U.S. Department of Justice
Federal Bureau of Prisons

Central Office
320 First St., NW
Washington, DC 20534

April 25, 2022

Stephen Raher
Prison Policy Initiative
P.O. Box 15189
Portland, OR 97293

Request Number: 2022-03341

Dear Mr. Raher:

This is in response to the above referenced Freedom of Information Act (FOIA) request in which you requested all currently operative contracts (including amendments) for the electronic scanning of incoming inmate (postal) mail, including but not limited to any such contract with Smart Communications.

The Bureau of Prisons (BOP) does not presently have an active contract for Mail Scanning at any institution. However, there were contracts for a Pilot Program for Mail Scanning at FCI Beckley and USP Canaan. The pilot programs at both institutions ran March 1, 2020 to June 30, 2021.

In response to your request, staff located 88 pages of responsive records, which were forwarded to this office for a release determination. After careful review, we determined 76 pages are appropriate for release in full and 12 pages are appropriate for release in part. Copies of releasable records are attached.

Pursuant to the Freedom of Information Act, 5 U.S.C. § 552, records were redacted under the following exemptions (b)(4); (b)(6);and (b)(7)(C) . BOP considered the foreseeable harm standard when reviewing responsive records and applying FOIA exemptions. An explanation of FOIA exemptions is enclosed.

If you have any questions about this response, please feel free to contact the undersigned, this office, or the Federal Bureau of Prisons' (BOP) FOIA Public Liaison, Mr. Eugene Baime, at: 320 First Street NW, Room 924, Washington, DC 20534; bop-ogc-efoia-s@bop.gov; or 202-616-7750 (phone).

Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road (OGIS), College Park, MD 20740-6001; ogis@nara.gov; 202-741-5770 (phone); 1-877-684-6448 (toll free); or 202-741-5769 (fax).

If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, DC 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account following the instructions on OIP's website: https://www.justice.gov/oip/submit-and-track-request-or-appeal. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,

S. Lilly

S. Lilly, GIS, for
Eugene E. Baime, Supervisory Attorney

Explanation of FOIA Exemptions Used by the Federal Bureau of Prisons

5 U.S.C. § 552(b)(1) protects classified information.

5 U.S.C. § 552(b)(2) concerns matters related solely to internal agency personnel rules or practices.

5 U.S.C. § 552(b)(3) concerns matters specifically exempted from release by statute.

5 U.S.C. § 552(b)(4) concerns trade secrets and commercial or financial information obtained from a person that is privileged or confidential.

5 U.S.C. § 552(b)(5) concerns certain inter- and intra-agency communications protected by the deliberative process privilege, the attorney work-product privilege, and/or the attorney-client privilege.

5 U.S.C. § 552(b)(6) concerns material the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties.

5 U.S.C. § 552(b)(7)(A) concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to interfere with enforcement proceedings.

5 U.S.C. § 552(b)(7)(B) concerns records or information compiled for law enforcement purposes the release of which would deprive a person of a right to a fair trial or an impartial adjudication.

5 U.S.C. § 552(b)(7)(C) concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties.

5 U.S.C. § 552(b)(7)(D) concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to disclose the identities of confidential sources and information furnished by such sources.

5 U.S.C. § 552(b)(7)(E) concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

5 U.S.C. § 552(b)(7)(F) concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to endanger the life or personal safety of an individual.

5 U.S.C. § 552(b)(8) concerns matters that are "contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions."

5 U.S.C. § 552(b)(9) concerns geological and geophysical information and data, including maps, concerning wells.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 & 30

1. REQUISITION NUMBER		
2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER
NNG15SC88B	09/16/2019	15BNAS19FU9M10356
5. SOLICITATION NUMBER		6. SOLICITATION ISSUE DATE
7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (*No collect calls*) / 8. OFFER DUE DATE / LOCAL TIME

9. ISSUED BY — CODE: BNAS
Federal Bureau of Prisons
Acquisitions Branch/National Acquisitions Section
320 First Street NW
Room 901-5
WASHINGTON, DC 20534

10. THE ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: % FOR
[ ] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
[ ] EDWOSB
[ ] 8(A)
NAICS: 541519
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS
NET 30

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[ ] RFQ [ ] IFB [ ] RFP

15. DELIVER TO — CODE: (b)(6); (b)(7)(C)
Federal Bueau of Prisons
Office of Security Technology
for USP Canaan
320 1st Street, NW
Washington, DC 20534

16. ADMINISTERED BY — CODE: BNAS
Federal Bureau of Prisons
Acquisitions Branch/National Acquisitions Section
320 First Street NW
Room 901-5
WASHINGTON, DC 20534

17a. CONTRACTOR/OFFEROR — CODE: 541159747 — FACILITY CODE: 884141599
SYSOREX GOVERNMENT SERVICES, INC.
13880 DULLES CORNER LN STE 175
HERNDON, VA 20171-4685
DUNS: 884141599
TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY — CODE: BCO
Federal Bureau of Prisons
Acquisitions Branch/Central Office Business Office
320 First Street NW
Room 901-4
WASHINGTON, DC 20534
Please ensure invoice ref the full contract/order number
(b)(6); (b)(7)(C)@bop.gov

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Delivery Date: 12/31/2019 Mail Scanning - USP Canaan See Continuation Sheet(s) (*Use Reverse and/or Attach Additional Sheets as Necessary*)				

25. ACCOUNTING AND APPROPRIATION DATA
SA-2019-02-FP070022M7-29F-31MN-2019

26. TOTAL AWARD AMOUNT (*For Govt. Use Only*)
(b)(4)

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED
[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [X] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (*SIGNATURE OF CONTRACTING OFFICER*)
(b)(6); (b)(7)(C) Digitally signed by (b)(6); (b)(7)(C)
Date: 2019.09.16 08:02:20 -04'00'

30b. NAME AND TITLE OF SIGNER (*TYPE OR PRINT*)	30c. DATE SIGNED	31b. NAME OF THE CONTRACTING OFFICER (*TYPE OR PRINT*)	31c. DATE SIGNED
		(b)(6); (b)(7)(C)	09/16/2019

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY		

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

STANDARD FORM 1449 (REV. 02/2012) BACK

Table of Contents

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	(b)(4)				
0002					
0003					
0004					
0005					
0006					
				TOTAL	(b)(4)

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
N/A	1	(b)(4)	SA-2019-02-FP070022M7-29F-31MN-2019
		TOTAL (b)(4)	

Award pursuant to the terms and conditions of NASA SEWP V Contract # NNG15SC88B

Section 3 - Contract Clauses

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)		
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov		
Clause	Title	Fill-ins (if applicable)
2852.232-79	INSPECTION AND ACCEPTANCE (DEC 1989)	
DJAR-PGD-08-05	Contractor Certification of Compliance with Federal Tax Requirements	
DJAR-PGD-15-02-1C	Contractor Certification of Compliance with Federal Tax Requirements - Solicitation - (DEVIATION 2015-02) (March 2015)	
DJAR-PGD-08-04	Security of Systems and Data, Including Personally Identifiable Information	
52.239-101	DOJ Residency Requirement - Information Technology (NOV 2008)	
DJAR-PGD-02-02B	Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems	
52.27-103-72	DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)	
DJAR-PGD-15-02-1A	Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - (DEVIATION 2015-02) (March 2015)	
52.219-70XX	Section 8(a) Direct Award (Aug 1998)	SBA Office Address: "Jacksonville FL District Office" SBA Address Line 2: "Florida"
BOP 2852.237-73	DEPARTMENT OF JUSTICE RESIDENCY REQUIREMENT CERTIFICATION FORM (JUNE 2004)	
BOP 2852.219-71	NOTIFICATION TO DELAY PERFORMANCE (JUNE 2007)	
BOP 2852.224-70	INFORMATION RESELLERS OR DATA BROKERS (MAR 2008)	

Clause	Title	Fill-ins (if applicable)
BOP 2852.242-71	EVALUATION OF CONTRACTOR PERFORMANCE UTILIZING CPARS (APR 2011)	
508	COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973, 1998 AMENDMENTS	

Clauses By Full Text

DJAR-PGD-15-03 Security of Department Information and Systems

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by theDOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor

---

NOTICE OF CONTRACTOR PERSONNEL SECURITY REQUIREMENTS
Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
##
1. Long-Term Contractor Personnel:
##
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term2 contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form 1-9, OMB No. 1615-0047, " Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:
•High Risk - Background Investigation (5 year scope)
•Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
•Low Risk - National Agency Check with Inquiries (NACI) investigation
d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;3
4) Waiver request memorandum, including both the Office of Personnel
Management schedule date and position sensitivity/risk level; and 5) Favorable review of the National Agency Check (NAC)4 portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM' s scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
##
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items la. and lb. above. The pre-appointment waiver requirements for short-term contractors are:
a.Favorable review of the security questionnaire form;
b.Favorable fingerprint results;
c.Favorable credit report, if required;5 and
d.Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PFV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
##
3. Intermittent Contractors:

##
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5.The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
##
NOTES:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201 /FIPS-201-22505.pdf.
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM 's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block "B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
(End of Clause)

DJAR-PGD-07-10 Ensuring New Acquisitions Include Common Security Configurations

The following language is to be used in all appropriate solicitations and contracts.
##
(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html
##
(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
(End of Clause)

DJAR-PGD-15-02-1B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Solicitation - (DEVIATION 2015-02) (March 2015)

None of the funds appropriated to the Department under its current Appropriations Act may be used to enter into a contract, grant, or cooperative agreement with an entity that requires employess or contractors of such entity that requires employees or contractors of such entity seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting such waste, fraud, ora buse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information. By submitting a response to this solicitation, the contractor certifies that it does *not* require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or

contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.
##

(End of Provision)

##

52.24-403-70 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;[3]
4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:
a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;
c. Favorable credit report, if required;[5] and
d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
3. Intermittent Contractors:
An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.237-76 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;[3]
4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:
a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;
c. Favorable credit report, if required;[5] and
d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
3. Intermittent Contractors:
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.239-70 DOJ Residency Requirement - Information Technology (NOV 2008)

Department of Justice (DOJ) Order 2640.2F prohibits the use of non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or assisting in the development, operation, management, or

maintenance of any DOJ Information Technology System. By signing this contract or by beginning performance, the contractor agrees to this restriction.
[End of Clause]

DJAR-PGD-15-02-2B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award - (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that it does not require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(End of Clause)

##

BOP 2852.237-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)

For three of the five years immediately prior to submission of an offer/bid/quote, or prior to performance under a contract or commitment, individuals or contractor employees providing services must have:
1. Legally resided in the United States (U.S.);
2. worked for the U.S. overseas in a Federal or military capacity; or
3. been a dependent of a Federal or military employee serving overseas.
If the individual is not a U.S. citizen, they must be from a country allied with the U.S. The following website provides current information regarding allied countries: http://www.opm.gov/employ/html/citizen.htm
By signing this contract or commitment document, or by commencing performance, the contractor agrees to this restriction.
[End of Clause]

Section 4 - List of Attachments

This Section Is Intentionally Left Blank

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE: NNG15SC88B

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUISITION NUMBER	5. PROJECT NUMBER *(If applicable)*
P00001	01/02/2020		

6. ISSUED BY CODE: BNAS

Federal Bureau of Prisons
Acquisitions Branch/National Acquisitions Section
320 First Street NW
Room 901-5
WASHINGTON, DC 20534

7. ADMINISTERED BY *(If other than Item 6)* CODE:

8. NAME AND ADDRESS OF CONTRACTOR *(Number, street, country, state and ZIP Code)*

SYSOREX GOVERNMENT SERVICES, INC.
13880 DULLES CORNER LN STE 175
HERNDON, VA 20171-4685
DUNS: 884141599

CODE 541159747 FACILITY CODE 884141599

(X) | 9A. AMENDMENT OF SOLICITATION NUMBER

9B. DATED *(SEE ITEM 11)*

10A. MODIFICATION OF CONTRACT/ORDER NUMBER: 15BNAS19FU9M10356

X | 10B. DATED *(SEE ITEM 13)*: 09/16/2019

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

SA-2019-02-FP070022M7-29F-31MN-2019

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.

CHECK ONE	
X	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A. 52.243-1(a)
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

The purpose of this modification is to reduce the scope of the original Statement of Work as follows: (b)(4)
(b)(4)
(b)(4) All other terms and conditions remain unchanged.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(b)(6); (b)(7)(C) CEO	(b)(6); (b)(7)(C) (b)(6); (b)(7)(C) (b)(6); *(Signature of person authorized to sign)*	3 JAN 2020	(b)(6); (b)(7)(C)	Digitally signed by (b)(6); (b)(6); (b)(7)(C) 03.10.01.47 -05'00' *(Signature of Contracting Officer)*	01/02/2020

Previous edition unusable

STANDARD FORM 30 (REV. 11/2016)
Prescribed by GSA FAR (48 CFR) 53.243

Table of Contents

Section 2 - Commodity or Services Schedule

Mail Scanning - USP Canaan

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	FEES	AMOUNT
0001	(b)(4)					
0002						
0003						
0004						
0005						

0006

0007

0008

0009

0010

0011	(b)(4)	
0012		
	PREVIOUS TOTAL	(b)(4)
	CHANGE	
	CURRENT TOTAL	

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
N/A	1	(b)(4)	SA-2019-02-FP070022M7-29F-31MN-2019

Award pursuant to the terms and conditions of NASA SEWP V Contract # NNG15SC88B

Section 3 - Contract Clauses

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov

Clause	Title	Fill-ins (if applicable)
2852.232-79	INSPECTION AND ACCEPTANCE (DEC 1989)	
DJAR-PGD-08-05	Contractor Certification of Compliance with Federal Tax Requirements	
DJAR-PGD-15-02-1C	Contractor Certification of Compliance with Federal Tax Requirements - Solicitation - (DEVIATION 2015-02) (March 2015)	
DJAR-PGD-08-04	Security of Systems and Data, Including Personally Identifiable Information	
52.239-101	DOJ Residency Requirement - Information Technology (NOV 2008)	
DJAR-PGD-02-02B	Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems	
52.27-103-72	DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)	
DJAR-PGD-15-02-1A	Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - (DEVIATION 2015-02) (March 2015)	
52.219-70XX	Section 8(a) Direct Award (Aug 1998)	SBA Office Address: "Jacksonville FL District Office" SBA Address Line 2: "Florida"
BOP 2852.237-73	DEPARTMENT OF JUSTICE RESIDENCY REQUIREMENT CERTIFICATION FORM (JUNE 2004)	
BOP 2852.219-71	NOTIFICATION TO DELAY PERFORMANCE (JUNE 2007)	
BOP 2852.224-70	INFORMATION RESELLERS OR DATA BROKERS (MAR 2008)	
BOP 2852.242-71	EVALUATION OF CONTRACTOR PERFORMANCE UTILIZING CPARS (APR 2011)	
508	COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973. 1998 AMENDMENTS	

Clauses By Full Text

DJAR-PGD-15-03 Security of Department Information and Systems

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of

individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO,

and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by theDOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor

NOTICE OF CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.

##

1. Long-Term Contractor Personnel:

##

In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term2 contractor employee whose background investigation (BI) process begins on or after October 27, 2005:

a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form 1-9, OMB No. 1615-0047, " Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);

b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;

c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

•High Risk - Background Investigation (5 year scope)

•Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)

•Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:

1) Favorable review of the security questionnaire form;

2) Favorable fingerprint results;

3) Favorable credit report, if required;3

4) Waiver request memorandum, including both the Office of Personnel

Management schedule date and position sensitivity/risk level; and 5) Favorable review of the National Agency Check (NAC)4 portion of the applicable BI that is determined by position sensitivity/risk level.

A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM' s scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).

e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.

##

2. Short-Term Contractor Personnel:

It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items la. and lb. above. The pre-appointment waiver requirements for short-term contractors are:

a.Favorable review of the security questionnaire form;

b.Favorable fingerprint results;

c.Favorable credit report, if required;5 and

d.Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.

A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PFV-I identity proofing process.

For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.

##

3. Intermittent Contractors:

##

An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.

b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.

c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5.The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
##
NOTES:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201 /FIPS-201-22505.pdf.
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM 's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block "B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
(End of Clause)

DJAR-PGD-07-10 Ensuring New Acquisitions Include Common Security Configurations

The following language is to be used in all appropriate solicitations and contracts.
##
(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html
##
(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
(End of Clause)

DJAR-PGD-15-02-1B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Solicitation - (DEVIATION 2015-02) (March 2015)

None of the funds appropriated to the Department under its current Appropriations Act may be used to enter into a contract, grant, or cooperative agreement with an entity that requires employess or contractors of such entity that requires employees or contractors of such entity seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting such waste, fraud, ora buse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information. By submitting a response to this solicitation, the contractor certifies that it does *not* require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.
##

(End of Provision)

##

52.24-403-70 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.

1. Long-Term Contractor Personnel:

In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:

a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);

b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;

c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:

1) Favorable review of the security questionnaire form;

2) Favorable fingerprint results;

3) Favorable credit report, if required;[3]

4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and

5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.

A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).

e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.

2. Short-Term Contractor Personnel:

It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:

a. Favorable review of the security questionnaire form;

b. Favorable fingerprint results;

c. Favorable credit report, if required;[5] and

d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.

A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.

For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.

3. Intermittent Contractors:

An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.

b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.

c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.

d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.

e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.237-76 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;[3]
4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:
a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;

c. Favorable credit report, if required;[5] and
d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
3. Intermittent Contractors:
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.239-70 DOJ Residency Requirement - Information Technology (NOV 2008)

Department of Justice (DOJ) Order 2640.2F prohibits the use of non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or assisting in the development, operation, management, or maintenance of any DOJ Information Technology System. By signing this contract or by beginning performance, the contractor agrees to this restriction.
[End of Clause]

DJAR-PGD-15-02-2B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award - (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that it does not require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(End of Clause)

##

BOP 2852.237-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)

For three of the five years immediately prior to submission of an offer/bid/quote, or prior to performance under a contract or commitment, individuals or contractor employees providing services must have:
1. Legally resided in the United States (U.S.);
2. worked for the U.S. overseas in a Federal or military capacity; or
3. been a dependent of a Federal or military employee serving overseas.
If the individual is not a U.S. citizen, they must be from a country allied with the U.S. The following website provides current information regarding allied countries: http://www.opm.gov/employ/html/citizen.htm
By signing this contract or commitment document, or by commencing performance, the contractor agrees to this restriction.
[End of Clause]

Section 4 - List of Attachments

No Clauses

No Attachments

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 & 30

1. REQUISITION NUMBER		
2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER
NNG15SC88B	09/16/2019	15BNAS19FU9M10355
5. SOLICITATION NUMBER		6. SOLICITATION ISSUE DATE
7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (*No collect calls*)
		8. OFFER DUE DATE / LOCAL TIME

9. ISSUED BY CODE BNAS
Federal Bureau of Prisons
Acquisitions Branch/National Acquisitions Section
320 First Street NW
Room 901-5
WASHINGTON, DC 20534

10. THE ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: % FOR
[ ] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
[ ] EDWOSB
[ ] 8(A)
NAICS: 541519
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS
NET 30

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[ ] RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE
Federal Bueau of Prisons
Office of Security Technology
for FCI Beckley
320 1st Street, NW
Washington, DC 20534
(b)(6); (b)(7)(C)

16. ADMINISTERED BY CODE BNAS
Federal Bureau of Prisons
Acquisitions Branch/National Acquisitions Section
320 First Street NW
Room 901-5
WASHINGTON, DC 20534

17a. CONTRACTOR/ OFFEROR CODE 541159747 FACILITY CODE 884141599
SYSOREX GOVERNMENT SERVICES, INC.
13880 DULLES CORNER LN STE 175
HERNDON, VA 20171-4685
DUNS: 884141599
TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE BCO
Federal Bureau of Prisons
Acquisitions Branch/Central Office Business Office
320 First Street NW
Room 901-4
WASHINGTON, DC 20534
Please ensure invoice ref the full contract/order number
(b)(6); (b)(7)(C) @bop.gov

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Delivery Date: 12/31/2019 Mail Scanning - FCI Beckley See Continuation Sheet(s) (*Use Reverse and/or Attach Additional Sheets as Necessary*)				

25. ACCOUNTING AND APPROPRIATION DATA
SA-2019-02-FP070022M7-29F-31MN-2019

26. TOTAL AWARD AMOUNT (*For Govt. Use Only*)
(b)(4)

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [X] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5) INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)
(b)(6); (b)(7)(C)
Digitally signed by (b)(6); (b)(7)(C)
Date: 2019.09.16 08:01:29 -04'00'

30b. NAME AND TITLE OF SIGNER (*TYPE OR PRINT*)	30c. DATE SIGNED	31b. NAME OF THE CONTRACTING OFFICER (*TYPE OR PRINT*)	31c. DATE SIGNED
		(b)(6); (b)(7)(C)	09/16/2019

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	
38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY		

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

STANDARD FORM 1449 (REV. 02/2012) BACK

Table of Contents

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	(b)(4)				
0002					
0003					
0004					
0005					
0006					
				TOTAL	(b)(4)

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
N/A	1	(b)(4)	SA-2019-02-FP070022M7-29F-31MN-2019
		TOTAL: (b)(4)	

Award pursuant to the terms and conditions of NASA SEWP V Contract # NNG15SC88B

Section 3 - Contract Clauses

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)		
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov		
Clause	Title	Fill-ins (if applicable)
2852.232-79	INSPECTION AND ACCEPTANCE (DEC 1989)	
DJAR-PGD-08-05	Contractor Certification of Compliance with Federal Tax Requirements	
DJAR-PGD-15-02-1C	Contractor Certification of Compliance with Federal Tax Requirements - Solicitation - (DEVIATION 2015-02) (March 2015)	
DJAR-PGD-08-04	Security of Systems and Data, Including Personally Identifiable Information	
52.239-101	DOJ Residency Requirement - Information Technology (NOV 2008)	
DJAR-PGD-02-02B	Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems	
52.27-103-72	DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)	
DJAR-PGD-15-02-1A	Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - (DEVIATION 2015-02) (March 2015)	
52.219-70XX	Section 8(a) Direct Award (Aug 1998)	SBA Office Address: "Jacksonville FL District Office" SBA Address Line 2: "Florida"
BOP 2852.237-73	DEPARTMENT OF JUSTICE RESIDENCY REQUIREMENT CERTIFICATION FORM (JUNE 2004)	
BOP 2852.219-71	NOTIFICATION TO DELAY PERFORMANCE (JUNE 2007)	
BOP 2852.224-70	INFORMATION RESELLERS OR DATA BROKERS (MAR 2008)	

Clause	Title	Fill-ins (if applicable)
BOP 2852.242-71	EVALUATION OF CONTRACTOR PERFORMANCE UTILIZING CPARS (APR 2011)	
508	COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973, 1998 AMENDMENTS	

Clauses By Full Text

DJAR-PGD-15-03 Security of Department Information and Systems

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by theDOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor

---

NOTICE OF CONTRACTOR PERSONNEL SECURITY REQUIREMENTS
Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
##
1. Long-Term Contractor Personnel:
##
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term2 contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form 1-9, OMB No. 1615-0047, " Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:
•High Risk - Background Investigation (5 year scope)
•Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
•Low Risk - National Agency Check with Inquiries (NACI) investigation
d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;3
4) Waiver request memorandum, including both the Office of Personnel
Management schedule date and position sensitivity/risk level; and 5) Favorable review of the National Agency Check (NAC)4 portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM' s scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
##
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items la. and lb. above. The pre-appointment waiver requirements for short-term contractors are:
a.Favorable review of the security questionnaire form;
b.Favorable fingerprint results;
c.Favorable credit report, if required;5 and
d.Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PFV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
##
3. Intermittent Contractors:

##
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5.The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
##
NOTES:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201 /FIPS-201-22505.pdf.
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM 's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block "B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
(End of Clause)

DJAR-PGD-07-10 Ensuring New Acquisitions Include Common Security Configurations

The following language is to be used in all appropriate solicitations and contracts.
##
(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html
##
(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
(End of Clause)

DJAR-PGD-15-02-1B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Solicitation - (DEVIATION 2015-02) (March 2015)

None of the funds appropriated to the Department under its current Appropriations Act may be used to enter into a contract, grant, or cooperative agreement with an entity that requires employess or contractors of such entity that requires employees or contractors of such entity seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting such waste, fraud, ora buse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information. By submitting a response to this solicitation, the contractor certifies that it does *not* require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or

contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.
##

(End of Provision)

##

52.24-403-70 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;[3]
4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:
a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;
c. Favorable credit report, if required;[5] and
d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
3. Intermittent Contractors:
An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.237-76 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;[3]
4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:
a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;
c. Favorable credit report, if required;[5] and
d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
3. Intermittent Contractors:
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.239-70 DOJ Residency Requirement - Information Technology (NOV 2008)

Department of Justice (DOJ) Order 2640.2F prohibits the use of non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or assisting in the development, operation, management, or

maintenance of any DOJ Information Technology System. By signing this contract or by beginning performance, the contractor agrees to this restriction.
[End of Clause]

DJAR-PGD-15-02-2B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award - (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that it does not require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(End of Clause)

##

BOP 2852.237-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)

For three of the five years immediately prior to submission of an offer/bid/quote, or prior to performance under a contract or commitment, individuals or contractor employees providing services must have:
1. Legally resided in the United States (U.S.);
2. worked for the U.S. overseas in a Federal or military capacity; or
3. been a dependent of a Federal or military employee serving overseas.
If the individual is not a U.S. citizen, they must be from a country allied with the U.S. The following website provides current information regarding allied countries: http://www.opm.gov/employ/html/citizen.htm
By signing this contract or commitment document, or by commencing performance, the contractor agrees to this restriction.
[End of Clause]

Section 4 - List of Attachments

This Section Is Intentionally Left Blank

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	
NNG15SC88B	

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUISITION NUMBER	5. PROJECT NUMBER *(If applicable)*
P00001	01/02/2020		

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
Federal Bureau of Prisons Acquisitions Branch/National Acquisitions Section 320 First Street NW Room 901-5 WASHINGTON, DC 20534	BNAS		

8. NAME AND ADDRESS OF CONTRACTOR *(Number, street, country, state and ZIP Code)*	(X)	9A. AMENDMENT OF SOLICITATION NUMBER
SYSOREX GOVERNMENT SERVICES, INC. 13880 DULLES CORNER LN STE 175 HERNDON, VA 20171-4685 DUNS: 884141599		9B. DATED *(SEE ITEM 11)*
	X	10A. MODIFICATION OF CONTRACT/ORDER NUMBER 15BNAS19FU9M10355
		10B. DATED *(SEE ITEM 13)* 09/16/2019

CODE 541159747 FACILITY CODE 884141599

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

SA-2019-02-FP070022M7-29F-31MN-2019

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.

CHECK ONE	
X	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A. 52.243-1(a)
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation date, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

The purpose of this modification is to reduce the scope of the original Statement of Work as follows: (b)(4)
(b)(4)
(b)(4) All other terms and conditions remain unchanged.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
(b)(6); (b)(7)(C) CEO	(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(b)(6); (b)(7)(C) *(Signature of person authorized to sign)*	3 JAN 2020	(b)(6); (b)(7)(C) Digitally signed by (b)(6); (b)(7)(C) 02:35 -05'00' *(Signature of Contracting Officer)*	01/02/2020

Previous edition unusable

STANDARD FORM 30 (REV. 11/2016)
Prescribed by GSA FAR (48 CFR) 53.243

Table of Contents

Section 2 - Commodity or Services Schedule

Mail Scanning - FCI Beckley

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	FEES	AMOUNT
0001	(b)(4)					
0002						
0003						
0004						
0005						

0006

0007

0008

0009

0010

0011	(b)(4)	
0012		
	PREVIOUS TOTAL	(b)(4)
	CHANGE	
	CURRENT TOTAL	

FUNDING DETAILS:

ITEM NO.	FUNDING LINE	OBLIGATED AMOUNT	ACCOUNTING CODES
N/A	1	(b)(4)	SA-2019-02-FP070022M7-29F-31MN-2019

Award pursuant to the terms and conditions of NASA SEWP V Contract # NNG15SC88B

Section 3 - Contract Clauses

Clauses By Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov

Clause	Title	Fill-ins (if applicable)
2852.232-79	INSPECTION AND ACCEPTANCE (DEC 1989)	
DJAR-PGD-08-05	Contractor Certification of Compliance with Federal Tax Requirements	
DJAR-PGD-15-02-1C	Contractor Certification of Compliance with Federal Tax Requirements - Solicitation - (DEVIATION 2015-02) (March 2015)	
DJAR-PGD-08-04	Security of Systems and Data, Including Personally Identifiable Information	
52.239-101	DOJ Residency Requirement - Information Technology (NOV 2008)	
DJAR-PGD-02-02B	Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems	
52.27-103-72	DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)	
DJAR-PGD-15-02-1A	Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - (DEVIATION 2015-02) (March 2015)	
52.219-70XX	Section 8(a) Direct Award (Aug 1998)	SBA Office Address: "Jacksonville FL District Office" SBA Address Line 2: "Florida"
BOP 2852.237-73	DEPARTMENT OF JUSTICE RESIDENCY REQUIREMENT CERTIFICATION FORM (JUNE 2004)	
BOP 2852.219-71	NOTIFICATION TO DELAY PERFORMANCE (JUNE 2007)	
BOP 2852.224-70	INFORMATION RESELLERS OR DATA BROKERS (MAR 2008)	
BOP 2852.242-71	EVALUATION OF CONTRACTOR PERFORMANCE UTILIZING CPARS (APR 2011)	
508	COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973. 1998 AMENDMENTS	

Clauses By Full Text

DJAR-PGD-15-03 Security of Department Information and Systems

I. Applicability to Contractors and Subcontractors

This clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of contractors, subcontractors, and CSPs (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. It establishes and implements specific DOJ requirements applicable to this Contract. The requirements established herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), including FAR 11.002(g) and 52.239-1, the Privacy Act of 1974, and any other applicable laws, mandates, Procurement Guidance Documents, and Executive Orders pertaining to the development and operation of Information Systems and the protection of Government Information. This clause does not alter or diminish any existing rights, obligation or liability under any other civil and/or criminal law, rule, regulation or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as "data," and "personally identifiable information" ("PII"), regardless of form.

B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.

D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, "processing, storing, or transmitting") Information.

E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.

B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.

C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of

individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, Contractor shall comply with all security requirements, including but not limited to the regulations and guidance found in the Federal Information Security Management Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, OMB Memoranda, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards, including DOJ Order 2640.2, as amended. These requirements include but are not limited to:

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise;

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;

3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;

4. Maintaining authorizations to operate any Covered Information System;

5. Performing continuous monitoring on all Covered Information Systems;

6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;

7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;

9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;

12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;

13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;

14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;

15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;

16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;

17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and

18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.

B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.

D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:

1. Media must be encrypted using a NIST FIPS 140-2 approved product;

2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;

4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,

5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.

F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.

G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.

H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.

I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO,

and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.

J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

A. **Cloud Computing** means an Information System having the essential characteristics described in NIST SP 800-145, The NIST Definition of Cloud Computing. For the sake of this provision and clause, Cloud Computing includes Software as a Service, Platform as a Service, and Infrastructure as a Service, and deployment in a Private Cloud, Community Cloud, Public Cloud, or Hybrid Cloud.

B. Contractor may not utilize the Cloud system of any CSP unless:

1. The Cloud system and CSP have been evaluated and approved by a 3PAO certified under FedRAMP and Contractor has provided the most current Security Assessment Report ("SAR") to the DOJ CO for consideration as part of Contractor's overall System Security Plan, and any subsequent SARs within 30 days of issuance, and has received an ATO from the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under contract; or,

2. If not certified under FedRAMP, the Cloud System and CSP have received an ATO signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under the contract.

C. Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

VI. Information System Security Breach or Incident

A. Definitions

1. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed unauthorized exposure, loss of control, compromise, exfiltration, manipulation, disclosure, acquisition, or accessing of any Covered Information System or any DOJ Information accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system.

2. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed, Covered Information System Security Breach.

3. **Security Incident** means any Confirmed or Potential Covered Information System Security Breach.

B. Confirmed Breach. Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO's Representative ("COR"). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 1-866-US4-CERT (1-866-874-2378) immediately (and in no event later than within 1 hour of discovery of the Confirmed Breach), and shall notify the CO and COR as soon as practicable.

C. Potential Breach.

1. Contractor shall report any Potential Breach within 72 hours of detection to the DOJ CO and the COR, unless Contractor has (a) completed its investigation of the Potential Breach in accordance with its own internal policies and procedures for identification, investigation and mitigation of Security Incidents and (b) determined that there has been no Confirmed Breach.

2. If Contractor has not made a determination within 72 hours of detection of the Potential Breach whether an Confirmed Breach has occurred, Contractor shall report the Potential Breach to the DOJ CO and COR within one-hour (i.e., 73 hours from detection of the Potential Breach). If the time by which to report the Potential Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call the DOJ Computer Emergency Readiness Team (DOJ-CERT) at 1-866-US4-CERT (1-866-874-2378) within one-hour (i.e., 73 hours from detection of the Potential Breach) and contact the DOJ CO and COR as soon as practicable.

D. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify (1) both the Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII, (2) all steps and processes being undertaken by Contractor to minimize, remedy, and/or investigate the Security Incident, (3) any and all other information as required by the US-CERT Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and (4) any other information specifically requested by theDOJ. Contractor shall continue to provide written updates to the DOJ CO regarding the status of the Security Incident at least every three (3) calendar days until informed otherwise by the DOJ CO.

E. All determinations regarding whether and when to notify individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials or the DOJ Core Management Team at DOJ's discretion.

F. Upon notification of a Security Incident in accordance with this section, Contractor must provide to DOJ full access to any affected or potentially affected facility and/or Information System, including access by the DOJ OIG and Federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

G. DOJ, at its sole discretion, may obtain, and Contractor will permit, the assistance of other federal agencies and/or third party contractors or firms to aid in response activities related to any Security Incident. Additionally, DOJ, at its sole discretion, may require Contractor to retain, at Contractor's expense, a Third Party Assessing Organization (3PAO), acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Information Systems.

H. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Personally Identifiable Information Notification Requirement

Contractor certifies that it has a security policy in place that contains procedures to promptly notify any individual whose Personally Identifiable Information ("PII") was, or is reasonably determined by DOJ to have been, compromised. Any notification shall be coordinated with the DOJ CO and shall not proceed until the DOJ has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by Contractor shall be coordinated with, and subject to the approval of, DOJ. Contractor shall be responsible for taking corrective action consistent with DOJ Data Breach Notification Procedures and as directed by the DOJ CO, including all costs and expenses associated with such corrective action, which may include providing credit monitoring to any individuals whose PII was actually or potentially compromised.

VIII. Pass-through of Security Requirements to Subcontractors and CSPs

The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with this Contract, including any CSP providing services for any other CSP under this Contract, and Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to Contractor.

DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor

NOTICE OF CONTRACTOR PERSONNEL SECURITY REQUIREMENTS
Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201)' entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
##
1. Long-Term Contractor Personnel:
##
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term2 contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form 1-9, OMB No. 1615-0047, " Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:
•High Risk - Background Investigation (5 year scope)
•Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
•Low Risk - National Agency Check with Inquiries (NACI) investigation
d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;3
4) Waiver request memorandum, including both the Office of Personnel
Management schedule date and position sensitivity/risk level; and 5) Favorable review of the National Agency Check (NAC)4 portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM' s scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
##
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items la. and lb. above. The pre-appointment waiver requirements for short-term contractors are:
a.Favorable review of the security questionnaire form;
b.Favorable fingerprint results;
c.Favorable credit report, if required;5 and
d.Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PFV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
##
3. Intermittent Contractors:
##
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.

c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5.The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
##
NOTES:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201 /FIPS-201-22505.pdf.
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM 's instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block "B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
(End of Clause)

DJAR-PGD-07-10 Ensuring New Acquisitions Include Common Security Configurations

The following language is to be used in all appropriate solicitations and contracts.
##
(a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html
##
(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
(End of Clause)

DJAR-PGD-15-02-1B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Solicitation - (DEVIATION 2015-02) (March 2015)

None of the funds appropriated to the Department under its current Appropriations Act may be used to enter into a contract, grant, or cooperative agreement with an entity that requires employess or contractors of such entity that requires employees or contractors of such entity seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting such waste, fraud, ora buse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information. By submitting a response to this solicitation, the contractor certifies that it does *not* require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.
##

(End of Provision)

##

52.24-403-70 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.

1. Long-Term Contractor Personnel:

In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:

a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);

b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;

c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:

1) Favorable review of the security questionnaire form;

2) Favorable fingerprint results;

3) Favorable credit report, if required;[3]

4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and

5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.

A badge may be issued following approval of the above waiver requirements.

If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).

e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.

2. Short-Term Contractor Personnel:

It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:

a. Favorable review of the security questionnaire form;

b. Favorable fingerprint results;

c. Favorable credit report, if required;[5] and

d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.

A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.

For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.

3. Intermittent Contractors:

An exception to the above-mentioned short-term requirements would be intermittent contractors.

a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.

b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.

c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.

d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.

e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.237-76 Notice of Contractor Personnel Security Requirements (OCT 2005)

Compliance with Homeland Security Presidential Directive-12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS 201) [1] entitled "Personal Identification Verification (PIV) for Federal Employees and Contractors," Phase I.
1. Long-Term Contractor Personnel:
In order to be compliant with HSPD-12/PIV I, the following investigative requirements must be met for each new long-term [2] contractor employee whose background investigation (BI) process begins on or after October 27, 2005:
a. Contractor Personnel must present two forms of identification in original form prior to badge issuance (acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification," and at least one document must be a valid State or Federal government-issued picture ID);
b. Contractor Personnel must appear in person at least once before a DOJ official who is responsible for checking the identification documents. This identity proofing must be completed sometime during the clearance process but prior to badge issuance and must be documented by the DOJ official;
c. Contractor Personnel must undergo a BI commensurate with the designated risk level associated with the duties of each position. Outlined below are the minimum BI requirements for each risk level:

###High Risk - Background Investigation (5 year scope)
###Moderate Risk - Limited Background Investigation (LBI) or Minimum Background Investigation (MBI)
###Low Risk - National Agency Check with Inquiries (NACI) investigation

d. The pre-appointment BI waiver requirements for all position sensitivity levels are a:
1) Favorable review of the security questionnaire form;
2) Favorable fingerprint results;
3) Favorable credit report, if required;[3]
4) Waiver request memorandum, including both the Office of Personnel Management schedule date and position sensitivity/risk level; and
5) Favorable review of the National Agency Check (NAC) [4] portion of the applicable BI that is determined by position sensitivity/risk level.
A badge may be issued following approval of the above waiver requirements.
If the NAC is not received within five days of OPM's scheduling date, the badge can be issued based on a favorable review of the Security Questionnaire and the Federal Bureau of Investigation Criminal History Check (i.e., fingerprint check results).
e. Badge re-validation will occur once the investigation is completed and favorably adjudicated. If the BI results so justify, badges issued under these procedures will be suspended or revoked.
2. Short-Term Contractor Personnel:
It is the policy of the DOJ that short-term contractors having access to DOJ information systems and/or DOJ facilities or space for six months or fewer are subject to the identity proofing requirements listed in items 1a. and 1b. above. The pre-appointment waiver requirements for short-term contractors are:
a. Favorable review of the security questionnaire form;
b. Favorable fingerprint results;

c. Favorable credit report, if required;[5] and
d. Waiver request memorandum indicating both the position sensitivity/risk level and the duration of the appointment. The commensurate BI does not need to be initiated.
A badge may be issued following approval of the above waiver requirements and the badge will expire six months from the date of issuance. This process can only be used once for a short-term contractor in a twelve month period. This will ensure that any consecutive short-term appointments are subject to the full PIV-I identity proofing process.
For example, if a contractor employee requires daily access for a three or four-week period, this contractor would be cleared according to the above short-term requirements. However, if a second request is submitted for the same contractor employee within a twelve-month period for the purpose of extending the initial contract or for employment under a totally different contract for another three or four-week period, this contractor would now be considered "long-term" and must be cleared according to the long-term requirements as stated in this interim policy.
3. Intermittent Contractors:
An exception to the above-mentioned short-term requirements would be intermittent contractors.
a. For purposes of this policy, "intermittent" is defined as those contractor employees needing access to DOJ information systems and/or DOJ facilities or space for a maximum of one day per week, regardless of the duration of the required intermittent access. For example, the water delivery contractor that delivers water one time each week and is working on a one-year contract.
b. Contractors requiring intermittent access should follow the Department's escort policy. Please reference the August 11, 2004, and January 29, 2001, Department Security Officer policy memoranda that conveys the requirements for contractor facility escorted access.
c. Due to extenuating circumstances, if a component requests unescorted access or DOJ IT system access for an intermittent contractor, the same pre-employment background investigation waiver requirements that apply to short-term contractors are required.
d. If an intermittent contractor is approved for unescorted access, the contractor will only be issued a daily badge. The daily badge will be issued upon entrance into a DOJ facility or space and must be returned upon exiting the same facility or space.
e. If an intermittent contractor is approved for unescorted access, the approval will not exceed one year. If the intermittent contractor requires unescorted access beyond one year, the contractor will need to be re-approved each year.
4. An individual transferring from another department or agency shall not be re-adjudicated provided the individual has a current (within the last five years), favorably adjudicated BI meeting HSPD-12 and DOJ's BI requirements.
5. The DOJ's current escorted contractor policy remains unchanged by this acquisition notice.
Notes:
1. FIPS 201 is available at: www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf
2. Under HSPD-12, long-term contractors are contractors having access to DOJ information systems and/or DOJ facilities or space for six months or longer. The PIV-I identity proofing process, including initiation and adjudication of the required background investigation, is required for all new long-term contractors regardless of whether it is the current practice to issue a badge. The second phase of HSPD-12 implementation (PIV-II) requires badge issuance to all affected long-term contractors.
3. For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
4. In order to avoid a delay in the hiring process, components should request an Advance NAC Report when initiating investigations to OPM. Per OPM ' s instructions, to obtain an Advance NAC Report, a Code " 3" must be placed in block " B " of the " Agency Use Only " section of the investigative form. This report is available for all case types.
5.For contractors in position sensitivity/risk levels above level 1, a favorable review of a credit check is required as part of the pre-appointment waiver package.
##
[End of Clause]

BOP 2852.239-70 DOJ Residency Requirement - Information Technology (NOV 2008)

Department of Justice (DOJ) Order 2640.2F prohibits the use of non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or assisting in the development, operation, management, or maintenance of any DOJ Information Technology System. By signing this contract or by beginning performance, the contractor agrees to this restriction.
[End of Clause]

DJAR-PGD-15-02-2B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award - (DEVIATION 2015-02) (March 2015)

By accepting this award or order, the contractor certifies that it does not require employees or contractors of the contractor seeking to report fraud, waste, and abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors from lawfully reporting waste, fraud, and abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(End of Clause)

##

BOP 2852.237-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)

For three of the five years immediately prior to submission of an offer/bid/quote, or prior to performance under a contract or commitment, individuals or contractor employees providing services must have:
1. Legally resided in the United States (U.S.);
2. worked for the U.S. overseas in a Federal or military capacity; or
3. been a dependent of a Federal or military employee serving overseas.
If the individual is not a U.S. citizen, they must be from a country allied with the U.S. The following website provides current information regarding allied countries: http://www.opm.gov/employ/html/citizen.htm
By signing this contract or commitment document, or by commencing performance, the contractor agrees to this restriction.
[End of Clause]

Section 4 - List of Attachments

No Clauses

No Attachments

Federal Bureau of Prisons

Statement of Work for

Mail Scanning FCI Beckley
Installation and Support

1. Background

The Federal Bureau of Prisons (BOP), has the responsibility for maintaining the security and safety of 177,000 inmates and 36,000 employees in 122 facilities around the country, BOP has the daunting task of controlling the movement of personnel, material, contraband and information. This is a highly complex task given the wide array of avenues available for moving all types of contraband currently in use.

The goal is to eliminate and/or mitigate the introduction of synthetic drug contraband secreted in the physical mail by using off-site postal mail scanning service that will reduce costs, streamline BOP operations, eliminate contraband and provide a whole new field of valuable investigative intelligence not currently available. Inmate mail will be processed and delivered same day it is received at the mail processing hub. This effort will install the required equipment and provide BOP with the digitization of general inmate mail correspondence, the ability to review the inmate mail via electronic file while protecting the institution staff and inmates from the introduction of contraband items.

Purpose

The contractor shall deliver and install a mail scanning system to meet the goals of the Bureau of Prisons' Office of Security Technology (OST). The contractor shall install, test, train staff and process incoming facility inmate mail. BOP presently receives inmate mail at each correctional facility where BOP staff opens and inspects each piece of mail for contraband prior to delivery to inmates. Senders sometimes attempt to smuggle contraband into BOP facilities through inmate mail which has caused BOP staff to be exposed to dangerous contraband, drugs, and other substances which leads to potential health problems and other hazards.

To reduce risks for BOP mail room staff and reduce levels of contraband entering BOP facilities, BOP has requested postal mail scanning, processing, and electronic delivery services provided by the contractor through an off-site mail scanning system. Through this solution, the contractor shall receive inmate mail at one or more mail processing center(s). The mail shall be opened and scanned into a digital format, each record of mail shall be assigned to the appropriate inmate, digital copies of mail shall be made available for review by BOP staff, (review and approve/reject selections to be made by BOP staff), and inmates will receive a printed copy of their mail and/or photographs from the BOP staff which will be batch printed from an electronic files received from the contractor on two (2) computers on the contractor provided network located in the mail room. One (1) computer will be installed in the SIS Office for required mail monitoring of inmates meeting that criteria.

3. Requirements

The BOP will provide the contractor with a periodic inmate data feed daily of all active inmates

at facilities where the mail scanning system is in use. This feed will include each active inmate's Federal Register number, first name, middle name, last name, facility, building and housing pod/dorm location within that facility. Inactive inmates (e.g. not in custody) will not be included. This file will include all active inmates at facilities where the mail scanning system is in use. This file is typically a plain text file in CSV format with one active inmate on each line. The file will be provided daily and will be made available for download by the contractor via secure File Transfer Protocol (FTP) or other mutually agreed upon secure transfer method.

The purpose of the inmate data file is to allow the contractor to properly assign incoming mail to the appropriate facility and housing unit for batch printing.

The contractor's staff will be responsible for the system stand up, testing, training, and close out. The contractor is not allowed to access the BOP network; therefore, the contractor is required to provide a data line at the BOP facility for the purpose of BOP staff accessing the vendor's web-based service. The data line is approved to be installed by the AD and CIO of IPPA. All installed equipment and all work performed will be in accordance with industry best practices, as well as local and national building codes. The contractor will provide all necessary project management, labor, hardware, licensing, and equipment for the installation.

The BOP will provide and install the required network cabling and low voltage power cabling (as specified below), cable path and raceway, provide space for the installation of required network switching, user terminals and power distribution equipment, and ensure adequate AC electrical power is available or installed for the web-based service upon completion of the initial site survey. Additionally, a BOP IT POC/Facility Liaison shall be identified and made available to provide access to telecommunications areas and consult on items specific to the layout and construction of each building.

The BOP shall be responsible for:

1. Providing the contractor with floor plan line diagrams, or other documentation of facility mailroom layout for initial review to ensure availability during the initial site survey. If copies cannot be provided in advance, BOP is to ensure two (2) copies are printed and available to contractor upon arrival for initial site survey. (The contractor will either return the line diagrams upon conclusion or ensure that the documentation is securely stored and restricted from access to only those persons necessary to complete the installation.
2. Providing the contractor with necessary forms to complete for background checks or other authorizations required for access to the work site at least two weeks prior to the arrival date.

The Contractor shall be responsible for:

1. Arriving on-site and providing appropriate personnel who can pass a required security and background clearance to work in a BOP institution.
2. Conducting a kick-off meeting with BOP personnel.
   a. Obtaining floor plan line diagrams, or other documentation of the facility mailroom layout from BOP staff for markup and notes if not provided in advance
   b. Conducting an initial site survey to determine the facility site prep items needed.
   c. Note location of BOP Staff terminals
   d. Providing information about the amount of rack space, electrical power supply, cable raceways, and other infrastructure necessary in MDF, IDF, or other telecommunications rooms; typically, 8U of rack space or less will be required in each area; specific rack sizing requirements will be determined and documented during the

site survey

e. Determining if additional rack space, wall racks, AC electrical circuits, or other infrastructure will need to be installed in MDF, IDF, or other telecommunications rooms
f. Identifying raceway between telecommunications rooms for uplink network connections
g. Identifying whether existing structured cabling such as unused fiber or unused network cable may be used to provide uplink network service between telecommunications rooms; if existing unused structured cabling is available, obtain permission from local IT/facilities to utilize it for network uplinks
h. Identifying broadband internet service providers (ISP) that can service the facility, ordering the data line and getting the ISP to install it.

3. A Color LaserJet MFP capable of 40 ppm and 1200 X 1200 dpi is to be provided by contractor for printing inmate mail and photographs this printer will be on the contractor provided network and available for printing the inmate mail and photographs from the BOP staff user terminals that will be installed by the contractor in the mail room. BOP shall be responsible for printer furnishing and installing replacement ink/toner and paper.

NOTE: All equipment installed will be Americans with Disabilities Act (ADA) compliant. BOP will identify and communicate any corresponding requirements during initial site survey. Section 508 Standards contain "scoping and technical requirements to ensure accessibility and usability by individuals with disabilities. Compliance with these standards is mandatory for Federal agencies subject to Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C.794d)."

Within one (1) week of completion of the initial site survey, contractor shall prepare formal notes to document the initial survey findings to include:

1. List of contractor and BOP staff assigned to the project with contact information
2. Marked-up floor plan to show locations of the MDF, IDF, user terminals and Printer(s). Note any ADA requirements.
3. Breakdown of each MDF, IDF, or other telecommunications location with a description and parts list for any network, power switching, power distribution, mounting hardware, or other equipment to be installed in each area. If existing rack space is to be utilized it should be identified, and if new racks or cabinets are to be installed the sizes and locations should be noted.
4. Identified Internet Service Providers
5. Any other pertinent site-specific information needed

Once prepared, the survey documentation shall be distributed to all parties involved with the installation for review.

The contractor shall place an order for service with an appropriate broadband Internet Service Provider (ISP) to bring broadband Internet service into the building. The specific details of the installation for Internet service, site visits by the ISP, and other requirements will be site-dependent and coordinated with BOP staff as needed to accommodate the ISP bringing service into the building and provisioning cabling, equipment, etc. to enable this solution. The contractor shall be listed as the customer for the ISP account and responsible for handling direct billing from the ISP.

The contractor shall be responsible for initially responding to any service outages or initiating

repair orders with the ISP once installed. The contractor will coordinate with BOP staff if an ISP technician requires access for maintenance after installation.

BOP staff shall be responsible for the following:

1. Create a suitable cable raceway between the designated telecommunications room as needed and identified in the site survey and each BOP staff terminal. This could include wall penetrations, surface mounted conduit, cable hangars, cable trays, or other means to create a secure pathway for network and low voltage cable to follow. All raceways shall be installed according to local building codes and industry best-practices.
2. Install network cable and low voltage power cable between the telecommunicationsroom as identified by the site survey and each BOP staff terminal location and printer(s). The following cable specifications shall be used:
   a. Network – Category 6 network cable. Solid core, solid copper cable shall be utilized. Copper-clad aluminum (CCA) cable shall not be used. Cable shall be appropriately rated for its installation environment (e.g. riser or plenum rated cable must be used when installed in those environments).
   b. Network and low voltage power cabling may share the same raceway
   c. During installation each cable shall be labeled on each end as to where the other end is located. Network cable and low voltage power shall be labeled individually.
   d. In the telecommunications room, cable shall be installed, routed, and dressed to within five (5) feet of where the patch panel will be installed. An additional 10 feet of cable shall be provided on the telecommunications side to allow for additional routing, dressing, and termination at the patch panel.
   e. In the mail room area, cable must be long enough to reach the BOP staff terminals and printer(s) through the designated raceway and terminated for CAT5/6. Cable runs shall be no longer than 300 feet.
   f. In the SIS Office, cable must be long enough to reach the BOP staff terminal through the designated raceway and terminated for CAT5/6. Cable runs shall be no longer than 300 feet.
   g. If any new cabling was specified to be installed between MDF, IDF, or telecommunications rooms, mail room or SIS Office, install as specified in the site survey documentation.
   h. If any new AC power circuits are called for in the survey notes, install to rack locations, mail room or SIS Office per survey documentation ensuring all local permit and code requirements are met.

Contractor staff shall be responsible for the following:

1. Arrive on-site and obtain the necessary credentials and escort to customer work spaces:
   a. Conduct follow-on meeting with customer personnel
   b. Conduct a review of facility-installed items to include:
      i. Visit telecommunications room(s), mail room and SIS office locations to ensure proper installation of cable raceway, and that network and power are installed, labeled, and staged for final connection into each user terminal
      ii. Be escorted to all MDF, IDF, and other telecommunications rooms to verify available rack space, wall space for new racks, AC power circuits, and that network and low voltage power cables have been installed to the correct locations

and are properly labeled

c. Verify uplink cabling has been installed and labeled between telecommunications rooms if required, or that designated existing fiber is still unused and available for use
d. Create a remediation checklist for BOP staff if any deficiencies are found and follow up on completion prior to scheduled installation
e. Schedule Installation Date
f. Arrange for shipping of materials to site attention to appropriate receiver

2. Arrive on-site and obtain the necessary credentials and escort to customer work spaces:

   a. Conduct on-site equipment inventory per survey documentation and make arrangements to replace any damaged or missing equipment
   b. Install equipment into MDF, IDF, and telecommunications rooms, mail room and SIS Office: install any new racks or cabinets for network infrastructure if called for.
      i. Install network patch panels and route, dress, and terminate network cable into patch panels, labeling ports per label on cabling (including uplinks to other telecommunications rooms if applicable)
      ii. Install network switches and appropriate patch cables between patch panels and switches
      iii. Install power distribution equipment
      iv. Route, dress, and attach low voltage power equipment to power distribution equipment, labeling ports per label on cabling
      v. Document which user terminals and printers are attached to which ports on network switches equipment
      vi. Install network-enabled power switches and attach power distribution equipment; document which distributors are connected to which outlets for remote management
   c. Install battery backup(s) and attach network switches and remote power switches
   d. Attach battery backup(s) to AC electrical circuits
   e. Install any uplink adapters for existing fiber if needed and connect fiber using appropriate patch cables (where applicable)
   f. Test uplink cabling between telecommunications rooms with a cable tester to ensure proper termination and continuity of all pairs and that length does not exceed 300 feet; remediate problems immediately if possible, add to post-installation remediation checklist if necessary

3. At MDF location: Test broadband Internet Service Provider and Internet access using a laptop; ensure static IP address is assigned and documented; verify DNS entry has been created

   a. Install firewall and MP-VPN router or another designated head-end equipment
   b. Configure and connect MP-VPN router or another designated head-end equipment to broadband Internet Service Provider
   c. Work with remote support staff to test remote access to the network from the contractor data center; troubleshoot and remediate as needed

4. At each staff user terminal and printer location: BOP to provide a suitable space, power and network connection

a. Route, dress, and size/cut network cable and terminate with an appropriate modular connector for the type of cable installed (cat5e, cat6, etc.)
b. Re-connect port on patch panel to network switch when testing is finished
c. Connect power to user terminal and printer(s)
d. Power on user terminal and printer(s) to ensure they properly boot up into the client software
e. If full network access has been established, ensure contractor web application is loading and that the accounts can sign in
f. Work with BOP IT POC/Liaison to install a Color LaserJet MFP capable of 40 ppm and 1200 X 1200 dpi on the three computers on the contractor network located in the mail room and SIS Office which will be used to batch print inmate mail from an electronic file received from the contractor.

Training may occur before, during, or after the network installation. Contractor staff shall work with BOP IT POC/Facility Liaison to arrange on-site training. Training shall involve facility administration and mailroom and SIS staff to cover:

1. Management console access and account management
2. Reviewing scanned mail for approval or rejection
3. Handling inmate requests for printed copies of mail
4. Requesting that a piece of mail be held for additional time or forwarded to the facility
5. Discussion of the postal mail transition process
6. Ongoing support procedures

4. Work Environment

The work under this contract shall primarily be performed at the Federal Bureau of Prisons, the Federal Correctional Institution Beckley, West Virginia. Typically, the work week will be the standard 40 hours a week. Depending on the task, however, additional work may be required (e.g. deployments or maintenance during non-official hours to avoid disruption).

Contractor's price and efforts are based on the assumptions, terms, and conditions as stated below:

1. BOP provides an inmate data feed to include all active inmates at facilities where the email scanning system will be in use.
2. All required network cable runs shall be installed by BOP and shall be compliant with all applicable building codes and according to design layout as directed by contractor's initial site survey.
3. All required low voltage power cable runs shall be installed by BOP and shall be compliant with all applicable building codes and according to design layout as directed by contractor's initial site survey.
4. Adequate electrical power shall be available in the MDF, IDF, and other telecommunications rooms and other installation areas to support the required equipment identified during the initial site visit.
5. Adequate rack space and wall space shall be available for all required equipment.
6. BOP shall provide power, space, and location for the staff terminals and printer. Following contractor's installation and setup, BOP shall be responsible for printer furnishing and installing replacement ink/toner and paper.
7. Mail room, SIS staff and other users who require access will be able to reach the

contractor's website to log in to the contractor management console to review mail, process print requests, and perform other system management tasks.

8. BOP shall establish hours of operation and have staff available during these hours to support project activities. Current installation planning is based on the contractor being provided uninterrupted access to all necessary areas to during normal business hours (Monday-Friday between 7:30 AM – 5:30 PM). Contractor shall be given physical access and permission to work in the facility MDF room, IDF rooms, telecommunications rooms, administrative areas, and the planned user terminal and printer(s) areas.
9. All security access protocols and credentials shall be established for contractor access, as required, at least two (2) weeks prior to contractor arriving on site.
10. BOP will provide escorts for the contractor's staff who have access to all installation areas.
11. BOP shall identify the shipping location and be aware of deliveries ahead of schedule.
12. BOP shall provide a secure staging area for storage of received equipment, tools, and other project materials.
13. BOP shall provide a suitable ladder, extension ladder, or powered lift to access staged cable during installation where applicable; BOP shall provide authorization for use of BOP-owned ladders and powered lifts where applicable or to provide personnel authorized to use such equipment if contractor personnel are not authorized to use it directly.
14. BOP is not imposing requirements for the brands, types, model numbers, etc. user terminals, network switches, power controllers, power distribution equipment, and other components installed into the facility. But BOP may disapprove the use of specific equipment if it implicates or introduces information security or correctional security concerns or risks (e.g. introduce unauthorized cellular communications, do not meet industry manufacturing standards, etc.). The repair or maintenance of any equipment which stores BOP data and requires the removal from BOP or vendor premises must be preceded by advance notice and concurrence of BOP.
15. Contractor shall hold original physical inmate mail at the processing center for 30 calendar days from the date it was scanned. Individual pieces of mail identified by BOP staff may be selected to be pulled and held for longer periods if justified (for example for a court proceeding). Individual pieces of mail may be requested to be forwarded to a BOP facility or other designated location if necessary. After the holding period has expired, contractor shall dispose of the physical original mail by securely shredding it and optionally recycling the resulting shredded paper.
16. Contractor shall designate an existing, or establish a new, regional mailbox for the receiving of inmate mail. Mail received will be forwarded to a mail processing center. BOP shall be responsible to communicate the address of the designated mailbox to the public through its normal communications channels.

Any changes to site access hours and/or dates must be agreed to in advance and in writing by both the contractor and the BOP. Any delays outside of the contractor's control may require an extension of the project schedule and additional charges may be incurred. Additional charges shall be based upon the additional time on-site and all associated expenses, including but not limited to per diem, travel, housing, etc.

5. Work Environment

5.1 Required Skills and Proficiencies

The contractor resource team must have the following skills/abilities: compliance with DOJ IT

security requirements, off site mail scanning, contraband detection, records management, and investigative analysis.

5.2 Security and Clearance Requirements

The specific system that will be used in this instance is classified at the medium risk level. The corresponding clearance is MBI (Minimum Background Investigation).

Contractor security clearances, including the submission of security clearance forms, etc., shall be coordinated with the Government Task Manager prior to contract employee engagement at the BOP's Central Office. As determined by the GTM and/or Human Resource Security Specialist, clearances may require one or all of the following:

- DOJ-99 (name check);
- FD-258 (fingerprint check);
- Law Enforcement Agency checks;
- Vouchering of Employers over past five years;
- Resume/Personal Qualifications;
- OPM-329-A (Authority for Release of Information);
- Urinalysis Test (for detection of marijuana and another drug usage).

Note: If it is determined that a urinalysis test is required, it will be administered at the closest BOP site. If a test is positive for drug usage, the assigned individual(s) shall be excluded from performance of work for this requirement, and subject to the same security requirements, the contractor shall provide acceptable replacement staff.

The contractor shall employ effective safeguards and security controls to ensure that information associated with the work is protected from loss, damage, computer viruses or other destructive incidents. The safeguards employed should ensure that materials and services are secured in a manner that prevents tampering, sabotage or other means of deliberate alteration. This provision applies to all BOP information resources while under the control of the contractor.

The contractor shall participate in annual refresher training (provided by the Bureau of Prisons) for information security awareness and such participation will be documented by the BOP. Failure to participate may result in exclusion or removal from work on this contract and require the vendor to provide suitable replacements.

Loss Reporting: If contractor experiences a loss of Personally Identifiable Information (PII) provided by the BOP under the terms of this contract, the contractor will follow OMB loss reporting guidelines (OMB M-17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information") and notify the BOP COR within one (1) hour of discovering any actual or suspected breach of such data (i.e., Loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic). If within one (1) hour the vendor has been unable to make a report to the BOP COR, the contractor will call the DOJ Computer Emergency Readiness Team (DOJCERT) at 1-866-US4-CERT (1-866-874-2378) and make the report.

Inspection: To ensure compliance with the security requirements of this contract and/or in the event of an actual or suspected loss or breach of PII, the BOP reserves the right to inspect the

facilities wherein BOP inmate mail will be or is received, processed and stored. Such inspections may be unannounced and will be performed by the BOP COR and Information Security Programs staff.

6. Government-Furnished Equipment

6.1 Government Furnished Property (GFP)

The facility is responsible for rack space, power and network drops at all installation locations.

6.2 GOVERNMENT FURNISHED MATERIALS (GFM)

The government will provide access to government facilities at no cost to the contractor, as needed and on a schedule mutually agreeable to the contractor and the government based on guidance of the OST. BOP will provide for paper and ink for printer(s).

6.3 GOVERNMENT FURNISHED INFORMATION (GFI)

GFI will be provided at no cost to the contractor on an as-needed basis as defined by the solutions provider and OST.

7. SCOPE OF WORK

The contractor shall deliver and install a mail scanning system to meet the goals of the Bureau of Prisons' Office of Security Technology (OST). The contractor shall install, test, train staff and process incoming facility Inmate Mail.

BOP presently receives inmate mail at each correctional facility where BOP staff opens and inspects each piece of mail for contraband prior to delivery to inmates. Senders sometimes attempt to smuggle contraband into BOP facilities through inmate mail which has caused BOP staff to be exposed to dangerous contraband, drugs, and other substances which leads to potential health problems and other hazards.

To reduce risks for BOP mail room staff and reduce levels of contraband entering BOP facilities, BOP has requested postal mail scanning, processing, and electronic delivery services provided by contractor through the mail scanning system.

Through this service, the contractor shall receive inmate mail at one or more mail processing center(s). The mail shall be opened and scanned into a digital format, each record of mail shall be assigned to the appropriate inmate, digital copies of mail shall be made available for review by BOP staff. After review and approve/reject selections are made by BOP staff, inmates will receive their approved mail via a printed copy from BOP staff.

8. Project Management

The Bureau will appoint a Government Task Manager (GTM) for this project. The GTM is responsible for receiving all deliverables, inspecting, and accepting the services provided for this requirement in accordance with the terms and conditions of this contract, providing direction to the contractor which clarifies the contract effort, fills in details, or otherwise serves to accomplish the technical scope of work, evaluates performance, and certifies all invoices/vouchers for acceptance of the services furnished for payment.

Contractor shall provide an off-site Project Manager. The Project Manager shall lead the overall

execution of the activities in this SOW, including providing oversight of any tasks required by the SOW.

Additionally, the Project Manager shall ensure that:

1. Staff understand and work toward SOW objectives;
2. Tasks are staffed by appropriate, highly-qualified personnel; and
3. All project management issues are communicated to and coordinated with the GTM. An initial project plan shall be submitted to the GTM for review and approval within 30 days of award. Status reporting on tasks shall provide accurate information concerning:

    i. Project Progress
    ii. Planned activities for the next reporting period
    iii. Issues that are affected, or are expected to affect, the project schedule
    iv. Any items that might enhance, or detract from, the overall success of the project

9. Period of Performance

The contractor will provide this support for a period of one (1) year from completion of installation.

10. Travel

Travel between contractor facilities and FCI Beckley will be required and as mutually agreed upon and in accordance with the effort.

11. Key Personnel

The requested Key Personnel for this SOW is one vendor Project Manager.

The contractor shall immediately remove any personnel determined unsuitable in compliance with security provisions or found to represent a threat to the safety of government records, government employees, or other contractor staff. Replacement of key personnel is subject to prior written approval of the GTM.

The contractor agrees that during the first ninety (90) calendar days of the contract performance period no key personnel substitutions will be permitted unless such substitutions are required by the Government, or necessitated by an individual's sudden illness, death or termination of employment. All requests for substitutions must provide a detailed explanation of the circumstances necessitating the proposed substitution, a resume for the proposed substitute, and any other information requested by the GTM to aid in the process of approving or disapproving the proposed substitute. Proposed substitutions shall have the same (or better) qualifications and experience as the personnel being replaced.

Past the ninety (90) day period, the contractor shall advise the GTM no later than 30 days in advance of any required replacement of key personnel. All requests for substitutions must provide a detailed explanation of the circumstances necessitating the proposed substitution, a resume for the proposed substitute, and any other information requested by the GTM to aid in the process of approving or disapproving the proposed substitute. Proposed substitutions shall have the same (or better) qualifications and experience as the personnel being replaced.

Federal Bureau of Prisons

Statement of Work for

Mail Scanning FCI Canaan
Installation and Support

1. Background

The Federal Bureau of Prisons (BOP), has the responsibility for maintaining the security and safety of 177,000 inmates and 36,000 employees in 122 facilities around the country, BOP has the daunting task of controlling the movement of personnel, material, contraband and information. This is a highly complex task given the wide array of avenues available for moving all types of contraband currently in use.

The goal is to eliminate and/or mitigate the introduction of synthetic drug contraband secreted in the physical mail by using off-site postal mail scanning service that will reduce costs, streamline BOP operations, eliminate contraband and provide a whole new field of valuable investigative intelligence not currently available. Inmate mail will be processed and delivered same day it is received at the mail processing hub. This effort will install the required equipment and provide BOP with the digitization of general inmate mail correspondence, the ability to review the inmate mail via electronic file while protecting the institution staff and inmates from the introduction of contraband items.

Purpose

The contractor shall deliver and install a mail scanning system to meet the goals of the Bureau of Prisons' Office of Security Technology (OST). The contractor shall install, test, train staff and process incoming facility inmate mail. BOP presently receives inmate mail at each correctional facility where BOP staff opens and inspects each piece of mail for contraband prior to delivery to inmates. Senders sometimes attempt to smuggle contraband into BOP facilities through inmate mail which has caused BOP staff to be exposed to dangerous contraband, drugs, and other substances which leads to potential health problems and other hazards.

To reduce risks for BOP mail room staff and reduce levels of contraband entering BOP facilities, BOP has requested postal mail scanning, processing, and electronic delivery services provided by the contractor through an off-site mail scanning system. Through this solution, the contractor shall receive inmate mail at one or more mail processing center(s). The mail shall be opened and scanned into a digital format, each record of mail shall be assigned to the appropriate inmate, digital copies of mail shall be made available for review by BOP staff, (review and approve/reject selections to be made by BOP staff), and inmates will receive a printed copy of their mail and/or photographs from the BOP staff which will be batch printed from an electronic files received from the contractor on two (2) computers on the contractor provided network located in the mail room. One (1) computer will be installed in the SIS Office for required mail monitoring of inmates meeting that criteria.

3. Requirements

The BOP will provide the contractor with a periodic inmate data feed daily of all active inmates

at facilities where the mail scanning system is in use. This feed will include each active inmate's Federal Register number, first name, middle name, last name, facility, building and housing pod/dorm location within that facility. Inactive inmates (e.g. not in custody) will not be included. This file will include all active inmates at facilities where the mail scanning system is in use. This file is typically a plain text file in CSV format with one active inmate on each line. The file will be provided daily and will be made available for download by the contractor via secure File Transfer Protocol (FTP) or other mutually agreed upon secure transfer method.

The purpose of the inmate data file is to allow the contractor to properly assign incoming mail to the appropriate facility and housing unit for batch printing.

The contractor's staff will be responsible for the system stand up, testing, training, and close out. The contractor is not allowed to access the BOP network; therefore, the contractor is required to provide a data line at the BOP facility for the purpose of BOP staff accessing the vendor's web-based service. The data line is approved to be installed by the AD and CIO of IPPA. All installed equipment and all work performed will be in accordance with industry best practices, as well as local and national building codes. The contractor will provide all necessary project management, labor, hardware, licensing, and equipment for the installation.

The BOP will provide and install the required network cabling and low voltage power cabling (as specified below), cable path and raceway, provide space for the installation of required network switching, user terminals and power distribution equipment, and ensure adequate AC electrical power is available or installed for the web-based service upon completion of the initial site survey. Additionally, a BOP IT POC/Facility Liaison shall be identified and made available to provide access to telecommunications areas and consult on items specific to the layout and construction of each building.

The BOP shall be responsible for:

1. Providing the contractor with floor plan line diagrams, or other documentation of facility mailroom layout for initial review to ensure availability during the initial site survey. If copies cannot be provided in advance, BOP is to ensure two (2) copies are printed and available to contractor upon arrival for initial site survey. (The contractor will either return the line diagrams upon conclusion or ensure that the documentation is securely stored and restricted from access to only those persons necessary to complete the installation.
2. Providing the contractor with necessary forms to complete for background checks or other authorizations required for access to the work site at least two weeks prior to the arrival date.

The Contractor shall be responsible for:

1. Arriving on-site and providing appropriate personnel who can pass a required security and background clearance to work in a BOP institution.
2. Conducting a kick-off meeting with BOP personnel.
   a. Obtaining floor plan line diagrams, or other documentation of the facility mailroom layout from BOP staff for markup and notes if not provided in advance
   b. Conducting an initial site survey to determine the facility site prep items needed.
   c. Note location of BOP Staff terminals
   d. Providing information about the amount of rack space, electrical power supply, cable raceways, and other infrastructure necessary in MDF, IDF, or other telecommunications rooms; typically, 8U of rack space or less will be required in each area; specific rack sizing requirements will be determined and documented during the

site survey

e. Determining if additional rack space, wall racks, AC electrical circuits, or other infrastructure will need to be installed in MDF, IDF, or other telecommunications rooms
f. Identifying raceway between telecommunications rooms for uplink network connections
g. Identifying whether existing structured cabling such as unused fiber or unused network cable may be used to provide uplink network service between telecommunications rooms; if existing unused structured cabling is available, obtain permission from local IT/facilities to utilize it for network uplinks
h. Identifying broadband internet service providers (ISP) that can service the facility, ordering the data line and getting the ISP to install it.

3. A Color LaserJet MFP capable of 40 ppm and 1200 X 1200 dpi is to be provided by contractor for printing inmate mail and photographs this printer will be on the contractor provided network and available for printing the inmate mail and photographs from the BOP staff user terminals that will be installed by the contractor in the mail room. BOP shall be responsible for printer furnishing and installing replacement ink/toner and paper.

NOTE: All equipment installed will be Americans with Disabilities Act (ADA) compliant. BOP will identify and communicate any corresponding requirements during initial site survey. Section 508 Standards contain "scoping and technical requirements to ensure accessibility and usability by individuals with disabilities. Compliance with these standards is mandatory for Federal agencies subject to Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C.794d)."

Within one (1) week of completion of the initial site survey, contractor shall prepare formal notes to document the initial survey findings to include:

1. List of contractor and BOP staff assigned to the project with contact information
2. Marked-up floor plan to show locations of the MDF, IDF, user terminals and Printer(s). Note any ADA requirements.
3. Breakdown of each MDF, IDF, or other telecommunications location with a description and parts list for any network, power switching, power distribution, mounting hardware, or other equipment to be installed in each area. If existing rack space is to be utilized it should be identified, and if new racks or cabinets are to be installed the sizes and locations should be noted.
4. Identified Internet Service Providers
5. Any other pertinent site-specific information needed

Once prepared, the survey documentation shall be distributed to all parties involved with the installation for review.

The contractor shall place an order for service with an appropriate broadband Internet Service Provider (ISP) to bring broadband Internet service into the building. The specific details of the installation for Internet service, site visits by the ISP, and other requirements will be site-dependent and coordinated with BOP staff as needed to accommodate the ISP bringing service into the building and provisioning cabling, equipment, etc. to enable this solution. The contractor shall be listed as the customer for the ISP account and responsible for handling direct billing from the ISP.

The contractor shall be responsible for initially responding to any service outages or initiating

repair orders with the ISP once installed. The contractor will coordinate with BOP staff if an ISP technician requires access for maintenance after installation.

BOP staff shall be responsible for the following:

1. Create a suitable cable raceway between the designated telecommunications room as needed and identified in the site survey and each BOP staff terminal. This could include wall penetrations, surface mounted conduit, cable hangars, cable trays, or other means to create a secure pathway for network and low voltage cable to follow. All raceways shall be installed according to local building codes and industry best-practices.
2. Install network cable and low voltage power cable between the telecommunicationsroom as identified by the site survey and each BOP staff terminal location and printer(s). The following cable specifications shall be used:
   a. Network – Category 6 network cable. Solid core, solid copper cable shall be utilized. Copper-clad aluminum (CCA) cable shall not be used. Cable shall be appropriately rated for its installation environment (e.g. riser or plenum rated cable must be used when installed in those environments).
   b. Network and low voltage power cabling may share the same raceway
   c. During installation each cable shall be labeled on each end as to where the other end is located. Network cable and low voltage power shall be labeled individually.
   d. In the telecommunications room, cable shall be installed, routed, and dressed to within five (5) feet of where the patch panel will be installed. An additional 10 feet of cable shall be provided on the telecommunications side to allow for additional routing, dressing, and termination at the patch panel.
   e. In the mail room area, cable must be long enough to reach the BOP staff terminals and printer(s) through the designated raceway and terminated for CAT5/6. Cable runs shall be no longer than 300 feet.
   f. In the SIS Office, cable must be long enough to reach the BOP staff terminal through the designated raceway and terminated for CAT5/6. Cable runs shall be no longer than 300 feet.
   g. If any new cabling was specified to be installed between MDF, IDF, or telecommunications rooms, mail room or SIS Office, install as specified in the site survey documentation.
   h. If any new AC power circuits are called for in the survey notes, install to rack locations, mail room or SIS Office per survey documentation ensuring all local permit and code requirements are met.

Contractor staff shall be responsible for the following:

1. Arrive on-site and obtain the necessary credentials and escort to customer work spaces:
   a. Conduct follow-on meeting with customer personnel
   b. Conduct a review of facility-installed items to include:
      i. Visit telecommunications room(s), mail room and SIS office locations to ensure proper installation of cable raceway, and that network and power are installed, labeled, and staged for final connection into each user terminal
      ii. Be escorted to all MDF, IDF, and other telecommunications rooms to verify available rack space, wall space for new racks, AC power circuits, and that network and low voltage power cables have been installed to the correct locations

and are properly labeled

c. Verify uplink cabling has been installed and labeled between telecommunications rooms if required, or that designated existing fiber is still unused and available for use
d. Create a remediation checklist for BOP staff if any deficiencies are found and follow up on completion prior to scheduled installation
e. Schedule Installation Date
f. Arrange for shipping of materials to site attention to appropriate receiver

2. Arrive on-site and obtain the necessary credentials and escort to customer work spaces:

   a. Conduct on-site equipment inventory per survey documentation and make arrangements to replace any damaged or missing equipment
   b. Install equipment into MDF, IDF, and telecommunications rooms, mail room and SIS Office: install any new racks or cabinets for network infrastructure if called for.
      i. Install network patch panels and route, dress, and terminate network cable into patch panels, labeling ports per label on cabling (including uplinks to other telecommunications rooms if applicable)
      ii. Install network switches and appropriate patch cables between patch panels and switches
      iii. Install power distribution equipment
      iv. Route, dress, and attach low voltage power equipment to power distribution equipment, labeling ports per label on cabling
      v. Document which user terminals and printers are attached to which ports on network switches equipment
      vi. Install network-enabled power switches and attach power distribution equipment; document which distributors are connected to which outlets for remote management
   c. Install battery backup(s) and attach network switches and remote power switches
   d. Attach battery backup(s) to AC electrical circuits
   e. Install any uplink adapters for existing fiber if needed and connect fiber using appropriate patch cables (where applicable)
   f. Test uplink cabling between telecommunications rooms with a cable tester to ensure proper termination and continuity of all pairs and that length does not exceed 300 feet; remediate problems immediately if possible, add to post-installation remediation checklist if necessary

3. At MDF location: Test broadband Internet Service Provider and Internet access using a laptop; ensure static IP address is assigned and documented; verify DNS entry has been created

   a. Install firewall and MP-VPN router or another designated head-end equipment
   b. Configure and connect MP-VPN router or another designated head-end equipment to broadband Internet Service Provider
   c. Work with remote support staff to test remote access to the network from the contractor data center; troubleshoot and remediate as needed

4. At each staff user terminal and printer location: BOP to provide a suitable space, power and network connection

a. Route, dress, and size/cut network cable and terminate with an appropriate modular connector for the type of cable installed (cat5e, cat6, etc.)
b. Re-connect port on patch panel to network switch when testing is finished
c. Connect power to user terminal and printer(s)
d. Power on user terminal and printer(s) to ensure they properly boot up into the client software
e. If full network access has been established, ensure contractor web application is loading and that the accounts can sign in
f. Work with BOP IT POC/Liaison to install a Color LaserJet MFP capable of 40 ppm and 1200 X 1200 dpi on the three computers on the contractor network located in the mail room and SIS Office which will be used to batch print inmate mail from an electronic file received from the contractor.

Training may occur before, during, or after the network installation. Contractor staff shall work with BOP IT POC/Facility Liaison to arrange on-site training. Training shall involve facility administration and mailroom and SIS staff to cover:

1. Management console access and account management
2. Reviewing scanned mail for approval or rejection
3. Handling inmate requests for printed copies of mail
4. Requesting that a piece of mail be held for additional time or forwarded to the facility
5. Discussion of the postal mail transition process
6. Ongoing support procedures

4. Work Environment

The work under this contract shall primarily be performed at the Federal Bureau of Prisons, the Federal Correctional Institution Beckley, West Virginia. Typically, the work week will be the standard 40 hours a week. Depending on the task, however, additional work may be required (e.g. deployments or maintenance during non-official hours to avoid disruption).

Contractor's price and efforts are based on the assumptions, terms, and conditions as stated below:

1. BOP provides an inmate data feed to include all active inmates at facilities where the email scanning system will be in use.
2. All required network cable runs shall be installed by BOP and shall be compliant with all applicable building codes and according to design layout as directed by contractor's initial site survey.
3. All required low voltage power cable runs shall be installed by BOP and shall be compliant with all applicable building codes and according to design layout as directed by contractor's initial site survey.
4. Adequate electrical power shall be available in the MDF, IDF, and other telecommunications rooms and other installation areas to support the required equipment identified during the initial site visit.
5. Adequate rack space and wall space shall be available for all required equipment.
6. BOP shall provide power, space, and location for the staff terminals and printer. Following contractor's installation and setup, BOP shall be responsible for printer furnishing and installing replacement ink/toner and paper.
7. Mail room, SIS staff and other users who require access will be able to reach the

contractor's website to log in to the contractor management console to review mail, process print requests, and perform other system management tasks.

8. BOP shall establish hours of operation and have staff available during these hours to support project activities. Current installation planning is based on the contractor being provided uninterrupted access to all necessary areas to during normal business hours (Monday-Friday between 7:30 AM – 5:30 PM). Contractor shall be given physical access and permission to work in the facility MDF room, IDF rooms, telecommunications rooms, administrative areas, and the planned user terminal and printer(s) areas.
9. All security access protocols and credentials shall be established for contractor access, as required, at least two (2) weeks prior to contractor arriving on site.
10. BOP will provide escorts for the contractor's staff who have access to all installation areas.
11. BOP shall identify the shipping location and be aware of deliveries ahead of schedule.
12. BOP shall provide a secure staging area for storage of received equipment, tools, and other project materials.
13. BOP shall provide a suitable ladder, extension ladder, or powered lift to access staged cable during installation where applicable; BOP shall provide authorization for use of BOP-owned ladders and powered lifts where applicable or to provide personnel authorized to use such equipment if contractor personnel are not authorized to use it directly.
14. BOP is not imposing requirements for the brands, types, model numbers, etc. user terminals, network switches, power controllers, power distribution equipment, and other components installed into the facility. But BOP may disapprove the use of specific equipment if it implicates or introduces information security or correctional security concerns or risks (e.g. introduce unauthorized cellular communications, do not meet industry manufacturing standards, etc.). The repair or maintenance of any equipment which stores BOP data and requires the removal from BOP or vendor premises must be preceded by advance notice and concurrence of BOP.
15. Contractor shall hold original physical inmate mail at the processing center for 30 calendar days from the date it was scanned. Individual pieces of mail identified by BOP staff may be selected to be pulled and held for longer periods if justified (for example for a court proceeding). Individual pieces of mail may be requested to be forwarded to a BOP facility or other designated location if necessary. After the holding period has expired, contractor shall dispose of the physical original mail by securely shredding it and optionally recycling the resulting shredded paper.
16. Contractor shall designate an existing, or establish a new, regional mailbox for the receiving of inmate mail. Mail received will be forwarded to a mail processing center. BOP shall be responsible to communicate the address of the designated mailbox to the public through its normal communications channels.

Any changes to site access hours and/or dates must be agreed to in advance and in writing by both the contractor and the BOP. Any delays outside of the contractor's control may require an extension of the project schedule and additional charges may be incurred. Additional charges shall be based upon the additional time on-site and all associated expenses, including but not limited to per diem, travel, housing, etc.

5. Work Environment

5.1 Required Skills and Proficiencies

The contractor resource team must have the following skills/abilities: compliance with DOJ IT

security requirements, off site mail scanning, contraband detection, records management, and investigative analysis.

5.2 Security and Clearance Requirements

The specific system that will be used in this instance is classified at the medium risk level. The corresponding clearance is MBI (Minimum Background Investigation).

Contractor security clearances, including the submission of security clearance forms, etc., shall be coordinated with the Government Task Manager prior to contract employee engagement at the BOP's Central Office. As determined by the GTM and/or Human Resource Security Specialist, clearances may require one or all of the following:

- DOJ-99 (name check);
- FD-258 (fingerprint check);
- Law Enforcement Agency checks;
- Vouchering of Employers over past five years;
- Resume/Personal Qualifications;
- OPM-329-A (Authority for Release of Information);
- Urinalysis Test (for detection of marijuana and another drug usage).

Note: If it is determined that a urinalysis test is required, it will be administered at the closest BOP site. If a test is positive for drug usage, the assigned individual(s) shall be excluded from performance of work for this requirement, and subject to the same security requirements, the contractor shall provide acceptable replacement staff.

The contractor shall employ effective safeguards and security controls to ensure that information associated with the work is protected from loss, damage, computer viruses or other destructive incidents. The safeguards employed should ensure that materials and services are secured in a manner that prevents tampering, sabotage or other means of deliberate alteration. This provision applies to all BOP information resources while under the control of the contractor.

The contractor shall participate in annual refresher training (provided by the Bureau of Prisons) for information security awareness and such participation will be documented by the BOP. Failure to participate may result in exclusion or removal from work on this contract and require the vendor to provide suitable replacements.

Loss Reporting: If contractor experiences a loss of Personally Identifiable Information (PII) provided by the BOP under the terms of this contract, the contractor will follow OMB loss reporting guidelines (OMB M-17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information") and notify the BOP COR within one (1) hour of discovering any actual or suspected breach of such data (i.e., Loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic). If within one (1) hour the vendor has been unable to make a report to the BOP COR, the contractor will call the DOJ Computer Emergency Readiness Team (DOJCERT) at 1-866-US4-CERT (1-866-874-2378) and make the report.

Inspection: To ensure compliance with the security requirements of this contract and/or in the event of an actual or suspected loss or breach of PII, the BOP reserves the right to inspect the

facilities wherein BOP inmate mail will be or is received, processed and stored. Such inspections may be unannounced and will be performed by the BOP COR and Information Security Programs staff.

6. Government-Furnished Equipment

6.1 Government Furnished Property (GFP)

The facility is responsible for rack space, power and network drops at all installation locations.

6.2 GOVERNMENT FURNISHED MATERIALS (GFM)

The government will provide access to government facilities at no cost to the contractor, as needed and on a schedule mutually agreeable to the contractor and the government based on guidance of the OST. BOP will provide for paper and ink for printer(s).

6.3 GOVERNMENT FURNISHED INFORMATION (GFI)

GFI will be provided at no cost to the contractor on an as-needed basis as defined by the solutions provider and OST.

7. SCOPE OF WORK

The contractor shall deliver and install a mail scanning system to meet the goals of the Bureau of Prisons' Office of Security Technology (OST). The contractor shall install, test, train staff and process incoming facility Inmate Mail.

BOP presently receives inmate mail at each correctional facility where BOP staff opens and inspects each piece of mail for contraband prior to delivery to inmates. Senders sometimes attempt to smuggle contraband into BOP facilities through inmate mail which has caused BOP staff to be exposed to dangerous contraband, drugs, and other substances which leads to potential health problems and other hazards.

To reduce risks for BOP mail room staff and reduce levels of contraband entering BOP facilities, BOP has requested postal mail scanning, processing, and electronic delivery services provided by contractor through the mail scanning system.

Through this service, the contractor shall receive inmate mail at one or more mail processing center(s). The mail shall be opened and scanned into a digital format, each record of mail shall be assigned to the appropriate inmate, digital copies of mail shall be made available for review by BOP staff. After review and approve/reject selections are made by BOP staff, inmates will receive their approved mail via a printed copy from BOP staff.

8. Project Management

The Bureau will appoint a Government Task Manager (GTM) for this project. The GTM is responsible for receiving all deliverables, inspecting, and accepting the services provided for this requirement in accordance with the terms and conditions of this contract, providing direction to the contractor which clarifies the contract effort, fills in details, or otherwise serves to accomplish the technical scope of work, evaluates performance, and certifies all invoices/vouchers for acceptance of the services furnished for payment.

Contractor shall provide an off-site Project Manager. The Project Manager shall lead the overall

execution of the activities in this SOW, including providing oversight of any tasks required by the SOW.

Additionally, the Project Manager shall ensure that:

1. Staff understand and work toward SOW objectives;
2. Tasks are staffed by appropriate, highly-qualified personnel; and
3. All project management issues are communicated to and coordinated with the GTM. An initial project plan shall be submitted to the GTM for review and approval within 30 days of award. Status reporting on tasks shall provide accurate information concerning:

    i. Project Progress
    ii. Planned activities for the next reporting period
    iii. Issues that are affected, or are expected to affect, the project schedule
    iv. Any items that might enhance, or detract from, the overall success of the project

9. Period of Performance

The contractor will provide this support for a period of one (1) year from completion of installation.

10. Travel

Travel between contractor facilities and FCI Beckley will be required and as mutually agreed upon and in accordance with the effort.

11. Key Personnel

The requested Key Personnel for this SOW is one vendor Project Manager.

The contractor shall immediately remove any personnel determined unsuitable in compliance with security provisions or found to represent a threat to the safety of government records, government employees, or other contractor staff. Replacement of key personnel is subject to prior written approval of the GTM.

The contractor agrees that during the first ninety (90) calendar days of the contract performance period no key personnel substitutions will be permitted unless such substitutions are required by the Government, or necessitated by an individual's sudden illness, death or termination of employment. All requests for substitutions must provide a detailed explanation of the circumstances necessitating the proposed substitution, a resume for the proposed substitute, and any other information requested by the GTM to aid in the process of approving or disapproving the proposed substitute. Proposed substitutions shall have the same (or better) qualifications and experience as the personnel being replaced.

Past the ninety (90) day period, the contractor shall advise the GTM no later than 30 days in advance of any required replacement of key personnel. All requests for substitutions must provide a detailed explanation of the circumstances necessitating the proposed substitution, a resume for the proposed substitute, and any other information requested by the GTM to aid in the process of approving or disapproving the proposed substitute. Proposed substitutions shall have the same (or better) qualifications and experience as the personnel being replaced.