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

1. REQUISITION NUMBER	PAGE 1 OF 34

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			15JA0523Q00000015	01/19/2023

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (*No collect calls*)	8. OFFER DUE DATE / LOCAL TIME
			02/06/2023 11:00 ET

9. ISSUED BY — CODE 15JA05

Executive Office for United States Attorney
175 N Street NE
6th Floor
Washington, DC 20530-0021

10. THE ACQUISITION IS — ☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % 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: 561492
SIZE STANDARD: $16.5M

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 15JA38

U.S. Attorneys Office District of Massachusetts
John J Moakley Courthouse
1 Courthouse Way Suite 9200
Boston, MA 02210

16. ADMINISTERED BY — CODE 15JA05

Executive Office for United States Attorney
175 N Street NE
6th Floor
Washington, DC 20530-0021
Mateaus.Flournoy@usdoj.gov

17a. CONTRACTOR/ OFFEROR — CODE ____ FACILITY CODE ____

TELEPHONE NO.

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

18a. PAYMENT WILL BE MADE BY — CODE 15JA38

U.S. Attorneys Office District of Massachusetts
John J Moakley Courthouse
1 Courthouse Way Suite 9200
Boston, MA 02210

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
	Grand Jury and Deposition Court Reporting Services for the U.S. Attorney's Office, District of Massachusetts Locations: Boston, Springfield, and Worcester Period of Performance: 4/1/2023 - 3/31/2028 Contract Type: Time-and-Materials **Questions due to the Contracting Officer NLT 1/27/2023,11:00 a.m. EST, via email mateaus.flournoy@usdoj.gov** See Continuation Sheet(s) (*Use Reverse and/or Attach Additional Sheets as Necessary*)				

25. ACCOUNTING AND APPROPRIATION DATA

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

☒ 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

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ 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*)

30b. NAME AND TITLE OF SIGNER (*TYPE OR PRINT*)	30c. DATE SIGNED	31b. NAME OF THE CONTRACTING OFFICER (*TYPE OR PRINT*)	31c. DATE SIGNED
		Mateaus Flournoy	

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

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	Labor PSC: R606 **Line Period of Performance:** 04/01/2023 - 03/31/2024 Base Period	0	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Materials PSC: R606 **Line Period of Performance:** 04/01/2023 - 03/31/2024 Base Period	0	EA	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003	**If you are requesting travel reimbursement, please quote on this line item.** All travel will be in accordance with Federal Travel Regulations (FTR). PSC: R606 **Line Period of Performance:** 04/01/2023 - 03/31/2024 Base Period	1	LT	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	Labor PSC: R606 **Line Period of Performance:** 04/01/2024 - 03/31/2025 Option Period	0	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002	Materials PSC: R606 **Line Period of Performance:** 04/01/2024 - 03/31/2025 Option Period	0	EA	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1003	**If you are requesting travel reimbursement, please quote on this line item.** All travel will be in accordance with Federal Travel Regulations (FTR). PSC: R606 **Line Period of Performance:** 04/01/2024 - 03/31/2025 Option Period	1	LT	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001	Labor PSC: R606	0	HR	$_____	$_____

	Line Period of Performance: 04/01/2025 - 03/31/2026 Option Period				
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002	Materials PSC: R606 **Line Period of Performance:** 04/01/2025 - 03/31/2026 Option Period	0	EA	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2003	**If you are requesting travel reimbursement, please quote on this line item.** All travel will be in accordance with Federal Travel Regulations (FTR). PSC: R606 **Line Period of Performance:** 10/01/2024 - 09/30/2025 Option Period	1	LT	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001	Labor PSC: R606 **Line Period of Performance:** 04/01/2026 - 03/31/2027 Option Period	0	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002	Materials PSC: R606 **Line Period of Performance:** 04/01/2026 - 03/31/2027 Option Period	0	EA	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3003	**If you are requesting travel reimbursement, please quote on this line item.** All travel will be in accordance with Federal Travel Regulations (FTR). PSC: R606 **Line Period of Performance:** 04/01/2026 - 03/31/2027 Option Period	1	LT	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001	Labor PSC: R606 **Line Period of Performance:** 04/01/2027 - 03/31/2028 Option Period	0	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002	Materials PSC: R606 **Line Period of Performance:** 04/01/2027 - 03/31/2028 Option Period	0	EA	$_____	$_____

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4003	**If you are requesting travel reimbursement, please quote on this line item.** All travel will be in accordance with Federal Travel Regulations (FTR). PSC: R606 **Line Period of Performance:** 04/01/2027 - 03/31/2028 Option Period	1	LT	$_____	$_____

Section 3 - Contract Clauses

A.1 ADDENDUM TO FAR 52.212-4, Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2021) - Alternate I (Nov 2021)

The terms and conditions for the following clauses are hereby incorporated into this solicitation and resulting contract as an addendum to FAR clause 52.212-4.

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)
52.224-2	Privacy Act (Apr 1984)	
52.216-32	Task-Order and Delivery-Order Ombudsman (Sep 2019)	(a)name: "Tara Jamison" (a)address: "Director, Office of Acquisition Management" (a)telephone: "(202) 616-3754" (a)email: "tara.jamison@usdoj.gov"
52.212-4 Alt I	Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2021) - Alternate I (Nov 2021)	
52.212-5	Contract Terms and Conditions Required To Implement Statutes or Executive Orders-Commercial Products and Commercial Services (May 2022)	(b)(4): "X" (b)(7): "X" (b)(8): "X" (b)(9): "X" (b)(14)(i): "X" (b)(22)(i): "X" (b)(27): "X" (b)(28): "X" (b)(29): "X"

Clause	Title	Fill-ins (if applicable)
		(b)(30)(i): "X" (b)(31)(i): "X" (b)(32)(i): "X" (b)(33): "X" (b)(34): "X" (b)(35)(i): "X" (b)(44): "X" (b)(47)(i): "X" (b)(49)(i): "X" (b)(58): "X" (b)(61): "X" (c)(1): "X" (c)(2): "X" (c)(7): "X" (c)(8): "X"
52.217-9	Option to Extend the Term of the Contract (Mar 2000)	(a) Period of Time: "30 days" (a) Days: "30" (c): "66 months"
52.244-2	Subcontracts (Jun 2020)	
52.216-18	Ordering (Aug 2020)	(a)From Date: "4/1/2023" (a)To Date: "3/31/2028"
52.216-19	Order Limitations (Oct 1995)	(a): "$1.00" (b)(1): "$3000.00" (b)(2): "$3000.00" (b)(3): "five (5)" (d): "30"
52.216-22	Indefinite Quantity (Oct 1995)	
52.216-27	Single or Multiple Awards (Oct 1995)	
52.217-8	Option to Extend Services (Nov 1999)	Period of Time: "30 days"
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper (May 2011)	

Clause	Title	Fill-ins (if applicable)
52.204-21	Basic Safeguarding of Covered Contractor Information Systems (Nov 2021)	
52.204-19	Incorporation by Reference of Representations and Certifications (Dec 2014)	
52.204-18	Commercial and Government Entity Code Maintenance (Aug 2020)	
52.204-13	System for Award Management Maintenance (Oct 2018)	
52.253-1	Computer Generated Forms (Jan 1991)	
52.224-1	Privacy Act Notification (Apr 1984)	

EOUSA AI-10-1E Federal Grand Jury Court Reporter Security Requirements (December 2015)

Federal Grand Jury Court Reporter Security Requirements (December 2015)
1. Grand Jury (GJ) Security.

The work to be performed under this contract will involve access to sensitive information subject to the rules of 6(e) of the Federal Rules of Criminal Procedures. The adequate and continual protection of the information (hereafter referred to as GJ information which includes GJ testimony, discussions, exhibits, etc.) and how it is used, shared, and stored, is extremely important. The secrecy and ultimate security of the GJ information and proceedings is vital to the performance of the U.S. Attorney's Office (USAO) and the Court. A failure to protect GJ information by anyone involved may be considered a breach of contract, breach of agreement, a violation of standards, and perhaps, an unlawful act. Disclosures of matters appearing before the GJ other than its deliberations, including the vote of any juror may be made available to the attorneys for the Government to use in the performance of their duties. Otherwise, a juror, attorney, interpreter, stenographer, or operator of recorded testimony may disclose matters appearing before the GJ only when so directed by the Court.

a. Violations of the Terms and Conditions. Unauthorized use of GJ information or material could subject the disclosing individual to contempt of court penalties and other applicable penalties. Sensitive information may include, but is not limited to: data found within GJ information, informant and witness information, investigative material, tax information, medical information, computer systems information, Privacy Act (as amended) information, Department of Justice proprietary information, or Federal information that is not releasable to the general public and/or under the guidelines of the Freedom of Information Act (FOIA). Unauthorized duplication or disclosure of the data and other information to which the Contractor may have access as a result of this contract is prohibited by Public Law and is subject to criminal penalties.

b. Court Reporter Security Training. The Contractor is responsible for ensuring all employees approved to work with and have access to GJ information and materials are familiar with - and required to follow - continuing responsibilities and the security requirements as outlined in the contract.

c. Failure to Meet Security Requirements. Should the Government determine that the Contractor has failed to comply with the security requirements of the contract, the Contractor may be held responsible, as a minimum, for all reasonable and necessary costs incurred by the Government to: (a) provide coverage (performance) through assignment of individuals employed by the Government or third parties in cases where absence of contract personnel would cause a delay in the proceedings, a security threat, and/or disrupt a DOJ program, and (b) conduct security investigations in excess of those which would otherwise be required. Nothing in this clause shall require the Contractor to bear costs involved in the conduct of security investigations for the replacement of an employee who becomes incapacitated, severely ill, or deceased. Any violation of this requirement subjects the Contractor, subcontractor, employees, etc., to certain penalties including, but not limited to termination of the contract, issuance of a cure notice for less serious violations, and being held in Contempt of Court for failing to safeguard federal GJ information.

d. List of Contractor's Employees. The Contractor shall submit to the USAO a list of the names of all principals, staff members, and regular employees requiring access to the work performed under the contract. This includes personnel of the principal Contractor and any subcontractor(s).

e. Sub-Contractors. The Contractor must ensure that any sub-contractor furnishing supplies and services which will involve access to GJ materials complies with the security requirement of the contract and has been approved by the Government.

2. Personnel Security.

The USAO will process the background investigations for GJ court reporter(s) identified by the Contractor to the USAO to perform work under this contract. However, this background investigation does not replace or supersede the employer's responsibility to sufficiently screen and eliminate unsuitable applicants and to take all necessary steps to ensure only qualified persons perform services.

a. Residency Requirement. All Contractor employees assigned to this contract and working within the United States shall meet the DOJ Residency Requirement. The Residency Requirement states that, for 3 of the 5 years immediately prior to applying for a position, the individual must have: (1) resided in the United States; (2) worked for the United States overseas in a Federal or military capacity; or (3) be a dependent of a Federal or military employee serving overseas.

b. Sufficient Personnel. The Contractor must maintain a sufficient number of approved personnel to execute the contract. The Contractor is not to assign GJ court reporting duties unless, and not until, the COR or representative of the USAO provides notification in writing that the employee has been granted the necessary security approval to perform GJ court reporting duties as outlined under this contract.

c. Suspension or Revocation of Access Approval. Access to GJ information can be suspended or revoked for cause at any time by the Contractor and/or the COR.

d. Required Suitability Approval and Background Investigation. Contractor employees must receive a security approval based upon: (1) A Government conducted Moderate Background Investigation (MBI) or higher background investigation, and (2) Favorable adjudication. A security waiver may be requested by the contractor prior to completion of a background investigation when necessary and as outlined by the Government. The Contractor will ensure the required security background investigation forms are completed and submitted. The intent and purpose of the investigation is to preclude the assignment of any individual who poses a threat to the Government or successful contract completion due to past unlawful or inappropriate behavior.

e. Background Investigation Process and Forms. The USAO will initiate the Electronic Questionnaires for Investigations Processing (e-QIP) upon receipt of the Contractor's or Contractor employee applicant's name and other information. The applicant will complete sign and submit e-QIP forms to the USAO/POC on the same day the signature pages are signed. The USAO will have 5 days to forward the forms to SEMS/PERSEC. Waiver package will include the following: e-QIP package, and the following forms; Certification, General Release, Medical Release, and Fair Credit pages, DOJ-555 Disclosure & Authorization Pertaining to Consumer Reports, Standards of Conduct Form, OF-306 Declaration for Federal Employment, Foreign Nat'l Relatives or Associates Form (if applicable), employment vouchers (2 if most recent employment is less than 2 years; 1 if most recent employment is more than 2 years), and fingerprints cards (form FD 258) or results. The forms shall be submitted to the SEMS/PERSEC upon completion of e-QIP. The Government may request additional security forms, or additional information, if the contract employee's security forms contain information which requires clarification (i.e. information concerning criminal history, financial problems, citizenship of family members, etc.)

3. Protecting the GJ Information.

a. Contractor's GJ Information Processing Site. The location selected by the Contractor and approved by the Government (USAO) for the processing, storage, and preparation of GJ information must be determined in advance of commencement of work. The location for processing is not to be changed or modified without the prior consent of the USAO unless extenuating circumstances or emergencies demand relocation. In such cases, the Contractor must coordinate with the CO or COR. The means and methods for transfer or relocation of any GJ material will also be coordinated and approved by the USAO in advance.

b. Contractor Physical Security Requirements. The physical security standards are extremely important to the Government. The Contractor has a duty and legal obligation to ensure that all physical security measures, practices, and policies are strictly followed and any deviation must be coordinated and approved by the CO. If the Contractor and the CO mutually agree to only using USAO provided space in lieu of the Contractor's own space, then the physical security requirements of subparagraphs 3d, 3e, and 3f contained in this Annex do not apply.

c. Designated Room or Space. The Contractor will have and use a designated room or space to process, proofread, and store GJ material. When a dedicated room is not feasible or practical, the Contractor must ensure that the room or space used

meets or exceeds the required physical security controls, protection standard, and has been pre-approved by the USAO. The requirement is to prevent unauthorized access to the GJ material. The GJ material must be protected against unauthorized disclosure and viewing by other tenants, co-business employees, and unauthorized persons (family, friends, customers, etc.)

d. Door and Locking Hardware. The designated room or space must have an operational door and lock which prevents unauthorized entry into the room or space. Doors must be closed and locked when the room is not in use and when the room is vacated for short periods of time. (The alarm is also to be set if the user is not expected to return within 5 minutes.) The Contractor must have total key control and accountability. Only persons who have been approved to access the GJ information are to possess a key to the pre-approved room or space. The Contractor must ensure that no one is allowed unsupervised and/or unrestricted access to the space where the GJ material is stored unless approved by the government.

e. Windows and Emergency Exits. Windows are allowed provided they are locked and the pre-approved room or space is alarmed and monitored. Emergency exits are allowed and if present, must be alarmed.

f. Intrusion Alarm and Monitoring Service. The designated room or workspace where the material is stored must be equipped with an Intrusion Detection System (IDS) that is connected to a central monitoring station. The Contractor will provide the USAO a copy of the call or notification list and responder protocols on alarm annunciation. The Contractor must notify the USAO within 2 business days of any alarm activation. The notification must include the time and date of the alarm activation, an explanation of cause if known, incident details including the identification of any missing GJ material (devices, storage media, paper, etc.), and a copy of the activity log from the monitoring station. The Contractor must provide the USAO with a copy of the IDS monitoring history log quarterly (every 90 days) and as requested by the USAO. Knowledge of the code number used to program, arm and/or disarm the system must be limited to those who have Government approved access to the GJ material. Remote monitoring services are not allowed to have the code number. The alarm must be set to "armed" whenever the room is not in use. Short absences of less than 5 minutes in duration do not require the alarm to be set to "armed." The alarm system is to be tested at least once per year to ensure it is functioning properly and the desired response occurs.

g. Contractor's GJ Information Storage. The GJ material must be stored only in USAO approved storage container(s). The container must be either equipped with an approved lock or locking mechanism. The combination of a lock shall be restricted to those who have a need-to-know the information and have a security approval. An entry/closure log shall be maintained to record each time a security container is opened and closed and by whom. Any combination will be changed when a person with knowledge of the combination no longer needs or is approved for access, or upon compromise of the combination. End of day security checks shall be performed within the contract facility to ensure that precautions are taken to protect GJ material. The Contractor or an approved contractor's employee is to make periodic checks to ensure all GJ material has been properly stored. The periodic security checks shall be annotated in a log or journal. The storage container must be locked when not in use. A storage container that can be easily moved or illegally removed should be mounted or anchored to the floor or wall. It is recommended that the Contractor use a GSA-approved container whenever possible. A Class 3, 4, 5, or 6 is sufficient.

h. Use and/or Sale of Grand Jury Information and Transcripts. Grand Jury transcripts may not be sold or made available to anyone other than the Government at any time under any circumstances.

i. Personal Identity Verification (PIV) of Contractor Personnel. The Contractor shall comply with agency personal identity verification procedures that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) Guidance M-05-24, and Federal Information Processing Standards Publication (FIPS Pub) Number 201. The Contractor's employees who require physical access to the USAO or to USAO controlled information technology or device may be required to be issued and use a PIV Card issued in accordance with HSPD-12. The Contractor must comply with access procedures, policies, and security requirements if and/or when physical and/or virtual access is required to a federally-controlled facility or information system(s).

4. Information Technology (IT) Equipment.

The Contractor must ensure that all devices used to process, store, record, and duplicate GJ information meet the requirements of the USAO and have been approved by the USAO for use. (IT equipment refers to computers, recording devices, scanners, printers, laptops, copiers, and all other devices used to process and/or store GJ information.) When processing GJ Information the computer/ laptop must be used as standalone with internet connectivity disabled. The computer/laptop can only be the internet enabled during the timeframe of transmitting files when using file exchange software. Administrative controls over all approved IT devices and settings used for this contract are to be restricted and approved by the Government.

a. Approval and Marking Approved Devices. The Contractor will provide to the USAO the serial numbers of all IT devices used in the performance of this contract over the term of the contract in advance of their use. The approved devices will be clearly marked and labeled as containing federal GJ information or FGI. The devices will also be marked as containing controlled unclassified information (CUI).

b. IT Processing, Transmitting, and Storing GJ. The GJ information processed and stored on a Contractor owned or provided device, must be used solely for the purpose of processing and/or storage of GJ information. Data must be encrypted, including

additional peripherals or devices such as a flash drive, thumb drive, and/or external storage. In addition to encryption, any temporary file(s) created by the operating system or user must be deleted after each use. Any and all portable devices or removable media used for GJ must be stored in the approved security container(s) when not in use. The contractor is required to establish an internal process for backing-up GJ information. The USAO can provide physical storage of backed-up GJ information for the Contractor upon request or necessity. The GJ information may not be processed or backed-up on a commercial mainframe, data server, cloud, or with a data warehousing service.

c. Modification and/or Changes to Approved IT. Any modification, repair, or replacement of any IT device used to process and/or store GJ information must be approved by the USAO. Only individuals approved by the USAO are authorized to repair or modify any previously approved device or equipment used for the processing and storage of GJ information.

d. Damaged or Defective Storage Devices. The Contractor will turn over any and all damaged or defective storage media used for processing and/or storing GJ information to the USAO throughout the term of the contract.

e. Access to IT. Access to IT used for, and any products created from or containing, GJ information must be restricted to individuals approved, by name, by the USAO or the Court. Equipment must be turned off and sufficiently secured when not in use even for short periods of time during normal business or working hours as well.

f. IT Storage Device No Longer Used and at End of Contract. When a storage device including a laptop, removable hard drive, flash drive, DVD, etc., is no longer needed during the course of the contract or upon termination of the contract, storage devices used will be given to the COR.

g. Security of Systems and Data including Personally Identifiable Information (PII) Data**.** *The term "PII," as defined in OMB Memorandum M-07-1616 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.*

Standard A (Storing PII on less than 25 Individuals). *This standard applies to Contractors handling electronically stored information containing PII on less than 25 individuals in connection with this contract. Refer to Standard B below if more than 25 individuals.)*

(1) Keep the computer in a safe place, such as a locked office or other location with limited access, when not in use.

(2) Mark any laptop with contact information in case of loss to facilitate its safe return.

(3) Keep the operating system, security, and application software used in connection with any computer updated on a regular basis.

(4) Use anti-viral software.

Standard B (Storing PII on more than 25 Individuals). *This standard applies to Contractors handling electronically stored information containing PII on more than 25 individuals in connection with this contract. Refer to Standard A above if less than 25 individuals.)*

(1) The work to be performed under this contract requires the handling of data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel. For all systems handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including, but not limited to, all Executive Branch system security requirements (*e.g.*, requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 2640.2F.

(2) The Contractor shall provide DOJ access to and information regarding the Contractor's systems when requested by the Department, in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, Federal Information Security Management Act (FISMA) data reviews, and access by the DOJ Office of the Inspector General for its reviews. The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the CO certifying the following requirements:

(a) Laptops must employ hard drive encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 validated product; (FIPS 140-2 is available on line at:

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. Instructions for obtaining a paper copy of FIPS 140-2 are outlined in the document as well.)

(b) The Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;

(c) Laptop will utilize anti-viral software;

(d) The Contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is sensitive information unless designated as non-sensitive by the Department. Contractor-owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, shall not be removed from DOJ facilities unless encrypted using a NIST FIPS 140-2 validated product;

(e) When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;
(f) Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;

(g) Rules of behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and PII; and

(h) All DOJ data will be removed from Contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractor's project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work.

h. Data Security Breach Reporting. By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified above, in the event of 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), the contractor will immediately (and in no event later than within one hour of discovery) report the breach to the CO and COR.) If the data breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, the contractor shall call the EOUSA Security Operations Center at (803) 705-5533 within one hour of discovery of the breach. The Contractor shall also notify the CO as soon as possible during regular business hours.
i. Personally Identifiable Information Security Breach Notification. The Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual who's PII has, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department, and shall not proceed until the Department 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 the Contractor shall be coordinated with and be subject to the approval of the Department. The Contractor assumes full responsibility for taking corrective action consistent with the Department's Data Breach Notification Procedures, which may include offering credit monitoring when appropriate.
j. Pass-through of IT Security Requirements to Subcontractors. The requirements set forth above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the Contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the Contractor.

5. Destruction Requirements.

The Contractor must destroy by cross-cut shredding that meets or exceeds National Security Agency/Central Security Service (NSA/ CSS) Level 4 requirement or by burning all waste documents associated with any GJ proceeding. Or as an alternative, the Contractor may elect to transport GJ waste (i.e., drafts, notes, working papers, CDs, DVDs, typewriter ribbons, copies of GJ information, and other material which is no longer needed) to the USAO for destruction. When GJ information and related working papers are no longer needed during the course of the contract or upon termination of the contract, the original documents and tapes shall be returned to the USAO. This includes storage devices such as hard drives (internal or external), flash drives, CDs or DVDs, memory cards, and other storage media used to store GJ information.

a. Destruction methods and equipment must be approved by the COR in writing.
b. The Contractor is not authorized to destroy any GJ material or replace any electronic storage devices without prior approval from the COR or USAO representative in writing.
c. When an electronic storage device is no longer needed during the course of the contract and/or upon termination of the contract, the storage devices used will be given to the COR for destruction by the Government.

6. Duplication of GJ Information.

The GJ information may not be copied without the approval of the COR or USAO. If duplication of GJ information is required, the Contractor will only produce the number of copies needed or requested. Copiers used to duplicate GJ information must have security features approved by the COR which may include an on-demand or automatic overwrite feature. Running the on-demand overwrite function of the copier immediately after copying the GJ material is encouraged.

7. Delivery, Shipping, and Packaging GJ Information to USAO.

The GJ information must be protected from unauthorized and/or inadvertent disclosure at all times. This includes during shipment and electronic transfer or delivery to the USAO. The Contractor must either (1) hand carry, (2) use government approved messengers/ messenger service, (3) use the U.S. Postal Service from an official post office or picked-up by a U.S. Postal employee, (4) use an overnight mail service with the online capability to track packages shipped and delivered, or (5) use a secure government provided file exchange system. The USAO must approve the method(s) before the Contractor can use a given method of delivery. The Contractor must maintain a delivery or shipping log, double-wrap GJ information (envelope within an envelope or box within a box, etc., with the inner packaged marked GJ Information), and must notify the USAO in advance when GJ information is shipped or is electronically transmitted by the Government's file exchange system to the USAO. The use of curbside collection is strictly prohibited when mailing packages containing GJ information.

a. Packing Materials. Grand Jury Information and Transcripts must be double wrapped in two opaque layers; both of which provide reasonable evidence of tampering and which conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, and must clearly display the following warning notice:

GRAND JURY MATERIAL ENCLOSED
TO BE OPENED BY AUTHORIZED PERSONNEL ONLY
UNAUTHORIZED VIEWING OF THIS MATERIAL IS A VIOLATION OF THE LAW

The outer enclosure shall also clearly identify the address of both the sender and the intended recipient except that no markings to indicate that the contents contain grand jury information shall be visible.

b. Using the U.S. Postal Service. When documents cannot be personally transported between authorized recipients, or by official couriers or messengers, the transmittal of GJ information and related working papers shall be transferred by the U.S. Postal Service Certified Mail with a return receipt. Facsimile is not permitted.

c. Using a Commercial Overnight Service. When an urgent requirement exists for overnight delivery of GJ information, the USAO may authorize the use of an overnight delivery service. Any such delivery service shall be U.S. owned and operated, provide automated in-transit tracking of the package, and ensure package integrity during transit. The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verification of the correct mailing address. The release signature block on the receipt label must not be waived under any circumstances. The use of external (street side) collection boxes is prohibited. The package must be physically handed to a uniformed employee of the delivery service and immediately registered into the automated tracking system.

d. Messenger/Courier Services. For the purpose of this contract, any messenger or courier service used by the Contractor is considered a sub-contractor or the contractor's employee and all security requirements apply.

e. File Exchange System. The use of the Government's file exchange system is an efficient and secure means of exchanging materials with the USAO. The CO will provide the file exchange system details, requirements, and procedures to the Contractor upon request.

8. Transportation of and/or Transmitting GJ Information to USAO.

The GJ information is vulnerable to loss, tampering, and even theft during transportation. Equipment used for recording and processing GJ information is also vulnerable to criminal activity. The Contractor must provide and ensure safe transport of GJ material from point of origin directly to facility previously approved by the USAO for the processing and/or storage of GJ information. Local delivery and courier services contracted by the Contractor to deliver GJ information to the USAO must be known to and approved by the USAO.

9. Site Security Reviews and Governmental Oversight.

The COR or a designated USAO representative may conduct an initial and/or recurring security review(s) of the Contractor's location(s) where GJ information is or is to be processed and/or stored.

a. Preliminary Security Review. Prior to the award of a GJ Court Reporter contract, the COR may assess the ability and feasibility of the Contactor to provide and sustain the security requirements contained in the Statement of Work. An inability to provide and sustain the security requirement, in whole or in part, could be cause for disqualification or warrant special arrangements with the USAO to process and store the materials within USAO space and control vice in a commercial facility and/or residence.

b. Initial and Periodic Security Review. At the time of award and periodically thereafter as determined by the COR and/or at the request of the Contractor, the COR or other designated USAO representative may complete an on-site security reviews of the Contractor's facility. The areas subject to inspection include all primary and secondary GJ processing locations and storage locations including proofreading sites. The purpose for the review is to ensure that all of the security requirements

and expectations outlined in the Contract are in place and sufficient to ensure the proper protection of the GJ information. The Government's *Federal Grand Jury Court Reporter Contract Security Review Checklist* is included in this Contract and will be used by the Government to complete the site security reviews. The results of the security review could result in termination for cause, issuance of a cure notice, or other remedial action as determined appropriate by the Government.

c. Essential Security Information. The Contractor is required to provide the Government (prior to the start of work and update as needed) the following specific essential security information:

1) The business name and owner.
2) The contactor's physical and mailing address(es) and telephone number(s).
3) A list of any other United States Attorney Offices (USAOs) supported by the contractor.
4) The list of government approved court reporter(s) to perform work under the contract along with the form and date of their latest completed background investigation or the date of temporary waiver if provided by the government; if a national security clearance is also required, list the level and date of clearance.
5) The business name(s), address(es) and telephone number(s) of any sub-contractor(s) including proofreaders.
6) The name(s) of the government approved sub-contractor personnel to perform work under the contractor along with the form and date of their completed background investigation or temporary waiver if provided by the government; if national security clearances are required by the contract, the level and date of clearance.
7) Processing and storage location information:
8) The physical address(es) where grand jury materials will be processed, reviewed and stored by the contractor.
9) Indicate the type of facility (commercial leased space, private residence, etc.).
10) The names of individuals having access (possess alarm code, key, etc.) to the location (room or area) approved by the government for processing and/or storing grand jury information. If it is a private home or a multi-use business location, also describe how the material will be safeguarded against unauthorized, inadvertent, or illegal access by other residents, employees, and guests.
11) The alarm service company name, address, and telephone number.
12) The list of government approved IT processing and storage device(s) consisting of make, model, serial number, and the names of approved users; also indicate who has "administrative privileges and/or rights" over the devices.
13) The location, brand, and model of safe(s) used to store grand jury materials and the date the combination was last changed.
14) The names of individuals having physical access to the government approved contractor maintained safe(s) and also those knowing each safe's combination.
15) The method of delivering or transporting grand jury materials to the USAO.

10. Reporting Requirements.

a. It is the Contractor's obligation to report any incident or situation that places the GJ information at risk of loss, unauthorized disclosure, unapproved review, theft, or tampering. It is essential that this be recorded, the COR informed, and measures taken to immediately minimize or mitigate risk(s). If a theft or break-in, or attempt thereof occurs, the local police are to be contacted. A copy of the police report is to be provided to the COR as soon as available.

b. The Government may request and require the execution of an inadvertent and/or unauthorized disclosure agreement as needed and appropriate. The COR will advise when and how this will be accomplished and will provide an agreement form when appropriate. In essence, the agreement provides notice that access was not approved and/or allowed and any further unauthorized disclosure could subject the individual to certain civil and criminal penalties, including being held in contempt of court.

(end of clause)

2852.201-70 Contracting Officer's Representative (COR) (NOV 2020)

(a) Mr./Ms. Catherine White of USAO-Massachusetts , 1 Courthouse Way, Suite 9200 , (617) 748-3237 , is hereby designated to act as Contracting Officer's Representative (COR) under TBD , for the period of 4/1/2023-3/31/2028 (specify the performance period of the contract that the designation covers).

(b) Performance of work under this contract is subject to the technical direction of the COR identified above, or another representative designated in writing by the Contracting Officer. The term "technical direction" includes, without limitation, the following:

(i) Receiving all deliverables;

(ii) Inspecting and accepting the supplies or services provided in accordance with the terms and conditions of this contract;

(iii) Clarifying, directing, or redirecting the contract effort, including shifting work between work areas and locations, filling in details, or otherwise serving to accomplish the contractual statement of work to ensure the work is accomplished satisfactorily;

(iv) Evaluating performance of the Contractor; and

(v) Certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.

(c) The COR does not have the authority to issue direction that:

(i) Constitutes a change of assignment or work outside the contract specification/work statement/scope of work.
(ii) Constitutes a change as defined in the clause entitled “Changes” or other similar contract term.
(iii) Causes, in any manner, an increase or decrease in the contract price or the time required for contract performance;
(iv) Causes, in any manner, any change in a term, condition, or specification or the work statement/scope of work of the contract;
(v) Causes, in any manner, any change or commitment that affects price, quality, quantity, delivery, or other term or condition of the contract or that, in any way, directs the contractor or its subcontractors to operate in conflict with the contract terms and conditions;
(vi) Interferes with the contractor's right to perform under the terms and conditions of the contract;
(vii) Directs, supervises, or otherwise controls the actions of the Contractor's employees or a Subcontractor's employees.
(d) The Contractor shall proceed promptly with performance resulting from the technical direction of the COR. If, in the opinion of the Contractor, any direction by the COR or the designated representative falls outside the authority of (b) above and/or within the limitations of (c) above, the Contractor shall immediately notify the Contracting Officer.
(e) Failure of the Contractor and Contracting Officer to agree that technical direction is within the scope of the contract is a dispute that shall be subject to the “Disputes” clause and/or other similar contract term.
(f) COR authority is not re-delegable.
(End of Clause)

EOUSA AI-10-1D Continuing Contract Performance During a Pandemic Influenza or other National Emergency (October 2007)

Continuing Contract Performance During a Pandemic Influenza or other National Emergency (October 2007)

During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation.

The types of actions a federal contractor should reasonably take to help ensure performance are:

Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.

Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.

Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.

Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.

Establish communication processes to notify employees of activation of this plan.

Integrate pandemic health crisis response expectations into telework agreements.

With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.

Determine how all employees who may telework will communicate with one another and with management to accomplish work.

Practice telework regularly to ensure effectiveness.

Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.

Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractors notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the Federal Acquisition Regulations.

(end of clause)

2852.233-70 Protests Filed Directly with the Department of Justice (Jan 1998)

(a) The following definitions apply in this provision:
(1) "Agency Protest Official" means the official, other than the contracting officer, designated to review and decide procurement protests filed with a contracting activity of the Department of Justice.
(2) "Deciding Official" means the person chosen by the protestor to decide the agency protest; it may be either the Contracting Officer or the Agency Protest Official.
(3) "Interested Party" means an actual or prospective offeror whose direct economic interest would be affected by the award of a contract or by the failure to award a contract.
(b) A protest filed directly with the Department of Justice must:
(1) Indicate that it is a protest to the agency.
(2) Be filed with the Contracting Officer.
(3) State whether the protestor chooses to have the Contracting Officer or the Agency Protest Official decide the protest. If the protestor is silent on this matter, the Contracting Officer will decide the protest.
(4) Indicate whether the protestor prefers to make an oral or written presentation of arguments in support of the protest to the deciding official.
(5) Include the information required by FAR 33.103(d)(2):
(i) Name, address, facsimile number and telephone number of the protestor.
(ii) Solicitation or contract number.
(iii) Detailed statement of the legal and factual grounds for the protest, to include a description of resulting prejudice to the protestor.
(iv) Copies of relevant documents.
(v) Request for a ruling by the agency.
(vi) Statement as to the form of relief requested.
(vii) All information establishing that the protestor is an interested party for the purpose of filing a protest.
(viii) All information establishing the timeliness of the protest.
(c) An interested party filing a protest with the Department of Justice has the choice of requesting either that the Contracting Officer or the Agency Protest Official decide the protest.
(d) The decision by the Agency Protest Official is an alternative to a decision by the Contracting Officer. The Agency Protest Official will not consider appeals from the Contracting Officer's decision on an agency protest.
(e) The deciding official must conduct a scheduling conference with the protestor within five (5) days after the protest is filed. The scheduling conference will establish deadlines for oral or written arguments in support of the agency protest and for agency officials to present information in response to the protest issues. The deciding official may hear oral arguments in support of the agency protest at the same time as the scheduling conference, depending on availability of the necessary parties.
(f) Oral conferences may take place either by telephone or in person. Other parties may attend at the discretion of the deciding official.
(g) The protestor has only one opportunity to support or explain the substance of its protest. Department of Justice procedures do not provide for any discovery. The deciding official may request additional information from either the agency or the protestor. The deciding official will resolve the protest through informal presentations or meetings to the maximum extent practicable.
(h) An interested party may represent itself or be represented by legal counsel. The Department of Justice will not reimburse the protester for any legal fees related to the agency protest.
(i) The Department of Justice will stay award or suspend contract performance in accordance with FAR 33.103(f). The stay or suspension, unless over-ridden, remains in effect until the protest is decided, dismissed, or withdrawn.
(j) The deciding official will make a best effort to issue a decision on the protest within twenty (20) days after the filing date. The decision may be oral or written.

(k) The Department of Justice may dismiss or stay proceeding on an agency protest if a protest on the same or similar basis is filed with a protest forum outside the Department of Justice.
(End of Clause)

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 202-357-7000 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 202-357-7000 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.

DOJ-01 Whistleblower Information Distribution (Oct 2021)

Within 30 days of contract award, the contractor and its subcontractors must distribute the "Whistleblower Information for Employees of DOJ Contractors, Subcontractors, Grantees, or Sub-Grantees or Personal Services Contractors" ("Whistleblower Information") document to their employees performing work in support of the products and services delivered under this contract (https://oig.justice.gov/sites/default/files/2020-04/NDAA-brochure.pdf). By agreeing to the terms and conditions of this contract, the prime contractor acknowledges receipt of this requirement, in accordance with 41 U.S.C. § 4712 and FAR 3.908 & 52.203-17, and commits to distribution. Within 45 days of award, the contractor must provide confirmation to the contracting officer verifying that it has distributed the whistleblower information as required.

(End of Clause)

DOJ-02 Contractor Privacy Requirements (JAN 2022)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984) and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DOJ system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.justice.gov/opcl/doj-systems-records.[1] Applicable SORNs published by other agencies may be accessed through those agencies' websites or by searching the Federal Digital System (FDsys) available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

Except where use of Contractor networks, IT, other equipment, or Workplace as a Service (WaaS) is specifically authorized within this contract, the Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or WaaS and Government information shall remain within the confines of authorized Government networks at all times. Any handling of Government information on Contractor networks or IT must be approved by the Senior Component Official for Privacy of the component entering into this contract. Except where remote work is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

The Contractor shall complete and submit an appropriate separation checklist to the Contracting Officer before any employee or Subcontractor employee terminates working on the contract. The Contractor must submit the separation checklist on or before the last day of employment or work on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposition of personally identifiable information (PII)[2], in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to PII or other sensitive information.

In the event of adverse job actions resulting in the dismissal of a Contractor or Subcontractor employee before the separation checklist can be completed, the Prime Contractor must notify the Contracting Officer within 24 hours and confirm receipt of the notification. In the case the Contractor is unable to notify the Contracting Officer, then the Contractor should notify the Contract Officer's Representative (COR).

Contractors must complete the separation checklist with the Contracting Officer or COR by returning all Government-furnished property including, but not limited to, computer equipment, media, credentials and passports, smart cards, mobile devices, Personal Identity Verification (PIV) cards, calling cards, and keys and terminating access to all user accounts and systems. Unless the Contracting Officer requests otherwise, the relevant Program Manager or other Key Personnel designated by the Contracting Officer or COR may facilitate the return of equipment.

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

The Contractor must ensure that all employees take appropriate privacy training, including Subcontractors who have access to PII as well as the creation, use, dissemination and/or destruction of PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle PII, including heightened security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of PII. These courses, along with more information about DOJ security and training requirements for Contractors, are available at https://www.justice.gov/jmd/learndoj. The Federal Information Security Modernization Act of 2014 (FISMA) requires all individuals accessing DOJ information to complete training on records management, cybersecurity awareness, and information system privacy awareness. Contractor employees are required to sign the "Privacy Rules of Behavior," acknowledging and agreeing to abide by privacy law, policy, and certain privacy safeguards, prior to accessing DOJ information. These Rules of Behavior are made available to all new users of DOJ's computer network and to trainees at the conclusion of DOJ-OPCL-CS-0005.

The Contractor should maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required privacy and cybersecurity training.

(2) Safeguarding PII Requirements

Contractor employees must comply with DOJ Order 0904 and other guidance published to the publicly-available Office of Privacy and Civil Liberties (OPCL) Resources page[3] relating to the safeguarding of PII, including the use of additional controls to safeguard sensitive PII (e.g., the encryption of sensitive PII). This requirement flows down from the Prime Contractor to all Subcontractors and lower tiered subcontracts.

(3) Non-Disclosure Agreement Requirement

Prior to commencing work, all Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (NDA) and the DOJ IT Rules of Behavior. The Non-Disclosure Agreement:

(a) prohibits the Contractor from retaining or divulging any PII or other sensitive information, or derivatives therefrom, furnished by the Government or to which they may otherwise come in contact as a result of their performance of work under the contract/task order that is otherwise not publicly available, whether or not such information has been reduced to writing; and

(b) requires the Contractor to report any loss of control, compromise, unauthorized disclosure, or unauthorized acquisition of PII or other sensitive information to the component-level or headquarters Security Operations Center within one (1) hour of discovery.

The Contractor should maintain signed copies of the NDA for all employees as a record of compliance. The Contractor should also provide copies of each employee's signed NDA to the Contracting Officer before the employee may commence work under the contract/task order.

(4) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial or administrative records or databases is not authorized to regularly store or include any sensitive PII or other confidential government information that is created, obtained, or provided during the performance of the contract without the written permission of the Senior Component Official for Privacy (SCOP). It is acceptable to list the names, titles and contact information for the Contracting Officer, COR, or other personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Actual or Suspected Data Breach

Contractors must report any actual or suspected breach of PII within one hour of discovery.[4] A "breach" is an incident or occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. The report of a breach must be made to DOJ. The Contractor must cooperate with DOJ's inquiry into the incident and efforts to minimize risks to DOJ or individuals, including remediating any harm to potential victims.

(a) The Contractor must develop and maintain an internal process by which its employees and Subcontractors are trained to identify and report the breach, consistent with DOJ Instruction 0900.00.01[5], Reporting and Response Procedures for a Breach of Personally Identifiable Information.

(b) The Contractor must report any such breach by its employees or Subcontractors to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000); Component-level Security Operations Center and Component-level Management Team, where appropriate; the COR; and the Contracting Officer within one (1) hour of the initial discovery.

(c) The Contractor must provide a written report to the DOJ Security Operations Center (dojcert@usdoj.gov, 202-357-7000) within 24 hours of discovery of the breach by its employees or Subcontractors. The report must contain the following information:

(i) Narrative or detailed description of the events surrounding the suspected loss or compromise of information.[6] Date, time, and location of the incident.
(ii) Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.
(iii) Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.[7]
(iv) Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
(v) Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.[8]
(vi) Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
(vii) Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

(d) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(e) At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access PII or to work on that contract based on their actions related to the loss or compromise of PII.

(6) Victim Remediation

At DOJ's request, the Contractor is responsible for notifying victims and providing victim remediation services in the event of a breach of PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose PII was lost or compromised. When DOJ requests notification, the Department Chief Privacy and Civil Liberties Officer and SCOP will direct the Contractor on the method and content of such notification to be sent to individuals whose PII was breached. By performing this work, the Contractor agrees to full cooperation in the event of a breach. The Contractor should be self-insured to the extent necessary to handle any reasonably foreseeable breach, with another source of income, to fully cover the costs of breach response, including but not limited to victim remediation.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the *DOJ Records and Information Training for New Employees (RIM)* training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. The Contractor shall maintain

copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records containing PII and those covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency information. The Contractor shall certify, in writing, the appropriate disposition or return of all Government information at the conclusion of the contract or at a time otherwise specified in the contract. In accordance with 36 CFR 1222.32, the Contractor shall maintain and manage all Federal records created in the course of performing the contract in accordance with Federal law. Records may not be removed from the legal custody of DOJ or destroyed except in accordance with the provisions of the agency records schedules.

(b) Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and may be considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain an Authority To Operate (ATO) for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) If this contract requires the development, maintenance or administration of information technology[9], the Contractor shall support the completion of the Initial Privacy Assessment (IPA) document, if requested by Department personnel. An IPA is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help components assess whether additional privacy protections may be needed in designing or implementing a project[10] to mitigate privacy risks, and whether compliance work may be needed. Upon review of the IPA, the OPCL determines whether a Privacy Impact Assessment (PIA) document and/or SORN, or modifications thereto, are required. The Contractor shall provide adequate support to complete the applicable risk assessment and PIA document in a timely manner, and shall ensure that project management plans and schedules include the IPA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DOJ, including IPAs, PIAs, and SORNs, is located on the DOJ OPCL website (https://dojnet.doj.gov/privacy/), including DOJ Order 0601, Privacy and Civil Liberties. The Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor

shall work with personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST 800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB Circular A-130.

[1] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).
[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), "'personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Regarding "sensitive PII," "[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals' names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information." OMB Circular A-130, at App. II-2.
[3] The DOJ OPCL Resources page is available at https://www.justice.gov/opcl/resources.
[4] As stated in DOJ Instruction 0900, "Contractors must notify the Contracting Officer, the Contracting Officer's Representative, and JSOC (or component-level SOC) within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines."
[5] https://www.justice.gov/file/4336/download
[6] As stated in DOJ Instruction 0900, the description should include the type of information that constitutes PII; purpose for which PII is collected, maintained, and used; extent to which PII identifies a peculiarly vulnerable population; the determination of whether the information was properly encrypted or rendered partially or completely inaccessible by other means; format of PII (e.g., whether PII was structured or unstructured); length of time PII was exposed; any evidence confirming that PII is being misused or that it was never accessed.
[7] As stated in DOJ Instruction 0900, the report should include the nature of the cyber threat (*e.g.*, Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents.
[8] As stated in DOJ Instruction 0900, the report should include analysis on whether the data is accessible, usable, and intentionally targeted.
[9] As defined in 40 U.S.C. § 11101, the term "information technology" means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.
[10] In this instance, the term "project" is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL.

(End of Clause)

DOJ-03 Personnel Security Requirements For Contractor Employees (Nov 2021)

Work performed under this contract will involve any one or more of the following: access to DOJ Information, which may include Controlled Unclassified Information (CUI), i.e., unclassified, sensitive DOJ information, and/or access to DOJ Information Technology (IT) systems, and/or unescorted access to DOJ space or facilities. Contractor employees will occupy Public Trust Positions, unless clause alternates are applied.

1. General Requirements

(a) (1) All references to "contract(or) personnel" and "contract(or) employee" in this clause means all individuals, without limitation, to include individuals employed by the contractor, team member, subcontractor, consultant, and/or independent contractor, who will have access to information of the Department of Justice (DOJ) or information that is within the custody and control of the DOJ, access to DOJ IT systems, and/or unescorted access to DOJ facilities/space in connection with the performance of this contract. "Employment" as used herein does not create nor imply an employer/employee relationship between the DOJ and contractor employees.

(b) (1) The type of security investigation required for each contractor employee will be governed by the type and risk level of information made available to the contractor employee. The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the Security Programs Manager (SPM), in consultation with the Contracting Officer's Representative if one is appointed, have received the requisite security

(c) Except where specifically noted otherwise, the federal government will be responsible for the cost and conduct of the investigation.

(d) The contractor shall ensure that no contractor employee commences performance prior to receipt of a written authorization from the contracting officer, COR, or the SPM that performance by the respective contractor employee is authorized.

(e) The data and other information to which the contractor may have access as a result of this contract is the property of, and/or within the custody and control of, the Department, and its disclosure to third parties is governed by various statutes and regulations, the violation of which may subject the discloser to criminal

2. Citizenship and Residency Requirements

(a) Residency Requirement. (1) Contractor employees in Public Trust positions, both U.S. citizens and non-U.S. citizens, must meet the Department's residency requirement if they will require access to DOJ information, IT systems, or unescorted access to facilities. For three years (not necessarily consecutive years) out of the last five years immediately prior to employment under the Department contract the contractor employee must have: (i) resided in the U.S.; (ii) worked for the U.S. in a foreign country as either an employee or contractor in a federal civilian or military capacity; or, (iii) been a dependent of a federal civilian or military employee or contractor working for the U.S. in a foreign country. At the Department's sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) for contractor employees on a case-by-case basis where justified by extenuating circumstances. The residency requirement does not apply to contractor employees residing in foreign countries that are hired to work in American embassies/consulates/missions located outside of the United States and who require access to DOJ information, IT systems, or unescorted access *provided that* an adequate background investigation can be conducted, with favorable adjudication, as determined by the DSO.

(b) Citizenship. (1) Aside from the specific exceptions set forth in Section 1.2(b)(2), for Public Trust positions, the DOJ requires that contractor employees be U.S. citizens and nationals, or lawful permanent residents seeking U.S. citizenship. Any prospective non-U.S. citizen contractor employee who requires access to DOJ information systems, DOJ information, and/or unescorted facilities access must also have been granted a waiver as described below in paragraphs 1.2(d) and/or (e). The contractor is responsible for verifying that the non-U.S. citizens working under this contract are lawful permanent residents seeking U.S.

> (2) *Exception for Certain Non-U.S. Citizen Contractor Employees*: (i) Non-U.S. citizen expert witnesses, litigative consultants, and interpreters in rare foreign languages are not required to be lawful permanent residents seeking U.S. citizenship. However, they must be granted a waiver for access to unclassified DOJ information, whether CUI or not, DOJ IT systems, and/or unescorted facility access, as described below in paragraph 1.2(d) and (e), regardless of the duration of their duties. (ii) Non-U.S. Citizen contractor employees residing in foreign countries who are hired to work for the Department of Justice in American embassies/consulates/missions outside of the United States are not required to be lawful permanent residents seeking U.S. citizenship.

(c) Dual Citizenship. (1) S. citizens who hold dual citizenship with a foreign country are considered U.S. citizens within the meaning of this clause, and may be considered for, but are not entitled to, contract employment as U.S. citizens consistent with this clause. The means by which the contractor employee obtained or exercises his or her dual citizenship status will be a consideration in the Public Trust Investigation (PTI) adjudication, and/or waiver approval processes discussed in this clause.

(d) Access to DOJ Information Technology Systems. Non-U.S citizens are not authorized to access DOJ information technology (IT) systems or assist in the development, operation, management, or maintenance of DOJ IT systems, including providing IT system

support, unless a waiver has been granted by the Head of the DOJ component or designee, with the prior concurrence of both the DSO and the DOJ Chief Information Officer, allowing computer access by the non-U.S. citizen. Such a waiver will be granted only in exceptional and unique circumstances on a case-by-case basis. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive DOJ IT system and any contractor employee who will need access to JCON must be a U.S. citizen or have received a In order for a waiver to be considered for approval: (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; (2) The type of personnel security vetting that has been conducted on the individual, and vetting results, that would mitigate risk; and (3) The waiver must be in the best interest of the federal government.

(e) Access to Unclassified DOJ Information and Unescorted Access to DOJ Facilities or Space. (1) Except as provided under 1.2(b)(2), non-U.S. citizens are not authorized to access DOJ information and/or unescorted access to DOJ facilities or space, unless a waiver has been granted by the DSO, allowing access by the non-U.S. citizen. Such a waiver will be granted on a case-by-case basis where justified at the discretion of the DSO.

3. Background Investigation Requirements

(a) (1) Unless otherwise stated below, all contractor personnel are subject to a Public Trust Investigation (PTI). The SPM will determine the type of investigation for each contractor employee based on the risk category (i.e., the nature of the position and degree of harm that could be caused by the individual in that position) and whether the position is long-term or short-term. The PTI risk categories are listed

(i) High Risk Positions. The minimum background investigation required is a Tier 4 (T4) investigation, and the five-year reinvestigation required is a Tier 4R (T4R) investigation. The 2017 version of the Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.
(ii) Moderate Risk Positions. The minimum background investigation required is a Tier 2 (T2) investigation. The five-year reinvestigation required is a Tier 2R (T2R) investigation. The 2017 version of the SF-85P is
(iii) Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a Tier 1 (T1) investigation and the required five-year reinvestigation is also a Tier 1 (T1) investigation. The SF 85, Questionnaire for Non-Sensitive Positions, is

(b) *Exception for Expert Witnesses*. Expert Witnesses, litigative consultants, and interpreters in rare foreign languages may not be subject to full background investigation requirements if alternative security requirements are approved by the DSO.

(c) *Short-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), short-term contractor employees (6 months or less) who are U.S. citizens are not subject to a full background investigation, however, must receive an approved pre-employment background investigation waiver. The required forms to complete and submit are listed in Section 1.4(b) and (c)(2).

(d) *Long-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), all long-term U.S. citizen employees (longer than 6 months) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(e) *Non-U.S. Citizen Contractor Employees*. Other than the exception in 1.3(b), all non-U.S. citizen contractor employees regardless of performance duration (short or long term) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(f) *Reciprocity*. (1) A Public Trust Investigation will be accepted under reciprocity if it meets the following guidelines: (i) the investigation is current (investigations are considered current if completed within the last five years) and favorably adjudicated, or the reinvestigation has been deferred; (ii) the investigation meets or exceeds the level of investigation required for the DOJ contractual instrument; (iii) there has been no continuous (not cumulative) break in federal contract/service employment of two years or more; (iv) there is no derogatory information since the favorable fitness determination or adjudication that calls into question the individual's fitness based on character or conduct; and (v) the investigative record does not show conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from position to position.

4. Background Investigation Process

(a) *e-QIP (or its successor)*. Public Trust background investigations/reinvestigations of contractor employees will be performed by the DCSA. The investigative process requires contractor employees to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and provide additional information as specified in paragraph 1.4(b) below. Immediately after contract award, the contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the SPM. The e-QIP Initiator must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being given

access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The contractor will then be responsible for initiating investigations for all contract personnel, whose previous investigation does not meet reciprocity, in e-QIP for completion of the security questionnaire form and forwarding the electronic form with the remainder of the security package to the SPM. Subject to the prior written approval of the SPM, the contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being provided access to e-QIP.

(b) *Additional Documentation*. (1) In addition to completing the e-QIP questionnaire (see 1.4(a), above), the contractor shall ensure that each contractor employee occupying Public Trust Positions, including short-term employees, completes and submits the following information through the contractor's Corporate Security Officer:

(i) Digital Fingerprinting/FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI or other law enforcement entity, as approved by the SPM, is required to ensure the identity of the person being fingerprinted and for printing quality. All pertinent information must be completed by the individual taking the fingerprints (FBI or other). Use of the physical FD-258 Applicant Fingerprint Card should only be used in extenuating circumstances.
(ii) DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This form will be required if the Component SPM determines a credit check is necessary for its Low Risk Level 1 contractor positions.
(iii) OF-306, Declaration for Federal Employment.
(iv) Foreign National Relatives or Associates Statement. This is only required if foreign national relatives or associates were not disclosed on the security questionnaire form.
(v) Self-Reporting Requirements for All Contractor Personnel. This is an acknowledgement and acceptance statement that every contractor must sign.
(vi) Additional information as may be required based on the review of the security questionnaire form.

The contractor shall review all forms/documents to ensure each is complete, accurate and meets all DOJ requirements, including applicable residency and citizenship requirements. The contractor shall resolve any issues or discrepancies with the contractor employee, including resubmission of corrected forms or documentation. Completed forms/documents shall be submitted to the SPM (or designee, which may include the COR) within five (5) calendar days after being finalized.

(c) Adjudication and Pre-Employment Background Investigation Waivers

(1) Except as set forth in this section, background investigations must be conducted and favorably adjudicated for each contractor employee prior to commencing their work on this contract. Where programmatic needs do not permit the federal government to wait for completion of the entire background investigation, a pre-employment background investigation waiver for *public trust contractors* can be granted by the SPM, in consultation with the cognizant COR. Pre-employment waivers cannot be used to circumvent delays in clearing classified contractors through the DCSA, if access to classified information is required.

(2) As directed by the SPM, the contractor shall initiate pre-employment waivers for Public Trust Positions when necessary. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the federal government. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contractor employee's favor. When a waiver has been disapproved, the CO, in consultation with the SPM and COR, will determine (i) whether the contractor employee will no longer be considered for work on a DOJ contract or (ii) whether to wait for the completion and favorable adjudication of the background investigation before the contractor employee commences work on a Department contract. The pre-employment background investigation waiver requirements include:

1. Verification of citizenship (copy of a birth certificate, naturalization certificate, or U.S. passport);
2. Verification of compliance with the *DOJ Residency Requirement* of this Clause;
3. Favorable review of the security questionnaire form;
4. Favorable FBI fingerprint results;
5. Favorable credit report;
6. Favorable review of the OF-306 form, Declaration for Federal Employment;
7. Verification of the initiation of the appropriate background investigation (for long-term personnel); and
8. Receipt of the signed DOJ *Self-Reporting Requirements for All Contractor Personnel* (see Section 1.6, below).

(3) The investigating agency (DCSA) will provide the SPM with the results of each proposed contractor employee's Public Trust investigation. Upon receipt of the investigation and any other pertinent documents from the investigating agency, the SPM will determine whether each proposed contractor employee should be granted employment security approval.

(4) The COR will notify the contractor of the results of Public Trust background investigations as they are completed and adjudicated, including any individual who is found ineligible for employment security approval. For any individual found ineligible for employment on a Department contract, the contractor shall propose a replacement and initiate the background investigation process consistent with this

5. Identity Proofing and Badging

(a) Access to DOJ Information, federally-controlled IT systems, and/or unescorted access to federally-controlled facilities or space (regardless of whether the contractor employee will be issued a DOJ PIV card or building access badge) shall be made available after each respective contractor employee has (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this

(b) (1) Public Trust contractor employees must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking two forms of identification in original form prior to commencement of work by the contractor employee and PIV card or building access badge issuance (as applicable). Approval will be documented by the DOJ official or an official of a trusted contract company. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

(c) [Reserved]

(d) All contractor employees requiring unescorted access to a DOJ controlled facility or space shall comply with the PIV card or building access badge requirements outlined below:

> (i) When any contractor employee enters a DOJ building for the first time, he/she shall allow one hour for security processing and the creation and issuance of a building access PIV cards require additional processing time and will not likely be issued on the same day.
> (ii) Building access badges shall be subject to periodic review by the contractor employee's supervisor and checked against his/her personal identification. The contractor employees shall present themselves for the issuance of renewed badges when required by the government as scheduled by the COR or his/her designee. The contractor shall notify the COR when contractor employee badges are lost, and must immediately apply for reissuance of a replacement badge. The contractor shall pay for reissued building access badges at no cost to the government. It is the contractor employee's responsibility to return badges to the COR or his/her designee when a contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

6. Employee Reporting Requirements

(a) All contractor employees must sign the DOJ *Self-Reporting Requirements for All Contractor Personnel* statement acknowledging and accepting the DOJ requirement that they immediately self-report certain information using the Department’s iReport system. The COR or SPM will provide the Self-Reporting statement as well as a list of reportable information, which varies by position sensitivity designation, to the contractor employee before commencing work under the contract. If the contractor employee does not have access to the DOJ iReport System, the COR or SPM will provide a fillable form for the contractor employee to complete and

(b) The COR and SPM will review the written report and documentation and make a determination regarding continued employment on a DOJ

(c) DOJ reporting requirements are in addition to the DCSA reporting requirements and the contractor’s internal reporting

7. Replacement Personnel

(a) The contractor shall make every effort to avoid costs to the government for security investigations for replacement of contractor employees, and in so doing shall ensure that otherwise satisfactorily performing and physically able contractor employees remain in contract performance for the duration of the contract. The contractor shall take all necessary steps to ensure that contractor personnel who are selected for assignment to this contract are professionally qualified and personally reliable, of reputable background and sound character, and able to meet all other requirements stipulated in the contract.

(b) The fact that the government performs security investigations shall not in any manner relieve the contractor of its responsibility to ensure that all contract personnel are reliable and of reputable background and sound character. Should a security investigation conducted by the government and/or a contractor’s self-report or failure to self-report render ineligible a contractor employee, the contracting officer will determine whether the contractor has violated this clause. The contracting officer may direct the contractor, at its own expense, to remove and replace any contractor personnel who fails to comply with or violates applicable requirements of

this contract. Such action may be taken at the government's direction without prejudice to its rights under any other provision of this contract, including termination for default, and the contractor may be held liable, at a minimum, for all reasonable and necessary costs incurred by the government to (i) provide coverage (performance) through assignment of individuals employed by the government or third parties in those cases where absence of contractor personnel would cause either a security threat or DOJ program disruption and (ii) conduct security investigations in excess of those which would otherwise be required.

(c) Nothing in this clause shall require the contractor to bear costs involved in the conduct of security investigations for replacement of a contractor employee who separates from the contractor of his/her own accord, is incapacitated, or is deceased.

(d) The contractor shall comply with the terms and conditions set forth under this clause and assumes all liability for failure to comply. The rights and remedies conferred upon the government by this clause are in addition to all and other rights and remedies pursuant to the contract and as established by law.

(End of Clause)

OBD-01 Electronic Signatures (MAY 2019)

(a) The Department of Justice is committed to doing business in the most
efficient and effective way possible, and to facilitate paperless processes. In furtherance of this goal, the Contracting Officer may apply their digital signature to procurement documents in the Portable Document Format (PDF) through the use of their government issued Personal Identity Verification (PIV) Card with a valid public key certificate. A digital signature made with these certificates is evidence that a specific individual signed the electronic record and that it was not altered. The recipient of a signed document can rely on the digital signature as evidence for a third party that the signature was generated by the claimed signer.
(b) For procurement documents that require a signature from a representative of the Contractor, the Contractor may utilize manual or electronic signature. Should the Contractor utilize an electronic signature, by returning the document with an electronic symbol affixed to the appropriate signature block, the Contractor representative signing on behalf of the Contractor certifies that:

(1) Electronic Form of Signature: The Contractor representative has knowingly adopted, applied or affixed an electronic symbol to the document;

(2) Intent to Sign: The Contractor representative has applied an electronic symbol with the intent to legally bind the Contractor;

(3) Association of Signature to Record: the Contractor representative's signature is attached to the electronic record being signed;

(4) Identification and Authentication of Signer: The Contractor has a means to identify and authenticate a particular person as the signer; and

(5) Integrity of Signed Record: The Contractor can attest to the integrity of the signed record between the time of signature and the returned record to the government.

This clause applies to this document and any subsequent documents (e.g., modifications, task/delivery orders) associated with this action.

[END OF ADDENDUM TO FAR 52.212-4]

Section 4 - List of Attachments

Identifier	Title	Number of Pages
1	Attachment 1 - SOW and Evaluation Procedures	22
2	Attachment 2 - Price List	4
3	Attachments 3-6.pdf	5
4	BST WD 2015-4047 Revision 22 Date of Last Revision December 27, 2022	11
5	SPF WD 2015-4095 Revision 23 Date of Last Revision December 27, 2022	11
6	WOR WD 2015-4103 Revision 23 Date of Last Revision December 27, 2022	11

Section 5 - Solicitation Provisions

A.2 ADDENDUM TO FAR 52.212-1, Instructions to Offerors-Commercial Products and Commercial Services (Nov 2021)

The terms and conditions for the following provisions are hereby incorporated into this solicitation as an addendum to FAR provision 52.212-1.

Provisions By Reference

52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)		
This solicitation incorporates one or more solicitation provisions 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. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): www.acquisition.gov		
Provision	Title	Fill-ins (if applicable)
52.212-2	Evaluation-Commercial Products and Commercial Services (Nov 2021)	
52.212-3	Offeror Representations and Certifications-Commercial Products and Commercial Services (May 2022)	
52.212-1	Instructions to Offerors-Commercial Products and Commercial Services (Nov 2021)	
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Nov 2021)	
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021)	
52.204-7	System for Award Management (Oct 2018)	
52.204-16	Commercial and Government Entity Code Reporting (Aug 2020)	
52.217-5	Evaluation of Options (July 1990)	

[END OF ADDENDUM TO FAR 52.212-1]