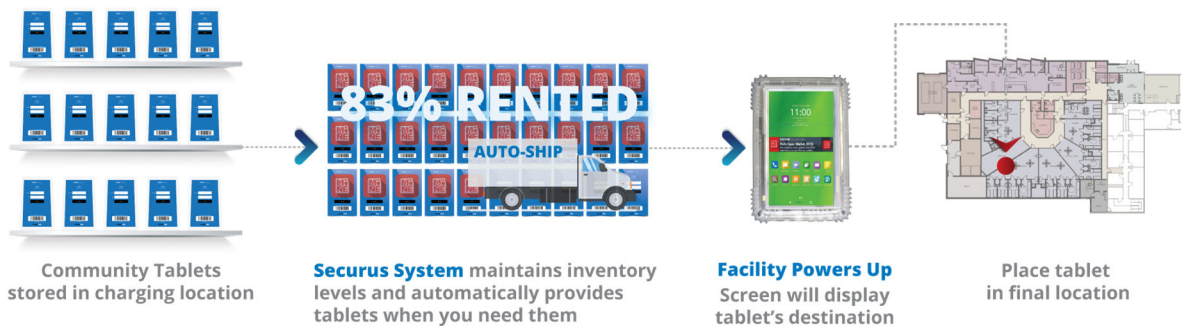
Personal Tablets

In addition to the assigned or unassigned community tablets, inmates can rent a tablet for their sole use.

Securus allows users to instantly rent their own Personal Tablets at $5 for the first day and receive an additional 29 days free.

Make Mine Feature

The "Make Mine" feature gives the Inmate the option to immediately convert a Community Tablet into a Personal Tablet. This feature will benefit the facility staff by eliminating the task of distributing tablets to inmates. This will allow an inmate to start their subscription to access premium content, either on their own or one started by the friend or family member. Once the inmate successfully completes the "Make Mine" process, all premium applications are automatically downloaded to the tablet.

MAKE MINE FEATURE

TABLET RENTAL PROCESS

Community Tablets provide all offenders with equal access to critical content

- Education
- Mental Health
- Forms & Grievances
- Calling
- eMessaging
- Religion
- Job Search
- Facility Documents & Videos

Offender purchases subscription from Inmate Debit account

Offender redeems subscription **Purchased by family & friends**

Immediately converted to Personal Tablet with access to purchase:

- Music
- Games
- Movies
- Videos
- Entertainment
- Additional Premium Content

SECUREVIEW TABLET FLOW

1 Picks up a **FREE** Community Tablet

2 All inmates have equal access to critical content

3 Inmate wants a Personal Tablet

Ability to use funds from Inmate Debit account -or- Redeems a prepaid subscription

4 Personal Tablet accesses premium content

5 Inmate is released -or- Subscription cancelled -or- Insufficient funds

6 Personal Tablet automatically reverts to FREE Community Tablet

The Make Mine process is simple:

1. Securus will deploy Free Community Tablets to meet the needs of all users throughout your agency to ensure equal access to essential applications

2. A user can easily transform a Free Community Tablet into a Personal Tablet by entering their credentials

3. Securus' Make Mine feature automatically checks the user's balance to ensure there are funds to pay for the subscription

4. All premium applications are automatically downloaded without any involvement from agency staff

When the user's subscription ends after 30 days or upon release, the Personal Tablet is automatically transformed back into a Free Community Tablet; again with no agency involvement.

PERSONAL TABLET RETURNS TO FREE COMMUNITY TABLET

FREE COMMUNITY TABLET

5

Inmate is **RELEASED**
-or-

Subscription cancelled
-or-
Insufficient funds

6

Personal Tablet
AUTOMATICALLY REVERTS
to **FREE** Community Tablet

From a Personal Tablet, users have unlimited access to FREE critical applications such as law library, job search and educational courses. Using a Personal Tablet, users may purchase and use premium media content including the latest releases in Music, Movies, and Games.

The Purpose of Personal Tablets:

- Through a low-monthly rental fee, inmate gains access to premium media that's always available without ongoing, per minute usage charges or expensive monthly subscription fees

- Reduces conflicts by not forcing inmates to share a device

- Maximizes opportunities for inmates to purchase and use premium media

- Reduces incentive for inmates to hide or dominate inmate tablets

- Maximizes amount of time an inmate can spend on a tablet

- Allows premium media to reside on the physical device; providing the best user experience

- Eliminates wait time to use premium media unlike shared only model

- Eliminates wait time for content to be downloaded to the device each time it is used

- Unlimited access to purchased and downloaded media for a one-time fee

PERSONAL TABLETS

WHY PERSONAL TABLETS?

Combines critical applications with an ability to access premium content

- Low-monthly rental fee gives access to **PREMIUM MEDIA**
- Not shared, reducing the need to hide or dominate the tablet
- **MAXIMIZES OPPORTUNITY** to use premium media with no waiting for content to download
- Purchased music and games are stored on device for **UNLIMITED OFFLINE USAGE**

TABLETS GET USED!

11:00

Personal Tablet Applications

The following list provides a summary of the applications available on the personal tablets:

- **Phone** – Allows the tablet to function as a fully integrated extension of the SCP platform. All features and restrictions of SCP will still apply.
- **Job Search** – Real-time job search database allowing inmates to perform millions of up-to-date local and nationwide job searches in numerous fields so they can make a plan for a successful re-entry into society
- **Law Library** – Provides inmates with up-to-date legal information allowing them to perform comprehensive legal research
- **Commissary** – Provide access to commissary ordering (with vendor agreement)
- **KA Lite** – Self-paced preloaded educational platform with access to thousands of videos and exercises providing the complete education experience
- **Forms and Grievance** – Fully automate the process of inmates 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)
- **eMessaging** – Two-way, corrections-grade digital messaging platform with facility regulated monitoring and control capabilities, as well as intelligence gathering opportunities
- **Podcasts** – Daily updated programming providing access to educational, mental health, self-help, addiction recovery, and more inmate betterment resources, as well as entertainment options that can keep inmates occupied for hours each day
- **Religion** – Religious books and podcasts providing sermons, teachings, and practices for wide range of faiths and beliefs
- **Books** – The largest library available - access to over 50 thousand titles
- **Mental Health & Addiction Recovery** – Dozens of resources designed to assist with anxiety relief, depression assistance, guided meditation, thriving after addiction, Alcoholics Anonymous, opiate addiction, 12 Step Programs, and much more
- **Music** – Over 15 million songs available, in multiple genres of music such as Country, Gospel, Rock, Pop, and more
- **Games** – 850+ games and growing – wide selection of titles at a low cost to inmates
- **Movies** – Non-explicit content only and many popular movies and TV shows available
- **FM Receiver** – Provides the ability to listen to facility audio broadcasts

- **Chasing the Dragon Movie** – Documentary developed as a resource to educate on the dangers of opiate addiction and how it can destroy lives
- **Clock**
- **Unlimited Possibilities**!

Upgrades and Updates

Securus is committed to making the tablet process as hassle free as possible with over the air updates. Software updates are automatic and on-going in order to ensure that the inmate maintains access to the latest and greatest content that Securus can provide.

OVER THE AIR (OTA) UPDATES

SEAMLESS AND SYSTEMATIC

- All updates are OTA, – connected to Securus Wi-Fi
- All software updates and tablet upgrades are automatic OTA
- No need to download content every session
- No staff involvement
- No shipping tablets for fulfillment and repairs

Cloud

Easy Tablet Replacement

The personal tablet replacement process is immediate, easy and hassle free. Using an authorized officer tablet, facility staff can easily approve a replacement tablet. Inmate simply picks up a community tablet, enters his or her credentials, redeems the replacement and regains access to purchased content.

If tablet needs a replacement

Officer authorizes replacement tablet

Offender chooses a new tablet

Offender logs in to tablet

Offender redeems replacement
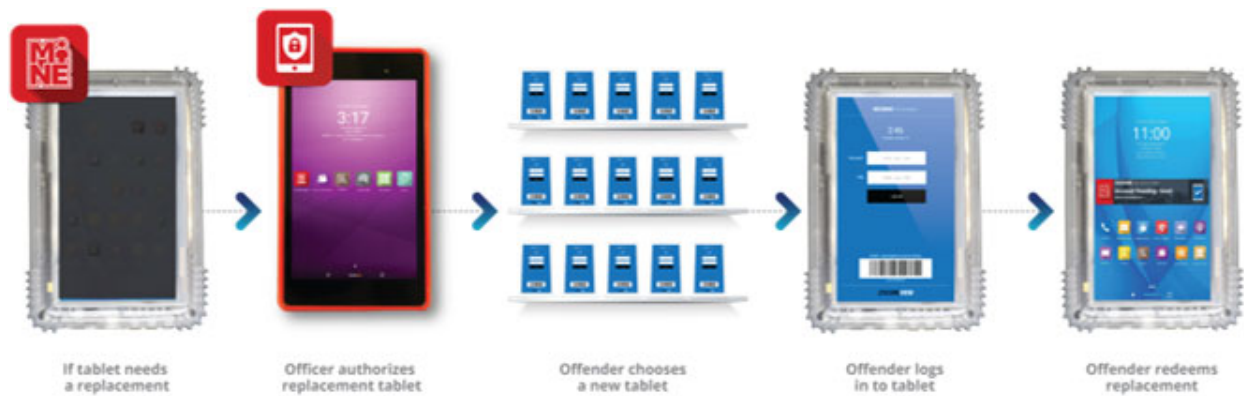
Command & Control Officer Tablets

Securus is the only provider that utilizes Officer Tablets. Securus' unmatched Command & Control officer tablets enable facility staff to easily control who gets a tablet, when the inmate can use it and what is on it.

The Officer tablets are customized Nexus 7 SecureView tablets and are provided at the POD level or as required by your facility. Officers have the ability to monitor any individual inmate activities as well as close out or activate individual applications by inmate or across multiple users. Additionally, an officer can deactivate all tablet functions by inmate, group of inmates or all inmates under his control - all in real time. Securus knew this level of control was critical for a successful tablet program.

COMMAND & CONTROL APPLICATIONS

Easy Command & Control capabilities for facility staff to regulate:
- Who gets a tablet
- What's on a tablet
- When the tablet can be used

Staff maintains complete control over:
- A single tablet
- A group of tablets
- All tablets within the facility

UNMATCHED level of Command & Control capabilities

SecureView Tablet Program Exclusive

SecureView tablet existing clients have confirmed that the ability to view activity by inmate and the ability to shut down applications and tablet access by inmate, group of inmates or the entire system has provided them with the administrative control necessary to ensure for overall safety and security. Command & Control officer tablets allow designated facility

personnel to remove any or all tablet functionality, which may be used as a means of discipline.

The Officer tablets have a detailed dashboard views that allow your staff real-time search functionality and analytics. Administrative functionality on Dashboards is comprehensive and flexible. We can provide more officer control or less officer control based on your facility's desired specifications.

The Command & Control tablet will allow your facility to control and offer required and optional services to inmates in an easy, efficient and cost effective way; all while promoting positive inmate productivity and betterment. Securus again proves its dedication to partnering with corrections to modernize incarceration and connect what matters.

Sub Manager App

The Sub Manager Application is utilized by corrections staff for the command and control of Inmate Tablets.

SubManager Application

Behavior Modification

The ability to remotely behavior modify an Inmate Tablet allows for an added level of safety and security, by removing the need for facility staff to interact physically with an inmate in order to control applications on a tablet, a group of tablets, or an entire facility of tablets.

Scheduled Behavior Modification feature allows authorized users to elect to have the request expire:

- Until manually changed by the user or someone with authorized permission
- Within "X" number of hours / days / weeks / months
- Until a selected Date / Time

Eligibility Check

Eligibility allows authorized users:

- Ability to determine if an inmate is eligible to receive a tablet
- Provides an explanation of ineligibility
- Provides the ability to place an inmate on the eligibility or ineligibility list

Availability Restrictions

The Availability Restrictions feature allow authorized users full control over when applications are available.

The ability to create application schedules to allow select applications to be active or inactive based on:

- Days of week
- Time of day
- Both days of week and time of day

Availability Restrictions may be activated for:

- Specific housing location(s) of tablets
- Entire facility of tablets

Availability Restrictions are designed to be customizable to fit the needs of your facilities scheduled events, such as Commissary distribution times, meal times, count times, etc.

Add a New Availability Restriction

View Availability Restrictions

Messages

The Messages feature provides authorized users the ability to have critical information and notifications regarding the status of all tablets.

Roles and Permissions

Roles and Permissions feature on the Command & Control Officer tablets support the ability to limit or restrict certain privileges.

Officer Tablets are configurable by facility designated Administrator(s), via the Administrator Tablet, to allow for hierarchal support structures. An 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.

Predefined Roles

Customizable Roles

Tablet Inventory

Securus automatically maintains the inventory by location. From the Inventory Page in SubManager, staff can see the number of tablets by location and tablet type.

When Community Tablet inventory goes beneath the predetermined threshold, Securus will automatically ship additional Community Tablets to the facility. The shipment date will be noted on this page.

Staff can also view the number of pending subscriptions (those that family and friends purchased) and who still needs to activate their subscription through the Make Mine application. This information is all available by location.

Pending Subscriptions

Viewer

The Viewer application allows custom PDF documents and .MP4 videos to be published to officer tablets. By publishing electronically, the Viewer app can save both time and paper costs.

An agency can load documents or videos for an officer to access via his/her tablet. Some examples may be facility policies, schedule, or the SecureView Officer Tablet User Guide.

E: ICER OVERVIEW

- **any value-added service features not specifically outlined within:**

Inmate Inter-Communication Evaluation and Reporting system (ICER™) Overview

Inmate-to-inmate communication (ITIC) 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: **inmate-to-inmate 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 inmate phone calls, we offer cutting-edge technology based on state-of-the-art, patent-pending, call-matching technology that identifies ITIC even when it's between two different correctional facilities across the country.

Although illegal ITIC 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.

Inmates are continually finding creative ways to speak to each other using the inmate phone system, and ICER listens to and identifies all of these illegal communication events. Whether two inmates 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—SCP.

The Threat

Inmates 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, ITIC was essentially undetectable due to no practical technology or uniform networking capability to identify such communications.

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

- Inmates use a variety of methods to go undetected when communicating with an inmate, whether that inmate is in a neighboring pod, a separate facility within the same state, or in a different state. Inmates 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 inmates can talk to other inmates without being detected.

- Until recently, ITIC 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, drug trafficking, racketeering, and inmate 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 inmate 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 ITIC 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 inmate 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, 2019 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	03/01/2019 07:36 pm	03/01/2019 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 inmate to inmate communication between separate facilities, which means you are no longer missing half of all of your inmate to inmate call traffic.

F: INVESTIGATOR PRO OVERVIEW

- **any value-added service features not specifically outlined within**

Investigator Pro

Investigator Pro™ (IPRO) is the most powerful voice biometrics solution in the industry. It was developed by JLG Technologies, which Securus Technologies acquired in 2014. IPRO includes a wide range of tools that identify voices by name, deter inmate PIN abuse, and provide leads for investigators pursuing illicit activity carried out over the inmate telephone system.

IPRO is a Securus solution and Securus manages the solution roadmap. The following table highlights the most popular of Investigator Pro's many features:

Integration with the Securus inmate telephone system	IPRO is fully integrated with the Securus call platform and is hosted in Securus' data centers. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.
Enrollment methods	The agency has a choice of inmate enrollment methods: supervised or covert.
	1. Supervised enrollment. Securus personnel obtain a recording of each inmate's voice after he types his ID/PIN. This provides a staff-verified voice-ID/PIN pair for each inmate. The investigator may later play an inmate's enrollment audio for his own reference.
	2. Covert enrollment. Investigator Pro creates inmate voice signatures with data from inmate calls and other sources and associates the signatures with inmate IDs/PINs. With covert enrollment inmates are less likely to know that their voices are being identified on telephone calls.
Initial voice biometrics: Pre-call PIN Check	The pre-call PIN Check feature helps prevent PIN sharing. When an inmate begins a call, it verifies in real time that the inmate's voice matches the sample associated with that inmate's ID/PIN in the system. If it does, the call goes through. If not, the call is blocked. The pre-call PIN Check feature is included with Investigator Pro but the agency chooses whether to enable it.
Continuous voice biometrics: Inmate voice identification by name	Using state-of-the-art voice biometrics technology, IPRO continuously identifies voices on inmate telephone calls. It identifies inmates by name throughout a call, no matter how many inmates are on the call or whose PIN was used to make the call.

| | It provides continuous call monitoring with no gaps. It provides 100% coverage of not only each and every call, but also 100% coverage of every second of every call for both the inmate and the called party, without gaps in the conversation and without tipping off the inmate or called party.

IPRO calculates the probability that a voice belongs to a particular inmate. That inmate may or may not be the owner of the PIN used to make the call. IPRO displays these probability numbers on relevant screens and in its call player to help investigators follow particular voices and to find imposters using other inmates' PINS to make calls. |
|---|---|
| **Continuous voice biometrics: Known called party voice identification by name** | Investigator Pro can identify called parties by name when they are known to the system, as in the case of released inmates. |
| **Voice search for inmates and called parties** | Investigator Pro provides the ability to search for all calls containing a particular voice on the inmate or called party side of calls. The investigator can do a voice search by inmate name, inmate ID, or a voice sample that he saved from a call. He can specify a date range or let the system default to the past 90 days. |
| **Identification of likely PIN abusers/imposters by name** | Investigator Pro finds and highlights calls that are likely cases of inmate PIN sharing/theft. In each of those cases the system gives the call a suspiciousness score which is a numeric indicator of the system's certainty, e.g. 95% or 80%, that there is an imposter using the PIN. IPRO names the likely imposter. |
| **Inmate-to-inmate communication: ICER integration** | Investigator Pro provides automatic detection of all inmate-to-inmate calls because ICER, the Inmate Intercommunication Evaluation and Reporting System, is integrated into Investigator Pro.

ICER detects and flags inmate-to-inmate telephone calls whether the inmates are within a facility or in different facilities across the country. It is the only system in the industry that detects these calls whether the two inmates called the same, or different, outside numbers to make the connection. |
| **Three-way call detection** | When the system suspects any three-way event(s) on a call, it flags that in the call player and in lists of calls. |

| Call player | Investigator Pro includes a feature-rich call player. Some of the most popular features are these:

• Skip pauses to save listening time.

• Mute either the inmate or called party side of the call.

• Add a note to the entire call or to a clip the investigator selects in the call, and distribute notes to colleagues.

• Slow down and speed up playback while keeping the call intelligible.

• See voice identification information about voices on the call.

• Save voices to use in voice searches of the call database.

• See information about PIN abuse, three-way activity and inmate-to-inmate communications (ICER). |
|---|---|
| Call database search | Investigators can search the call database by criteria such as inmate name, inmate ID, date range, inmate or called party voice, custom High Interest Group label, ICER event calls, three-way calls, originating station, and case number. |
| Custom high-interest group labelling | Investigators can add custom "High Interest Group" labels such as gang names, contraband risk groups and narcotics trafficking to inmates and called party numbers. Icons representing those labels then appear in call tables and IPRO's QuickFind Fast Facts whenever those inmates and telephone numbers appear. The labels can be used as search criteria in IPRO's CallFinder. |
| Custom gang data feeds | Investigator Pro can be customized by Securus to automatically import the agency's own gang data, removing the need for investigators to manually add High Interest Group labels to inmates and called numbers. |
| Management tools | Investigator Pro includes management tools such as role-based access permissions, the ability to see officers' use of individual IPRO features, the ability to create, organize, search for, and forward notes on calls/call clips, and a feature to burn calls to CD. |
| Reports | Investigator Pro can generate many reports with data useful to investigators. For example, it can report on pre-call PIN Check results, likely PIN abusers, the most common called party numbers, and IPRO voice learning results. |

G. PUBLIC PHONE RATES

7)   Must include all services offered and the applicable proposed rates. The proposer shall indicate, within their submission, if the rates being proposed are regulated and if so by what regulatory agency.

SECURUS TECHNOLOGIES, INC.
RATE SHEET

Pursuant to Texas S.B. No. 980, Section 52.007 (c), Securus Technologies, Inc. will no longer file this Price List with the Public Utilities Commission. However, as required by the rule, Securus Technologies, Inc. will update this information on its internet site so that the information is kept current.

Public Payphone Rates

<u>Local Calling Options</u>

    <u>Option 1</u>
    $0.50 for the first 15 minutes
    $0.25 for each additional 5 minutes

    <u>Option 2</u>
    $0.35 for unlimited minutes

    <u>Option 3</u>
    $0.50 for unlimited minutes

<u>Long Distance Calling Options</u>

    <u>Option 1</u>
    $0.25 per minute, with a four minute minimum

    <u>Option 2</u>
    $1.00 for the first four minutes
    $0.10 for each additional minute

    <u>Option 3</u>
    $1.25 for the first minute
    $0.10 for each additional minute

    <u>Option 4</u>
    $2.20 for the first minute
    $0.10 for each additional minute

Effective: June 20, 2016

H. ADDENDA ACKNOWLEDGEMENT

DALLAS COUNTY
PURCHASING DEPARTMENT
900 Jackson Street, Suite 680
Dallas, Texas 75202

Michael Frosch
Purchasing Director

September 4, 2019

ADDENDUM #1

Solicitation # 2019-064-6828

REQUEST FOR PROPOSAL FOR INMATE PHONE, VIDEO VISITATION SERVICE and INMATE MULTI- FUNCTION KIOSK PROVIDER

WHEREAS, a Site Visit will be conducted on September 16, 2019 @ 10:00am.

SITE **V**ISIT **L**OCATION: **F**RANK **C**ROWLEY **B**UILDING, 133 N. **R**IVERFRONT **B**LVD. **1**ST **F**LOOR ROOM **A5** NEAR THE CAFETERIA

INSTRUCTION: Please submit names an email address of members that are intending to come to site visit. (Please limit to **2** people per form). Please submit names by 9/6/19 at 10:00am to receive additional information for background in the secure facility

WHEREAS, Section IV in the proposal is hereby removed

WHEREAS, the following forms are hearby added to the proposal

- "Small Business Enterprise (SBE) Program",
- "Dallas County Subcontractor Intent form",
- "Small Business Utilization Affidavit"
- "Dallas County Good faith Effort Form"

Except as provided herein/above, all other specification requirements of the original solicitation referenced shall remain unchanged in full force and effect. This addendum should be signed and returned with your Solicitation package on or before October 14, 2019, @ 2:00 P.M. (CDT).

Rev. 1
03.11.19
Addendum

This addendum is hereby acknowledged, understood and considered in our Solicitation.

Printed Name: Robert E. Pickens

Signature of Authorized Representative: _____

Title: Chief Executive Officer

Company: Securus Technologies, Inc.

DALLAS COUNTY
PURCHASING DEPARTMENT
900 Jackson Street * 6th Floor * Suite 680
Dallas, Texas 75202
Michael Frosch
Purchasing Director

September 17, 2019

ADDENDUM No. 2

RFP No. 2019-064-6828

Request for Proposal
Inmate Phone, Video Visitation Service and Inmate Multi-Function Kiosk Provider

Whereas, the Purchasing Point of Contact is hereby:

Abri-Gayle Sterlacci-
Email: abri-gayle.sterlacci@dallascounty.org
Phone: 214-653-7763

Whereas, all forms and language referring to Small Business Enterprise (SBE) program is hereby replaced with the Attachment.

Except as provided herein/above, all other specification requirements of the original solicitation referenced shall remain unchanged and in full force and effect. This addendum should be signed and returned with your RFP proposal response on or before **OCTOBER 14, 2019@ 2:00 P.M, Local Time (Dallas, Texas) Central Time Zone.**

This addendum is hereby acknowledged, understood and considered in our proposal.

Printed Name: Robert E. Pickens

Signature of Authorized Representative: RA Licc

Title: Chief Executive Officer

Company: Securus Technologies, Inc.

DALLAS COUNTY
PURCHASING DEPARTMENT
900 Jackson Street * 6th Floor * Suite 680
Dallas, Texas 75202
Michael Frosch
Purchasing Director

October 4, 2019

ADDENDUM No. 3

RFP No. 2019-064-6828

Request for Proposal
Inmate Phone, Video Visitation Service and Inmate Multi-Function Kiosk Provider

This addendum extends the due date for proposal, answers all questions received to the best of Dallas County's knowledge and ability. This addendum also identifies changes in equipment and evaluation criteria. Attached is a revised RFP document addressing all changes.

Whereas, the due date for receipt of proposals has been extended to the following date:
October 21, 2019 @ 2:00PM
*All clarification requests must be submitted no later than close of business on October 09, 2019. Responses will be provided by the County no later than close of business on October 11, 2019.

Whereas, all language concerning SBE criteria for this solicitation has been removed in its entirety. Evaluation points previously associated with SBE have been reallocated to the Cost criteria. However Dallas County still anticipates the use of SBE contractors on any subcontracting opportunities.

Whereas, the following equipment will be required for Cook Chill Location:
Four (4) phones

Questions and Answers:

1. Page 21, Section D, 8., a., "If any payment service fees exceed the current Dallas County fee of $5.95, the bidder is required to provide a copy of the providers contract with the third-party payment service provider, signed by the owner, chief financial officer or president, explaining why the listed fee is not acceptable for this service contract." Could you please clarify what payment service fees you are referring to?

   Response: ANY and ALL fees charged to clients (whether by IPS vendor, financial vendor or payment processing center for the receipt, processing or holding payments) relating to the payment for minutes/use of inmate phone/video/kiosk/applications. Fees charge by 3rd party to receive monies related to inmate phone/video/kiosk/applications

2. Page 21, Section D, 9: "Unclaimed Funds". Can the County provide an example of the "Certification of Compliance with the state treasurers unclaimed assets programs?"

   Response: This is the first time this request has been made as related to Inmate phones/video/kiosk funds. Dallas County is looking for your companies practice for returning unused funds to the client/friends/family and evidence of compliance in reporting "Unclaimed funds" to the Texas State Comptroller.

3. On Page 24, Section D, "The County reserves the right to select multiple vendors to facilitate the aforementioned agreement." Is it permissible to partner with another vendor if that vendor has not attended the mandatory pre-bid meeting and/or site visit?

   Response: The County will allow for vendors who were not at the mandatory pre-bid meeting to partner with a prime vendor who did attend the mandatory pre-bid meeting.

4. Is the County interested in the technology that would allow the audio recording of the onsite face to face visits?

   Response: The DCSD would defer this question to the DA's office for review and assessment. An attorney representing an inmate could potentially have a face to face visit with the inmate in a booth designated for friends and family visitation due to space limitations and at that time it would be inappropriate to record the conversation.

5. Would it be possible to extend the deadline of October 14, 2019 for submission of the RFP for 60-90 days? We want to give maximum opportunity to SBE contractors in accordance with the goals of the County as expressed in the RFP. This entails learning about their capabilities; interviewing; doing due diligence; and finally, entering into subcontract arrangements. Since we do not yet have your list of qualified organizations, we have not been able to commence this process.

   Response: The due date for receipt of proposals has been extended to the following date:
   <u>October 21, 2019 @ 2:00PM</u>
   All clarification requests must be submitted no later than close of business on October 09, 2019. Responses will be provided by the County no later than close of business on October 11, 2019.

6. As mentioned on page 9, section Rate and Call Charge Requirements, "Each Contractor qualified during Phase 1 will receive cost information from the County, what are the qualifications for Phase 1?

   Response: Phase I is qualified proposals which have been evaluated and submitted to Commissioners Court identifying the firms scored susceptible of advancing to Phase II

7. What are the current call rates and fees for all call and deposit types?

   Response: Automated payment by phone or website $3. Per use. (FCC rule)
   Payment through a live agent: $5.95 per use. (FCC rule)-Per DC agreement cost is $4.95.
   Paper/bill statement fee: $2 per use. (FCC rule)
   Third-party financial transaction fees, such as charged by MoneyGram or Western Union, maybe passed through with no mark-up. (FCC rule)
   All other ancillary service charges are prohibited. (FCC rule)

   "Effect June 20, 2016, the following changes will go into effect for Dallas County, Texas –
   (i) The per minute calling rate for each intrastate (local, IntraLata and InterLata) call will be $.24; (ii) $0.04 per minute of each such intrastate (local, IntraLata and InterLata) call will not be commissionable; and (iii) the fee for automated payments by phone or website are reduced to $3.00 per use (the fee payment through a live agent remains at $4.95 per use)"
   Interstate collect calls $.21 per minute.

8. What is the expected implementation timeframe?

    Response: Dallas County has not determined a set date/timeframe for implementation. DCSD would request the implementation of the Video Visitation System/Inmate Phone system without undue delay.

9. Please provide a list of current SBE vendors that would be approved to work on this project?

    Response: Please see attached list of SBE vendors

10. Is there a current SBE vendor that is working on any part of this project today, or that was part of the implementation of this project originally?

    Response: No SBE subcontractors were identified under the current contract.

11. Please provide a layout of the facility/blueprint broken down by number of dorms per facility and number of inmates per dorm. This is important information to help vendors estimate overall cost to the project.

    Response: The DCSD doesn't have access to facility/blueprints and opines for operational security reasons it would not be prudent to provide such documents for operational security reasons

12. How many face-to-face visits (via the recorded visitation phones) were held in 2018?

    Response: Per TCJS mandate, the DCSD has both face-to-face visitation and the use of a Video Visitation System. DCSD tracked Face-to-Face visits and Video Visits and can provide the following 2018 yearly comparison as follows:

    North Tower Face to Face via visitation phones - 71,104
    North Tower Video Visit- 11,594

    West Tower Face to Face via visitation phones -7,777
    West Tower Video Visit- 1,646

    South Tower (Kays Tower) Face to Face no visitation phones - 34,860
    South Tower (Kays Tower) Video Visit- 5,588

13. As a follow up to the pre-bid meeting, please confirm again that the awarded vendor for this project will have to replace all existing hardware with new/updated equipment (All phones, kiosks, video terminals, etc.).

    Response: Yes, the awarded firm shall provide all new equipment.

14. Please provide a contact for the in-house JMS and also a contact for the courts software for interfacing purposes.

    Response: Current Legacy System – AIS – During the solicitation phase all questions shall be directed to the POC identified in solicitation. Upon award Dallas County will provide the awarded firm will all proper POC. Please note, Dallas County will require the flexibility to interface with alternative systems in the future.

15. Who is the vendor that provides all the court software for Dallas County?

    Response: Current Court system (FORVUS - Mainframe) is managed by IT Applications. During the solicitation phase all questions shall be directed to the POC identified in solicitation. Upon award Dallas County will provide the awarded firm will all proper POC. Please note, Dallas County will require the flexibility to interface with alternative systems in the future.

16. What is the average length of stay for inmates housed at Dallas County?

    Response: DCSD has determined the average length of stay for inmates housed at Dallas County to be approximately 30 days +/- two (2) to three (3) days per month

17. Please specify how awarded vendor should calculate Bond as this is a zero cost to the County?

    Response: The County shall remove the bond requirement for this solicitation. Please see revised RFP for removal.

18. Please confirm that call data information provided in the RFP includes ALL call data made to and from each facility, even items such as Single Call revenue, including number of calls, revenue, and fees? (as an example, but not limited to InstantPay, Text2Connect, AdvanceConnect Single Call, PayNow, etc)

    Response: Yes, Attachment 3 of the solicitation document is all inclusive of call data.

19. Please provide a list of the current education classes being provided? And how are these courses being delivered today?

    Response: DCSD currently provides the following educational classes and related group activities to assist in the education/treatment for the inmate population. Classes are currently being offered through verbal instruction to the inmate, group discussions, instructional pamphlets, books, written documents and in some cases the use of portable laptop computers owned and operated by the agency providing the classes:

    •GED/HiSET – High school equivalency/education classes

    •OSHA – Occupational Safety and Health Administration classes/certifications - OSHA 10- Training (2-day classes)

    •Momentous Institute – Parent Education Classes (Trauma Focused)

    •The Family Place - Batterer Intervention Prevention Program (BIPP)

    •Alpha Friday – Twelve Step Celebrate Recovery Group

    •Holistic Safety, Inc. – Self Improvement Classes – Self-Esteem, Anger Management, Drugs and Alcohol Use, and Health & Hygiene Class

    •The Haven of Love Program (Understanding codependency, hurt, anger, shame, guilt, and identifying self-worth)

    •UT Southwestern – Healthy Relationships Classes; HIV Prevention

•Prison Fellowship – Offers female's life skills, Relapse Prevention, Cognitive Thinking, Dealing with Trauma, provides resources such as TORI and Potter House Referrals

•The Family Place – Trauma/Survivors Groups

•VOA/Resolana Program – Job Readiness, Relapse Prevention, Dialectical behavior therapy, Seeking Safety (DV Victims), Mindful Meditation

•IMPACT Program – Mission of the program is to positively impact lives in the community and abroad by Imparting Knowledge, Mentoring and Molding, Preparing Futures, Admonishing Growth, Creating Leaders, and Teaching Life Skills & Leadership Principles (Offered to female inmates)

•Substance Abuse Support Groups – Alcoholic Anonymous, Narcotic Anonymous, and Crystal Meth Anonymous

Upcoming/Planed/Future Inmate Programs that maybe suitable for use of advanced technology to deliver instructions and materials:

•Recovery Resource Council – Trauma and Informed chemical dependency program for adult males/females and PREA males/females. Services include assessment, individualized case management, and group counseling along with outside resources once inmates are released into the community. The program will offer individual planning for continuity of care and aftercare groups.

•TORI (Texas Offenders Re-entry Initiative) – The program will be offered re-entry and mentoring services to women in custody, aged 18-25. TORI will assist in creating a transition plan based on the 6 Core Components that are the keystone of TORI's empirically validated continuum of care: Employment, Education, Spiritual Guidance, Family Unification, Housing, Mentorship, and Case Management.

20. Who is the current jail management system provider?

Response: Current production system is AIS (Adult Information System) during the solicitation phase all questions shall be directed to the POC identified in solicitation. Upon award Dallas County will provide the awarded firm will all proper POC. Please note, Dallas County will require the flexibility to interface with alternative systems in the future.

21. As mentioned on page 27, section A Bonds, "Performance Bond: If Applicable to this Solicitation" Is a performance bond applicable to this RFP?

Response: No a performance bond is not applicable to this solicitation

22. How many total visitor stations are currently being utilized for video visitation?

Response: DCSD is currently utilizing 10 video visitation stations located on the first floor of the South Tower.

23. As mentioned on page 19, section Financial Capability, #2, "If the year end of the most recent completed audit (or review) is earlier than nine (9) months prior to the issuance date of this RFP, then the most recent unaudited financial statement (consisting of items b, c, d, e and f above) shall also be provided by the respondent in addition to the audited statement required in Section 3.3.1.1." Please confirm where to locate section 3.3.1.1 of this RFP?

    Response: This section has been removed. Please see attached Revised RFP for removal.

24. What is the County's expectation of the SBE% revenue based on?

    Response: 4The SBE evaluation criteria has been removed. However the County still anticipates SBE participation on any subcontracting opportunities.

25. Page 10 – Evaluation Criteria; if the county conducts a site visit and/or an oral presentation, how will these events impact the evaluation point scale on page 10?

    Response: All evaluations will be conducted as outline in the Solicitation document.

26. Page 45 – Attachment 5; there are two references to commissions in this attachment however on page 21 of the RFP, the Cost category indicates the county is not seeking any commission. Please clarify the county's intentions regarding commissions?

    Response: The County will not being seeking a commissions, items requesting commission have been hereby removed from the solicitation document. Please see attached revised RFP for removal.

27. Page 45 – Attachment 5; please provide how the 20 points will be allocated between each of the 6 categories listed. Will fees be allocated points (funding fees, single call fees, etc.), if so how will points be allocated to fees versus the rates requested in Attachment 5. In addition, are vendors required to list the additional fees as there is no area to list all fees? If so, where should the fees be listed?

    Response: All evaluations will be conducted as outline in the Solicitation document.

28. Page 45 – Attachment 5; what methodology will be used to evaluate the rates for calling rates for Collect, Prepaid and Debit calls? Will the County use the historical volumes in Attachment 3 to create a weighted evaluation? Or will the County evaluate the rates independent of these historical volumes?

    Response: All evaluations will be conducted as outline in the Solicitation document.

29. Page 45 – Attachment 5; what methodology will be used to evaluate the rates for Video Visitation calls? Will the County use the historical volumes in Attachment 4 to create a weighted evaluation? Or will the County evaluate the rates independent of these historical volumes?

    Response: All evaluations will be conducted as outline in the Solicitation document.

30. Page 45 – Attachment 5; what methodology will be used to evaluate "Other Technology" as there were not historical volumes provided?

    Response: All evaluations will be conducted as outline in the Solicitation document.

31. Page 45 – Attachment 5; The Cost Category "Other Technology" provides offerors the opportunity to include additional services not specified by the county. Will the additional services be evaluated independently of each other to create different evaluation point scales?

    Response: All evaluations will be conducted as outline in the Solicitation document.

32. Page 45 – Attachment 5; if multiple offers are provided how will all of the offers be evaluated and scored?

    Response: Proposals will be evaluated based on the information requested and the criteria listed in the RFP.

33. How many of the 273 video visitation stations are wall mounted vs portable kiosks?

    Response: DCSD has the following Kiosk systems:

    South Tower:
    50 Video Kiosks which include:
    10 public visitation kiosks
    2 Kiosks in Law Library
    2 Kiosks to schedule visits (for Family and Friends)

    North Tower:
    115 Video Kiosks which include:
    2 Kiosks to schedule visits (for Family and Friends)
    3 Kiosks in Law Library

    West Tower:
    41 Video Kiosks which include:
    1 Kiosk in Law Library

    Med Ops:
    23 Video Kiosks
    24 Total Portable Kiosk systems:

    North Tower:
    8 Portable Video Kiosks

    West Tower:
    16 Portable Video Kiosks

34. How will vendors be evaluated/allocated points for evaluation criteria C. Transition/Implementation Plan and Timeline fairly across all vendors including incumbent when incumbent has the advantage of already having a system installed?

    Response: All evaluations will be conducted as outline in the Solicitation document.

35. Please provide the statistics on the amount of subpoena support provided in the last 12 months?

    Response: This requirement can fluctuate however Dallas County averages approximately 10-15 Subpoenas annually.

36. How many VRS systems does the County require? How many VRS systems does the County currently have?

    Response: DCSD is requesting/requiring five (5) total VRS systems. One (1) will be located in Intake, one (1) will be located in Release and three (3) mobile/portable units will be located in each Tower (North Tower, West Tower and South Tower). DCSD currently does not own or have any VRS systems.

37. Please note that all major cell phone carriers have publicly announced a major shift from past practices. Publicly available document is found here
    https://docs.fcc.gov/public/attachments/DOC-357494A2.pdf.
    The carriers will now only share cell phone location information under limited circumstances, which excludes those circumstances contemplated by this requirement. Accordingly, we respectfully request that the County strike this requirement as we believe that no bidder will be able to meet the requirement without location information from cell phone carriers.

    Response: The County will remove this requirement, however Dallas County reserves the right to require this in the future in conjunction with any applicable law supplements.

38. As mentioned on page 17; Delivery of Proposals, Will the County accept 3-ring binders instead of spiral bound proposal responses?

    Response: Please follow all proposal requirements as outline in the solicitation.

39. At the site visit, we noticed several of the kiosks mounted on pedestals, does the County own these, or are these owned by the current vendor? How many units are mounted on pedestals today?

    Response: The current vendor owns and is responsible to the maintenance and upkeep of the pedestals that the Kiosks are mounted on.

    Breakdown of Kiosk systems on pedestals are as follows:

    North Tower
    8 Video Kiosks are on pedestals for single cell areas
    2 West uppers (2) and lowers (2)
    2 East uppers (2) and lowers (2)

    South Tower/Kays 1st Floor
    9 mounted units' total- 1 in each pod
    10 mounted units in the 1st floor visitation area for public use

    South Tower/Kays 2nd Floor
    9 mounted units' total- 1 in each pod

    South Tower/Kays 3rd Floor

9 mounted units' total - 1 in each pod

South Tower/Kays 4th Floor
9 mounted units' total- 1 in each pod

West Tower does not have Video Kiosks mounted on pedestals

Additional Information:

Visitation Handsets/Visitation Booths

North Tower
Six (6) Floors x 12 Booths x 2 handsets per booth =288 total phones

West Tower
Nine (9) Floors x 10 Booths (variable handset numbers) = 175 total phones

South Tower
South Tower does not utilize visitation phone handsets = 0 total phones

40. Page 21. B. System Functionality, Technical Compliance and Approach. Should this section be responded to in two parts, Statement of Need/Services Sought and Completion of Attachment 6? If so, how will the points be allocated between the two parts?

Response: All evaluations will be conducted as outline in the Solicitation document.

41. Page 10 Section IV - Evaluation Criteria: Will the 30 points for System Functionality all be allocated to Attachment 6. Please clarify how points will be allocated in Attachment 6. For example, will responses with a Y get a specific point allocation, T, a specific point allocation, U.....etc.?

Response: All evaluations will be conducted as outline in the Solicitation document.

42. Page 18. Company Profile: How will the points be allowed between Business/Corporate Experience, Business/Corporate Entity Details, Organizational Chart, Financial Capability, and References?

Response: All evaluations will be conducted as outline in the Solicitation document.

43. Page 21. C. Transition/Implementation Plan and Timeline: How will points be allocated between 1) procedures for transition, 2) times when telephone instruments will be operational..., 3) service coordination, 4) Software programming and preparation for installation, 5) Responsibilities of Dallas County. In addition, how will vendors be evaluated against the incumbent who is already installed versus a new vendor?

Response: All evaluations will be conducted as outline in the Solicitation document.

44. When does the contract with the current vendor end?

Response: December 31, 2019

45. Please provide a copy of all current contracts and amendments pertaining to inmate phones, video visitation, inmate kiosks, tablets, and any other services requested in this RFP.

    Response: This information can be requested through an open records request through Dallas County

46. Attachment 1 says the Government Center Jail is currently de-populated. Does the County anticipate that it will be re-populated during the course of this contract and, if so, when?

    Response: This facility has been decommissioned, there is no plan to re-populate this facility.

47. What is the anticipated start date for this contract?

    Response: Currently the County's anticipated start date is not set due to the solicitation process still ongoing

48. The References requirement on RFP page 20 requires five references with services "similar in magnitude and scope to those requested in the RFP (i.e., 900 or more phones)." This requirement exceeds the experience requirement on page 18 that bidders have at least five contracts with "a minimum 450 phones or more to constitute qualification." If the references must have 900+ phones, this requirement effectively supersedes the experience requirement mandating 450+ phones, raising the minimum qualification to bid to 900+ phones. Will the County change the References requirement on page 20 to "i.e., 450 or more phones" to match the experience requirement on page 18?

    Response: Page 20 has been corrected to say 450 phones. Please see attached RFP document for revision.

49. The price proposal table for video visitation calls on RFP p. 46 requires disclosure of the charge for a 15-minute video visitation. Most video visitation systems provide a 20- or 30-minute visitation session. Does the County require video visitations to be limited to 15 minutes in length?

    Response: Video calls do not have a time limit, the calls can be as long as the customer is will to pay for and do require scheduling. However, please note a proper warning must be provided to the current user of the kiosk to ensure all calls are completed as scheduled.

Except as provided herein/above, all other specification requirements of the original solicitation referenced shall remain unchanged and in full force and effect. This addendum should be signed and returned with your RFP proposal response on or before OCTOBER 21, 2019@ 2:00 P.M, Local Time (Dallas, Texas) Central Time Zone.

This addendum is hereby acknowledged, understood and considered in our proposal.

Printed Name: Robert E. Pickens

Signature of Authorized Representative: _____

Title: Chief Executive Officer

Company: Securus Technologies, Inc.

DALLAS COUNTY
PURCHASING DEPARTMENT
900 Jackson Street * 6th Floor * Suite 680
Dallas, Texas 75202
Michael Frosch
Purchasing Director

October 11, 2019

ADDENDUM No. 4

RFP No. 2019-064-6828

Request for Proposal
Inmate Phone, Video Visitation Service and Inmate Multi-Function Kiosk Provider

This addendum answers all questions received to the best of Dallas County's knowledge and ability.

Questions and Answers:

1. **Please provide current rates and fees for everything listed in Attachment 5. This is necessary to predict how any proposed rate changes will impact the usage rates shown in Attachments 3 and 4.**

    Response: All rates and fees identified to the County are listed in Attachment 5 or Addendum 3.

2. **RFP p. 45 states, "If more than one rate and commission structure is offered, please complete a chart for each optional package using the format below." Please confirm that bidders can offer more than one rate structure**

    Response: Please submit Proposal as outlined in the RFP document.

3. **Please provide the average daily inmate population for each of the three facilities in Attachment 1.**

    Response: Please see addendum 3 for average inmate population on an annual basis.

4. **Are any of the facilities in Attachment 1 connected to each other via fiber?**

    Response: All facilities are standalone facilities.

5. **Please provide a breakdown by housing unit of the inmate capacity and the number of phones and visitation units in each.**

    Response: This varies based on location. Please see addendum 3 and solicitation for current numbers and breakdowns.

6. **Please provide the schedule in which the inmates have access to the inmate phones.**

    Response: Currently inmate video visitations are scheduled ahead of time using the vendor's website.

    Phones usage and video visitation follow the following schedule:

No video visitation for Wednesdays, phones can be used.

Phone/Video visitation hours of usage:

Sunday – Thursday: 7 am to midnight
Friday – Saturday: 7 am to 1 am next morning

Exceptions: there are emergency exceptions where video visitation/phone usage is stopped at 10 pm.

7. RFP page 4 specifies 358 face-to-face visitation phones. Is this 179 booths, for a total of 358 handsets? Are these phones recorded today?

   Response: Face to Face Visitation is not recorded.
   West Tower
   (9 floors – 10 booths – most have 2 handsets (inmate/visitor) some booths have 0 handsets, some have 1 or some have 3)
   175 visitation booth phones
   North Tower
   6 floors, 12 booths east/12 boots west – 24 phones per floor = 144 total in North Tower
   12 attorney booths = 24 attorney booth phones
   168 visitation booth phones
   South Tower
   No phones, all visitation is done in a booth face to face through a screen/slot, no phone handsets.
   Visitation can be done with a Kiosk on the first floor if they want.
   175 visitation booth phones west tower
   168 visitation booth phones north tower
   343 total visitation booth phones

8. What kind of wiring connects the video visitation phones to the equipment room?

   Response: This information will be further outlined with awarded vendor

9. In order to determine adequate network bandwidth, it is necessary to have a breakdown of equipment by facility. For each of the three facilities specified in Attachment 1, please provide the total number of wall-mounted phones, cart phones, cordless phones, TDDs, face-to-face visitation phones, inmate video visitation phones, public video visitation phones, and mobile / cart-mounted video visitation phones.

   Response: This information has been outlined in RFP document and addendum 3.

10. It seems that Dallas County's current vendor may have had influence on the RFP specifications, as some non-essential characteristics of the underlying service have been given undo importance. For example, RFP p. 58 requires video visitation terminals to have "A shatterproof 15-inch minimum LCD or larger touchscreen monitor." A 15-inch or larger monitors significantly increase the cost of inmate kiosks and thereby the cost for inmates and their friends and family, but have no impact on the functionality offered. As a result, the industry has moved to 10-inch monitors that maintain high-quality visual presentation and offer the same functionality as larger monitors, but at a lower cost. As such, will the County revise the requirement to the industry standard of a 10-inch minimum size?

Response: The County has not had discussions with current vendor regarding this solicitation. The screen requirement is what Dallas County currently has and would be open to other solutions proposed.

11. RFP page 4 and Attachment 4 mention Job View. Is Job View a requirement of this contract? If so, since it is owned by your current IPS provider, has your IPS provider agreed to interface with any new IPS vendor to provide ongoing access to this service on kiosks and tablets? Will they charge other IPS vendors for such an interface?

Response: It is our goal to provide inmate with tools to assist them with employment upon release and reduce recidivism. If you company, has a similar solution to assist with employment Dallas County is open to hear about other solutions.

12. As it is written, the RFP strongly favors the incumbent vendor and mandates technology that is proprietary to that vendor. Specifically, the "Investigative Software" on RFP pages 63-64 describe technology that is proprietary to the incumbent vendor and cannot be provided by any other vendor, thus limiting competition under this RFP to one bidder. Therefore:
    a. To your knowledge, does the County utilize any of the aforementioned technology today? If so, is the County charged (via invoice or commission deductions) for the use of any of these services?
    b. Will the County consider revising the RFP to remove these requirements?
       No, Investigative tools are very important as related to inmate phone/video services.
    c. Or, in the alternative, will the County convert these sections to "optional" requirements and state the impact, if any, that the provision of these services will have on the proposal evaluation?

    Response:
       a. Dallas County currently utilizes this technology.
       b. No, Investigative tools are very important as related to inmate phone/video services
       c. The County will utilized current evaluation criteria to evaluate all proposers

13. RFP page 4 specifies "16 mobile/roll around phones." RFP page 54 requires "portable or 'movable' cordless inmate telephones." Are these two requirements for the same thing? If so, please clarify, are these cordless phones, or are they cart-mounted inmate phones (corded)? If the cordless phones on page 54 are a separate requirement, how many of these phones are required?

Response: Yes, 16 mobile phones are required and must be able to be rolled to a cell and plugged in for individual use.

14. RFP p. 59 states, "Has the capability to provide tablet technology to compliment the kiosk/video visitation." Do you have a preferred number of tablets to compliment the video kiosks?

Response: Dallas County is open to a recommended number of tablets by proposer

15. Attachment 5 lists tablets and email under Other Technology. Does the County have inmate tablets and/or email today? If so:
    a. How many tablets does the County have today?
    b. Who is the tablet manufacturer?
    c. Do inmates share the tablets? How do they check them out?

    d. Exactly what services and applications are offered on the tablets?

Response: Dallas County is not currently utilizing tablets.

16. Please provide usage reports for any tablets and email programs that are in use today.

Response: Dallas County is not currently utilizing tablets.

17. Requirement D.8 on page 21 requires bidders to disclose third-party fees that are charged to the client, such as Western Union and MoneyGram. Some vendors offer the ability for a call recipient to pay for a single phone call using a credit or debit card, without the need to set up a prepaid account. The "pass-through fees" associated with these calls may sometimes be as high as $14.99 per call. Please confirm that these types of fees must also be disclosed in accordance with Requirement D.8.

Response: ANY and ALL fees charged to clients (whether by IPS vendor, financial vendor or payment processing center for the receipt, processing or holding payments) relating to the payment for minutes/use of inmate phone/video/kiosk/applications. Fees charge by 3rd party to receive monies related to inmate phone/video/kiosk/applications

18. RFP page 17 requires "two (2) original spiral bound copies of the entire proposal."
    a. Is the requirement for one signed original and one copy, or does the County want two originals with original signatures?
    b. Please confirm these printed copies should include the Cost information.
    c. Should the information in Envelope 2: Cost be submitted on a USB/CD, or printed?
    d. Does the County want two copies of Envelopes 2, or just one copy of each?

Response: Please submit proposal in accordance with the RFP document

19. RFP page 18 lists a few exceptions to the 8.5" x 11" page size limit. Will the County allow for implementation plans to exceed this limit, as well? These plans are typically produced in MS Project, resulting in Gantt charts that print more legibly on 11" x 17" paper.

Response: Please submit proposal in accordance with the RFP document

20. RFP page 21 describes the contents of proposal Tab B. Please clarify, should this tab contain a written description of the system(s) proposed, or should it contain only RFP Attachment 6?

Response: Please submit proposal in accordance with the RFP document

21. RFP page 21 requires that proposal Tab C contain a plan/schedule that includes "procedures for transition of service/equipment from the existing IPS to the new IPS…." Should this plan also include video visitation?

Response: Please submit proposal in accordance with the RFP document

22. The instructions on Attachment 6 advise that "additional comments are encouraged." However, the Comments columns offers very limited space for text. May bidders create a written attachment to the matrix to provide lengthier explanations and visual aids, where appropriate?

Response: Please submit proposal in accordance with the RFP document

23. What percentage of the total dollar amount of the current IPS contract is subcontracted today, and for what types of services?

Response: Due to the nature of the services provided under this contract Dallas County does not have a dollar amount for the subcontract services being performed under the current contract.

24. RFP p. 9 states, "Each Contractor qualified during Phase 1 will receive cost information from the County. This will consist of the rates, which the County desires to be implemented." However, proposed rates are part of the evaluation criteria. Does the County intend to evaluate bidders' proposed calling rates and then later set different rates? If the County intends to set the rates, would you consider doing so in the RFP and removing this scoring component so that everyone is on a level playing field regarding rates?

    Response: Dallas County will evaluate as outline in the RFP document. All proposals will be evaluated in the same manner as outlined

25. How many on-site personnel does the current vendor provide today? How many hours per week are they stationed onsite currently?

    Response: Currently there are onsite personnel working under this contract.

26. RFP p. 33 states, "The vendor may agree to extend their cost to the local governments in the State of South Carolina with agreement of both parties." Is this intentional?

    Response: Dallas County does request confirmation on the extension of costs to local governments. However the County will be removing the State of South Carolina from this request.

27. Please provide the DA's answer as to whether visitation phones should be connected to the ITS for monitoring/recording of non-confidential visits.

    Response: This information will be identified and shared with the awarded vendor

28. Will the County please address the second part of this question: Are vendors required to list additional fees, and if so, where should they be listed? It is unclear from RFP instructions whether this information is required.

    Response: Any and All fees being charged to client SHALL be outline in proposal.

29. The equipment listed under the heading "Additional Information" describes across-the-glass visitation booths, not video visitation, correct?

    Response: "Additional Information" as a heading was not located in the RFP.
    However – Visitation booths are located in all three towers. South Tower has face to face with no handsets/phones but also has 10 Video Kiosks open to the public to be used for visitation purposes. North Tower and West Tower have visitation booths that have a phone handset and/or a Video Kiosk in some select booths.

    Hosted Video Visitation – Hardware Requirements
    Hosted Video Visitation – Technical Requirements

30. Will the County please address the part of this question that seeks clarification to the RFP instructions: "Should this section [System Functionality, Technical Compliance and Approach] be responded to in two parts, Statement of Need/Services Sought [1st part – a narrative response] and Completion of Attachment 6 [2nd part – filling out the matrix]? Or do the instructions on page 21 intend for vendors to complete this section only by filling out Attachment 6?

    Response: Please submit proposal as outline in the RFP document

31. The County's response says, "Page 20 has been corrected to say 450 phones." However, we do not see this reflected in the revised RFP. Is this an oversight?

    Response: Yes, Dallas County's intent is to correct all references to 900 phone reference to 450 phones for references

32. Will a new vendor list be provided, since Shawntech Communications is now a certified SBE vendor?

    Response: A revised list will be updated on Dallas County SBE website.

33. Are the SBE percentage requirements optional on contracts?

    Response: SBE scoring requirement has been removed from this solicitation, although the County still expects that SBE contractors be utilized for Subcontracting opportunities

34. Is the agency considering a lower requirement amount from the original percentage stated on the RFP?

    Response: SBE scoring requirement has been removed from this solicitation, although the County still expects that SBE contractors be utilized for Subcontracting opportunities

35. When will the dates and agenda be issued for the formal Presentation/Demo's and Interviews?

    Response: Once proposals have been received and reviewed firms being interviewed will be notified and provided proper information to prepare.

Except as provided herein/above, all other specification requirements of the original solicitation referenced shall remain unchanged and in full force and effect. This addendum should be signed and returned with your RFP proposal response on or before OCTOBER 21, 2019@ 2:00 P.M, Local Time (Dallas, Texas) Central Time Zone.

This addendum is hereby acknowledged, understood and considered in our proposal.

Printed Name: Robert E. Pickens

Signature of Authorized Representative:

Title: Chief Executive Officer

Company: Securus Technologies, Inc.

DALLAS COUNTY
PURCHASING DEPARTMENT
900 Jackson Street * 6th Floor * Suite 680
Dallas, Texas 75202
Michael Frosch
Purchasing Director

October 16, 2019

ADDENDUM No. 5

RFP No. 2019-064-6828

Request for Proposal
Inmate Phone, Video Visitation Service and Inmate Multi-Function Kiosk Provider

This addendum answers all questions received to the best of Dallas County's knowledge and ability.

Questions and Answers:

1. Will Dallas County consider SBE firms who have pending applications with any of the three certification agencies recognized by policy?

   Response: Yes, Dallas County will consider firms who have pending applications for SBE certification with any of the recognized agencies. Please include the firms with your submittals and indicate their SBE certification is pending and include the application number if possible. Please provide the average daily inmate population for each of the three facilities in Attachment 1.

Except as provided herein/above, all other specification requirements of the original solicitation referenced shall remain unchanged and in full force and effect. This addendum should be signed and returned with your RFP proposal response on or before OCTOBER 21, 2019@ 2:00 P.M, Local Time (Dallas, Texas) Central Time Zone.

This addendum is hereby acknowledged, understood and considered in our proposal.

Printed Name: Robert E. Pickens

Signature of Authorized Representative: _____

Title: Chief Executive Officer

Company: Securus Technologies, Inc.