

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 & 30			1. REQUISITION NUMBER	PAGE 1 OF 35
2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER 15B41823Q00000017	6. SOLICITATION ISSUE DATE 02/22/2023
7. FOR SOLICITATION INFORMATION CALL:	a. NAME Mike Gibson mpgibson@bop.gov		b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE / LOCAL TIME 03/24/2023 16:00 ET

9. ISSUED BY Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	CODE 15B418	10. THE ACQUISITION IS <input type="checkbox"/> UNRESTRICTED OR <input checked="" type="checkbox"/> SET ASIDE: 100.00 % FOR <input checked="" type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> EDWOSB <input type="checkbox"/> 8(A) NAICS: 813110 SIZE STANDARD:
---	----------------	---

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE	12. DISCOUNT TERMS NET 30	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>	13b. RATING
		14. METHOD OF SOLICITATION <input checked="" type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP	

15. DELIVER TO Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	CODE 15B418	16. ADMINISTERED BY Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	CODE 15B418 Mike Gibson (O) 812-244-4473 mpgibson@bop.gov
---	----------------	--	---

17a. CONTRACTOR/OFFEROR CODE	FACILITY CODE	18a. PAYMENT WILL BE MADE BY Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	CODE 15B418
TELEPHONE NO.		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM	

<input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER	<input type="checkbox"/> 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED
--	---

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
0001	Firm Fixed Price Hours worked as a Transition Coach with Life Connections Program, including group facilitation, group planning, reviewing student work & progress, curriculum development, and training. curriculum development, and training. Base Year PSC: G002 See Continuation Sheet(s) <i>(Use Reverse and/or Attach Additional Sheets as Necessary)</i>	1,440	SS	\$ _____	\$ _____

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT (For Govt. Use Only)
---------------------------------------	---

<input checked="" type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input checked="" type="checkbox"/> ARE NOT ATTACHED	<input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED
---	--

<input type="checkbox"/> 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.	<input type="checkbox"/> 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) Michael Gibson	31c. DATE SIGNED 02/24/2023

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 <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	37. CHECK NUMBER
--	--------------------	---------------------------------	--	------------------

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 (<i>Print</i>)	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT (<i>Location</i>)
		42c. DATE REC'D (<i>YY/MM/DD</i>)

Table of Contents

<u>Section</u>	<u>Description</u>	<u>Page Number</u>
1	Solicitation/Contract Form.....	1
2	Commodity or Services Schedule.....	4
3	Contract Clauses.....	5
	DJAR-PGD-15-03 Security of Department Information and Systems.....	5
	52.203-17 Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (Jun 2020).....	5
	52.204-13 System for Award Management Maintenance (Oct 2018).....	5
	52.212-4 Contract Terms and Conditions-Commercial Products and Commercial Services (Dec 2022).....	5
	52.228-5 Insurance-Work on a Government Installation (Jan 1997).....	5
	52.232-18 Availability of Funds (Apr 1984).....	5
	52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Nov 2021).....	5
	52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders-Commercial Products and Commercial Services (Dec 2022).....	5
	52.216-18 Ordering (Aug 2020).....	10
	52.216-21 Requirements (Oct 1995).....	11
	52.217-9 Option to Extend the Term of the Contract (Mar 2000).....	11
	52.232-19 Availability of Funds for the Next Fiscal Year (Apr 1984).....	11
	52.218-000 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OR OTHER NATIONAL EMERGENCY (May 2008).....	12
	52.21-603-70 Contracting Officer's Representative (COR) (June 2012).....	12
	52.27-103-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004).....	13
	BOP 2852.237-77 Contractors Classified as Common Law Employees for Federal Income Tax Purposes (July 2017).....	13
	BOP 2852.242-71 EVALUATION OF CONTRACTOR PERFORMANCE UTILIZING CPARS (APR 2011).....	13
	DOJ-01 Whistleblower Information Distribution (Oct 2021).....	13
	DOJ-03 Personnel Security Requirements For Contractor Employees (Nov 2021).....	14
	DOJ-02 Contractor Privacy Requirements (JAN 2022).....	18
	52.217-8 Option to Extend Services (Nov 1999).....	23
4	List of Attachments.....	30
5	Solicitation Provisions.....	31
	52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021).....	34
	52.212-3 Offeror Representations and Certifications-Commercial Products and Commercial Services (Dec 2022).....	34
	52.204-7 System for Award Management (Oct 2018).....	34
	2852.233-70 Protests Filed Directly with the Department of Justice (NOV 2020).....	34
	BOP 2852.237-78 Submission/Evaluation of Quotations/Offer by Individuals (Nov 2014).....	34
	BOP 2852.237-71 Requirements for Religious Services (July 2017).....	34
	52.212-1 Instructions to Offerors-Commercial Products and Commercial Services (Nov 2021).....	34

Section 2 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
	Line Period of Performance: 05/01/2023 - 04/30/2024 Base Period			\$ _____	\$ _____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Hours worked as a Transition Coach with Life Connections Program, including group facilitation, group planning, reviewing student work & progress, curriculum development, and training. curriculum development, and training. Option Year One PSC: G002 Line Period of Performance: 05/01/2024 - 04/30/2025 Option Period 1	1,440	SS	\$ _____	\$ _____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003	Hours worked as a Transition Coach with Life Connections Program, including group facilitation, group planning, reviewing student work & progress, curriculum development, and training. curriculum development, and training. Option Year Two PSC: G002 Line Period of Performance: 05/01/2025 - 04/30/2026 Option Period 2	1,440	SS	\$ _____	\$ _____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004	Hours worked as a Transition Coach with Life Connections Program, including group facilitation, group planning, reviewing student work & progress, curriculum development, and training. curriculum development, and training. Option Year Three PSC: G002 Line Period of Performance: 05/01/2026 - 04/30/2027 Option Period 3	1,440	SS	\$ _____	\$ _____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005	Hours worked as a Transition Coach with Life Connections Program, including group facilitation, group planning, reviewing student work & progress, curriculum development, and training. curriculum development, and training. Option Year Four PSC: G002 Line Period of Performance: 05/01/2027 - 04/30/2028 Option Period 4	1,440	SS	\$ _____	\$ _____

Section 3 - Contract Clauses

A.1 ADDENDUM TO FAR 52.212-4, Contract Terms and Conditions-Commercial Products and Commercial Services (Dec 2022)

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)
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (Jun 2020)	
52.204-13	System for Award Management Maintenance (Oct 2018)	
52.212-4	Contract Terms and Conditions-Commercial Products and Commercial Services (Dec 2022)	
52.228-5	Insurance-Work on a Government Installation (Jan 1997)	
52.232-18	Availability of Funds (Apr 1984)	
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (Nov 2021)	

Clauses By Full Text

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

I. Applicability to Contractors and Subcontractors

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

II. General Definitions

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

- A. **Information** means any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. Information includes information in an electronic format that allows it be stored, retrieved or transmitted, also referred to as “data,” and “personally identifiable information” (“PII”), regardless of form.
- B. **Personally Identifiable Information (or PII)** means any information about an individual maintained by an agency, including, but not limited to, information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
- C. **DOJ Information** means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, Information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired in order to perform the contract.
- D. **Information System** means any resources, or set of resources organized for accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of (hereinafter collectively, “processing, storing, or transmitting”) Information.
- E. **Covered Information System** means any information system used for, involved with, or allowing, the processing, storing, or transmitting of DOJ Information.

III. Confidentiality and Non-disclosure of DOJ Information

- A. Preliminary and final deliverables and all associated working papers and material generated by Contractor containing DOJ Information are the property of the U.S. Government and must be submitted to the Contracting Officer (“CO”) or the CO’s Representative (“COR”) at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14.
- B. All documents produced in the performance of this contract containing DOJ Information are the property of the U.S. Government and Contractor shall neither reproduce nor release to any third-party at any time, including during or at expiration or termination of the contract without the prior written permission of the CO.
- C. Any DOJ information made available to Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, Contractor assumes responsibility for the protection of the confidentiality of any and all DOJ Information processed, stored, or transmitted by the Contractor. When requested by the CO (typically no more than annually), Contractor shall provide a report to the CO identifying, to the best of Contractor’s knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

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

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

2. Providing security awareness training including, but not limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems;
 3. Creating, protecting, and retaining Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information;
 4. Maintaining authorizations to operate any Covered Information System;
 5. Performing continuous monitoring on all Covered Information Systems;
 6. Establishing and maintaining baseline configurations and inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Information Systems;
 7. Ensuring appropriate contingency planning has been performed, including DOJ Information and Covered Information System backups;
 8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods where required;
 9. Establishing an operational incident handling capability for Covered Information Systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and reporting incidents to appropriate officials and authorities within Contractor's organization and the DOJ;
 10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance;
 12. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media;
 13. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized U.S. citizens unless a waiver has been granted by the Contracting Officer ("CO"), and protecting the physical facilities and support infrastructure for such Information Systems;
 14. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards;
 15. Assessing the risk to DOJ Information in Covered Information Systems periodically, including scanning for vulnerabilities and remediating such vulnerabilities in accordance with DOJ policy and ensuring the timely removal of assets no longer supported by the Contractor;
 16. Assessing the security controls of Covered Information Systems periodically to determine if the controls are effective in their application, developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Information Systems, and monitoring security controls on an ongoing basis to ensure the continued effectiveness of the controls;
 17. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security; and
 18. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate action in response.
- B. Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an Authority to Operate ("ATO") for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. The DOJ standards and requirements for obtaining an ATO may be found at DOJ Order 2640.2, as amended. (For Cloud Computing Systems, see Section V, below.)

- C. Contractor shall ensure that no Non-U.S. citizen accesses or assists in the development, operation, management, or maintenance of any DOJ Information System, unless a waiver has been granted by the by the DOJ Component Head (or his or her designee) responsible for the DOJ Information System, the DOJ Chief Information Officer, and the DOJ Security Officer.
- D. When requested by the DOJ CO or COR, or other DOJ official as described below, in connection with DOJ's efforts to ensure compliance with security requirements and to maintain and safeguard against threats and hazards to the security, confidentiality, integrity, and availability of DOJ Information, Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.
- E. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause is prohibited until Contractor provides a letter to the DOJ CO, and obtains the CO's approval, certifying compliance with the following requirements:
1. Media must be encrypted using a NIST FIPS 140-2 approved product;
 2. Contractor must develop and implement a process to ensure that security and other applications software is kept up-to-date;
 3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism;
 4. Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information is sensitive information unless specifically designated as non-sensitive by the DOJ; and,
 5. A Rules of Behavior ("ROB") form must be signed by users. These rules must address, at a minimum, authorized and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the user that he or she has no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.
- F. Contractor-owned removable media containing DOJ Information shall not be removed from DOJ facilities without prior approval of the DOJ CO or COR.
- G. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with DOJ security requirements.
- H. Contractor must keep an accurate inventory of digital or electronic media used in the performance of DOJ contracts.
- I. Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 15 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned to the DOJ in a format and form acceptable to the DOJ. The removal and return of all DOJ Information must be accomplished in accordance with DOJ IT Security Standard requirements, and an official of the Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 15 days of the removal and return of all DOJ Information.
- J. DOJ, at its discretion, may suspend Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident (see Section V.E. below), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to the DOJ, and that upon request by the CO, Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at Contractor's expense.

V. Cloud Computing

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

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

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

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

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

VI. Information System Security Breach or Incident

A. Definitions

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

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

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

B. **Confirmed Breach.** Contractor shall immediately (and in no event later than within 1 hour of discovery) report any Confirmed Breach to the DOJ CO and the CO’s Representative (“COR”). If the Confirmed Breach occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, Contractor must call DOJ-CERT at 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 the DOJ. 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.

52.216-18 Ordering (Aug 2020)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from first day of the current performance period through the last day of the current performance period through _____ [*insert dates*].

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) A delivery order or task order is considered "issued" when--

(1) If sent by mail (includes transmittal by U.S. mail or private delivery service), the Government deposits the order in the mail;

(2) If sent by fax, the Government transmits the order to the Contractor's fax number; or

(3) If sent electronically, the Government either--

(i) Posts a copy of the delivery order or task order to a Government document access system, and notice is sent to the Contractor; or

(ii) Distributes the delivery order or task order via email to the Contractor's email address.

(d) Orders may be issued by methods other than those enumerated in this clause only if authorized in the contract.

(End of clause)

52.216-21 Requirements (Oct 1995)

(a) This is a requirements contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies or services specified in the Schedule are estimates only and are not purchased by this contract. Except as this contract may otherwise provide, if the Government's requirements do not result in orders in the quantities described as "estimated" or "maximum" in the Schedule, that fact shall not constitute the basis for an equitable price adjustment.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. Subject to any limitations in the Order Limitations clause or elsewhere in this contract, the Contractor shall furnish to the Government all supplies or services specified in the Schedule and called for by orders issued in accordance with the Ordering clause. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(c) Except as this contract otherwise provides, the Government shall order from the Contractor all the supplies or services specified in the Schedule that are required to be purchased by the Government activity or activities specified in the Schedule.

(d) The Government is not required to purchase from the Contractor requirements in excess of any limit on total orders under this contract.

(e) If the Government urgently requires delivery of any quantity of an item before the earliest date that delivery may be specified under this contract, and if the Contractor will not accept an order providing for the accelerated delivery, the Government may acquire the urgently required goods or services from another source.

(f) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after the last day of the effective performance period. [*insert date*].

(End of clause)

52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within the last day of the effective performance period. [*insert the period of time within which the Contracting Officer may exercise the option*]; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days [*60 days unless a different number of days is inserted*] before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5.5 (months)(years).

(End of clause)

52.232-19 Availability of Funds for the Next Fiscal Year (Apr 1984)

Funds are not presently available for performance under this contract beyond September 30 of the base period or any option year exercised. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond September 30 of the base period or any option year exercised, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

52.218-000 CONTINUING CONTRACT PERFORMANCE DURING A PANDEMIC INFLUENZA OR OTHER NATIONAL EMERGENCY (May 2008)

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.
- 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 contractor's 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]

52.21-603-70 Contracting Officer's Representative (COR) (June 2012)

(a) Jonathon Sutter , Chaplain , FCC Terre Haute, 812-244-4458, is hereby designated as the Contracting Officer's Representative (COR) under this contract.

(b) The COR is responsible, as applicable, for: receiving all deliverables, inspecting and accepting the supplies or services provide hereunder in accordance with the terms and conditions of this contract; providing direction to the contractor which clarifies the contractor effort, fills in details or otherwise serves to accomplish the contractual Scope of Work; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payment.

(c) The COR does not have the authority to alter the contractor's obligations under the contract, and/or modify any of the expressed terms, conditions, specifications, or cost of the agreement. If as a result of technical discussions it is desirable to alter/change contractual obligations or the Scope of Work, the Contracting Officer shall issue such changes.

52.27-103-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)

For three of the five years immediately prior to submission of an offer/bid/quote, or prior to performance under a contract or commitment, individuals or contractor employees providing services must have:

1. Legally resided in the United States (U.S.);
2. worked for the U.S. overseas in a Federal or military capacity; or
3. been a dependent of a Federal or military employee serving overseas.

If the individual is not a U.S. citizen, they must be from a country allied with the U.S. The following website provides current information regarding allied countries: <http://www.opm.gov/employ/html/citizen.htm>

By signing this contract or commitment document, or by commencing performance, the contractor agrees to this restriction.
[End of Clause]

BOP 2852.237-77 Contractors Classified as Common Law Employees for Federal Income Tax Purposes (July 2017)

(a) When award is made to an individual other than a corporation, the provision of these services by an individual makes that individual a "common law employee" of the Bureau for federal income tax purposes only. Therefore, the Bureau is responsible for the payment of FICA taxes and the withholding of the individual contractor's taxes.

(b) An award made to an individual resulting from this solicitation is not subject to FAR 52.212-4, Prompt Payment Act.

(c) Upon contract award, the following forms shall be completed by the individual awardee:

Direct Deposit (SF-1199A).

Federal/State/City/County Tax forms (as applicable).

Employee Locator Form (DOJ-233).

Ethnicity and Race Information (SF-181).

Self-Identification of Disability (SF-256).

Employment Eligibility Verification (I-9).

(d) Even if an individual contractor is denoted a "common law employee" for federal income tax withholding purposes, the contractor remains an independent contractor. No employment relationship will be created between the Bureau and the contractor by the award of this contract to an individual contractor. An individual contractor awardee is not entitled to other aspects of employment with the Bureau, such as the filing of Equal Employment Opportunity claims, tort claims, etc.

[End of Clause]

BOP 2852.242-71 EVALUATION OF CONTRACTOR PERFORMANCE UTILIZING CPARS (APR 2011)

The services, although not directly supervised, shall be reviewed by Federal Bureau of Prisons (BOP) staff to ensure contract compliance. The contractor's performance will be evaluated in accordance with FAR 42.15. Contract monitoring reports will be prepared by the Contacting Officer's Representative (COR) and maintained in the contract file.

In accordance with FAR 42.1502 and 42.1503, agencies shall prepare an evaluation of contractor performance and submit it to the Past Performance Information Retrieval System (PPIRS). The BOP utilizes the Department of Defense (DOD) web-based Contractor Performance Assessment Reporting System (CPARS) to provide contractor performance evaluations. The contractor shall provide and maintain a current e-mail address throughout the life of the contract. The contractor will receive an e-mail from the Focal Point thru the following website address webpmsmh@navy.mil when the contract is registered in CPARS. The e-mail will contain a "user ID" and temporary password to register in the CPARS system. The contractor must be registered to access and review its evaluation and/or provide a response. If assistance is required when registering, please contact the Contracting Staff/Focal Point.

(End of Clause)

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-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 waiver. 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)

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/learndo>. 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)

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 [*insert the period of time within which the Contracting Officer may exercise the option*].

(End of clause)

[END OF ADDENDUM TO FAR 52.212-4]

52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders- Commercial Products and Commercial Services (Dec 2022)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

- (1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
- (2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).
- (3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).
- (4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).
- (5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).
- (6) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004)(Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[*Contracting Officer check as appropriate.*]

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Nov 2021) (41 U.S.C. 4704 and 10 U.S.C. 4655).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509)).

(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

X (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

__ (5) [Reserved].

__ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

__ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Nov 2021) (31 U.S.C. 6101 note).

__ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

__ (10) [Reserved].

__ (11) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Oct 2022) (15 U.S.C. 657a).

__ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2022) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

__ (13) [Reserved]

X (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

__ (ii) Alternate I (Mar 2020) of 52.219-6.

__ (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

__ (ii) Alternate I (Mar 2020) of 52.219-7.

X (16) 52.219-8, Utilization of Small Business Concerns (Oct 2022) (15 U.S.C. 637(d)(2) and (3)).

__ (17)(i) 52.219-9, Small Business Subcontracting Plan (Oct 2022) (15 U.S.C. 637(d)(4)).

__ (ii) Alternate I (Nov 2016) of 52.219-9.

__ (iii) Alternate II (Nov 2016) of 52.219-9.

__ (iv) Alternate III (Jun 2020) of 52.219-9.

__ (v) Alternate IV (Sep 2021) of 52.219-9.

__ (18)(i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

__ (ii) Alternate I (Mar 2020) of 52.219-13.

X (19) 52.219-14, Limitations on Subcontracting (Oct 2022) (15 U.S.C. 657s).

__ (20) 52.219-16, Liquidated Damages-Subcontracting Plan (Sep 2021) (15 U.S.C. 637(d)(4)(F)(i)).

__ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Oct 2022) (15 U.S.C. 657f).

X (22)(i) 52.219-28, Post-Award Small Business Program Rerepresentation (Oct 2022) (15 U.S.C. 632(a)(2)).

__ (ii) Alternate I (Mar 2020) of 52.219-28.

__ (23) 52.219-29, Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Oct 2022) (15 U.S.C. 637(m)).

- (24) 52.219-30, Notice of Set-Aside for, or Sole-Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Oct 2022) (15 U.S.C. 637(m)).
- (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).
- (26) 52.219-33, Nonmanufacturer Rule (Sep 2021) (15 U.S.C. 657s).
- (27) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
- (28) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (Dec 2022) (E.O. 13126).
- (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- (30)(i) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).
- (ii) Alternate I (Feb 1999) of 52.222-26.
- (31)(i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
- (ii) Alternate I (July 2014) of 52.222-35.
- (32)(i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
- (ii) Alternate I (July 2014) of 52.222-36.
- (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
- (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- (35)(i) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).
- (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).
- (36) 52.222-54, Employment Eligibility Verification (May 2022). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial products or commercial services as prescribed in FAR 22.1803.)
- (37)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c) (3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).
- (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
- (40)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).
- (ii) Alternate I (Oct 2015) of 52.223-13.
- (41)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).
- (ii) Alternate I (Jun 2014) of 52.223-14.
- (42) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).
- (43)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

__ (ii) Alternate I (Jun 2014) of 52.223-16.

X (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020) (E.O. 13513).

__ (45) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).

__ (46) 52.223-21, Foams (Jun 2016) (E.O. 13693).

__ (47)(i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

__ (ii) Alternate I (Jan 2017) of 52.224-3.

__ (48)(i) 52.225-1, Buy American--Supplies (Oct 2022) (41 U.S.C. chapter 83).

__ (ii) Alternate I (Oct 2022) of 52.225-1.

__ (49)(i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (Dec 2022) (19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, 19 U.S.C. chapter 29 (sections 4501-4732), Public Law 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

__ (ii) Alternate I [Reserved].

__ (iii) Alternate II (Dec 2022) of 52.225-3.

__ (iv) Alternate III (Jan 2021) of 52.225-3.

__ (v) Alternate IV (Oct 2022) of 52.225-3.

__ (50) 52.225-5, Trade Agreements (Dec 2022) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

X (51) 52.225-13, Restrictions on Certain Foreign Purchases (Feb 2021) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

__ (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

__ (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

__ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

__ (55) 52.229-12, Tax on Certain Foreign Procurements (Feb 2021).

__ (56) 52.232-29, Terms for Financing of Purchases of Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

__ (57) 52.232-30, Installment Payments for Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

X (58) 52.232-33, Payment by Electronic Funds Transfer--System for Award Management (Oct 2018) (31 U.S.C. 3332).

__ (59) 52.232-34, Payment by Electronic Funds Transfer--Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

__ (60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

__ (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

__ (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017)(15 U.S.C. 637(d)(13)).

__ (63)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631).

__ (ii) Alternate I (Apr 2003) of 52.247-64.

__ (iii) Alternate II (Nov 2021) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[Contracting Officer check as appropriate.]

__ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

__ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards--Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

__ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

__ (7) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).

__ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).

__ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record.* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, as defined in FAR 2.101, on the date of award of this contract and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial products or commercial services. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509).

- (ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
- (iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).
- (iv) 52.204–25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).
- (v) 52.219-8, Utilization of Small Business Concerns (Oct 2022) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
- (vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015)
- (vii) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).
- (viii) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
- (ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
- (x) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212)
- (xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
- (xii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
- (xiii) (A) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O 13627).
- (B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O 13627).
- (xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).
- (xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).
- (xvi) 52.222-54, Employment Eligibility Verification (May 2022) (E.O. 12989).
- (xvii) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).
- (xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).
- (xix)(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
- (B) Alternate I (Jan 2017) of 52.224-3.
- (xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).
- (xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
- (xxii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

Section 4 - List of Attachments

This Section Is Intentionally Left Blank

Section 5 - Solicitation Provisions

52.212-1 Instructions to Offerors-Commercial Products and Commercial Services (Nov 2021)

(a) *North American Industry Classification System (NAICS) code and small business size standard.* The NAICS code(s) and small business size standard(s) for this acquisition appear elsewhere in the solicitation. However, the small business size standard for a concern that submits an offer, other than on a construction or service acquisition, but proposes to furnish an end item that it did not itself manufacture, process, or produce is 500 employees if the acquisition--

(1) Is set aside for small business and has a value above the simplified acquisition threshold;

(2) Uses the HUBZone price evaluation preference regardless of dollar value, unless the offeror waives the price evaluation preference; or

(3) Is an 8(a), HUBZone, service-disabled veteran-owned, economically disadvantaged women-owned, or women-owned small business set-aside or sole-source award regardless of dollar value.

(b) *Submission of offers.* Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. As a minimum, offers must show--

(1) The solicitation number;

(2) The time specified in the solicitation for receipt of offers;

(3) The name, address, and telephone number of the offeror;

(4) A technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation. This may include product literature, or other documents, if necessary;

(5) Terms of any express warranty;

(6) Price and any discount terms;

(7) "Remit to" address, if different than mailing address;

(8) A completed copy of the representations and certifications at Federal Acquisition Regulation (FAR) 52.212-3 (see FAR 52.212-3(b) for those representations and certifications that the offeror shall complete electronically);

(9) Acknowledgment of Solicitation Amendments;

(10) Past performance information, when included as an evaluation factor, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information); and

(11) If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) *Period for acceptance of offers.* The offeror agrees to hold the prices in its offer firm for 30 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(d) *Product samples.* When required by the solicitation, product samples shall be submitted at or prior to the time specified for receipt of offers. Unless otherwise specified in this solicitation, these samples shall be submitted at no expense to the Government, and returned at the sender's request and expense, unless they are destroyed during preaward testing.

(e) *Multiple offers.* Offerors are encouraged to submit multiple offers presenting alternative terms and conditions, including alternative line items (provided that the alternative line items are consistent with FAR subpart 4.10), or alternative commercial products or commercial services for satisfying the requirements of this solicitation. Each offer submitted will be evaluated separately.

(f) *Late submissions, modifications, revisions, and withdrawals of offers.*

(1) Offerors are responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation by the time specified in the solicitation. If no time is specified in the solicitation, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that offers or revisions are due.

(2)(i) Any offer, modification, revision, or withdrawal of an offer received at the Government office designated in the solicitation after the exact time specified for receipt of offers is "late" and will not be considered unless it is received before award is made, the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition; and--

(A) If it was transmitted through an electronic commerce method authorized by the solicitation, it was received at the initial point of entry to the Government infrastructure not later than 5:00 p.m. one working day prior to the date specified for receipt of offers; or

(B) There is acceptable evidence to establish that it was received at the Government installation designated for receipt of offers and was under the Government's control prior to the time set for receipt of offers; or

(C) If this solicitation is a request for proposals, it was the only proposal received.

(ii) However, a late modification of an otherwise successful offer, that makes its terms more favorable to the Government, will be considered at any time it is received and may be accepted.

(3) Acceptable evidence to establish the time of receipt at the Government installation includes the time/date stamp of that installation on the offer wrapper, other documentary evidence of receipt maintained by the installation, or oral testimony or statements of Government personnel.

(4) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.

(5) Offers may be withdrawn by written notice received at any time before the exact time set for receipt of offers. Oral offers in response to oral solicitations may be withdrawn orally. If the solicitation authorizes facsimile offers, offers may be withdrawn via facsimile received at any time before the exact time set for receipt of offers, subject to the conditions specified in the solicitation concerning facsimile offers. An offer may be withdrawn in person by an offeror or its authorized representative if, before the exact time set for receipt of offers, the identity of the person requesting withdrawal is established and the person signs a receipt for the offer.

(g) *Contract award (not applicable to Invitation for Bids).* The Government intends to evaluate offers and award a contract without discussions with offerors. Therefore, the offeror's initial offer should contain the offeror's best terms from a price and technical standpoint. However, the Government reserves the right to conduct discussions if later determined by the Contracting Officer to be necessary. The Government may reject any or all offers if such action is in the public interest; accept other than the lowest offer; and waive informalities and minor irregularities in offers received.

(h) *Multiple awards.* The Government may accept any item or group of items of an offer, unless the offeror qualifies the offer by specific limitations. Unless otherwise provided in the Schedule, offers may not be submitted for quantities less than those specified. The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit prices offered, unless the offeror specifies otherwise in the offer.

(i) *Availability of requirements documents cited in the solicitation.*

(1)(i) The GSA Index of Federal Specifications, Standards and Commercial Item Descriptions, FPMR Part 101-29, and copies of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained for a fee by submitting a request to--

Washington, DC 20407
Telephone (202) 619-8925
Facsimile (202) 619-8978.

(ii) If the General Services Administration, Department of Agriculture, or Department of Veterans Affairs issued this solicitation, a single copy of specifications, standards, and commercial item descriptions cited in this solicitation may be obtained free of charge by submitting a request to the addressee in paragraph (i)(1)(i) of this provision. Additional copies will be issued for a fee.

(2) Most unclassified Defense specifications and standards may be downloaded from the following ASSIST websites:

(i) ASSIST (<https://assist.dla.mil/online/start/>).

(ii) Quick Search (<http://quicksearch.dla.mil/>).

(3) Documents not available from ASSIST may be ordered from the Department of Defense Single Stock Point (DoDSSP) by--

(i) Using the ASSIST Shopping Wizard (<https://assist.dla.mil/wizard/index.cfm>);

(ii) Phoning the DoDSSP Customer Service Desk (215) 697-2179, Mon-Fri, 0730 to 1600 EST; or

(iii) Ordering from DoDSSP, Building 4, Section D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Telephone (215) 697-2667/2179, Facsimile (215) 697-1462.

(4) Nongovernment (voluntary) standards must be obtained from the organization responsible for their preparation, publication, or maintenance.

(j) *Unique entity identifier*. (Applies to all offers that exceed the micro-purchase threshold, and offers at or below the micro-purchase threshold if the solicitation requires the Contractor to be registered in the System for Award Management (SAM).) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation "Unique Entity Identifier" followed by the unique entity identifier that identifies the Offeror's name and address. The Offeror also shall enter its Electronic Funds Transfer (EFT) indicator, if applicable. The EFT indicator is a four-character suffix to the unique entity identifier. The suffix is assigned at the discretion of the Offeror to establish additional SAM records for identifying alternative EFT accounts (see FAR subpart 32.11) for the same entity. If the Offeror does not have a unique entity identifier, it should contact the entity designated at www.sam.gov for unique entity identifier establishment directly to obtain one. The Offeror should indicate that it is an offeror for a Government contract when contacting the entity designated at www.sam.gov for establishing the unique entity identifier.

(k) [Reserved].

(l) Debriefing. If a post-award debriefing is given to requesting offerors, the Government shall disclose the following information, if applicable:

(1) The agency's evaluation of the significant weak or deficient factors in the debriefed offeror's offer.

(2) The overall evaluated cost or price and technical rating of the successful and the debriefed offeror and past performance information on the debriefed offeror.

(3) The overall ranking of all offerors, when any ranking was developed by the agency during source selection.

(4) A summary of the rationale for award;

(5) For acquisitions of commercial products, the make and model of the product to be delivered by the successful offeror.

(6) Reasonable responses to relevant questions posed by the debriefed offeror as to whether source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities were followed by the agency.

(End of provision)

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)
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021)	
52.212-3	Offeror Representations and Certifications-Commercial Products and Commercial Services (Dec 2022)	
52.204-7	System for Award Management (Oct 2018)	
2852.233-70	Protests Filed Directly with the Department of Justice (NOV 2020)	
BOP 2852.237-78	Submission/Evaluation of Quotations/Offers by Individuals (Nov 2014)	
BOP 2852.237-71	Requirements for Religious Services (July 2017)	

Provisions By Full Text

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):

[Insert one or more Internet addresses]

(End of provision)

[END OF ADDENDUM TO FAR 52.212-1]