SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

NOTE: OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24 AND 30.

1. REQUISITION NUMBER: 15B11926PR000159
PAGE 1 OF 42

2. CONTRACT NUMBER
3. AWARD/EFFECTIVE DATE
4. ORDER NUMBER
5. SOLICITATION NUMBER: 15B11926Q00000013
6. SOLICITATION ISSUE DATE: 07/07/2026

7. FOR SOLICITATION INFORMATION CALL:
a. NAME: Jessica Hutchison J2Hutchison@bop.gov
b. TELEPHONE NUMBER (*No collect calls*)
8. OFFER DUE DATE / LOCAL TIME: 08/28/2026 12:00 ET

9. ISSUED BY
Federal Bureau of Prisons
FCI Gilmer
201 FCI LANE
Glenville, WV 26351
CODE 15B119

10. THE ACQUISITION IS
[X] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB)
[ ] UNRESTRICTED OR
[ ] WOMEN-OWNED SMALL BUSINESS (WOSB)
[ ] ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
[ ] 8(A)
[X] SET ASIDE: 100.00 % FOR
NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 561320
SIZE STANDARD: 34,000,000

11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER THE DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM - DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[X] REQUEST FOR QUOTE (RFQ)
[ ] INVITATION FOR BID (IFB)
[ ] REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO
Federal Bureau of Prisons
FCI Gilmer
201 FCI LANE
Glenville, WV 26351
CODE 15B119

16. ADMINISTERED BY
Federal Bureau of Prisons
FCI Gilmer
201 FCI LANE
Glenville, WV 26351
CODE 15B119

17a. CONTRACTOR/ OFFEROR
CODE
FACILITY CODE
TELEPHONE NUMBER

18a. PAYMENT WILL BE MADE BY
Federal Bureau of Prisons
FCI Gilmer
201 FCI LANE
Glenville, WV 26351
CODE 15B119
Business Office
GIL-BusinessOffice-S@bop.gov

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

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

19. ITEM NUMBER	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	BLANKET PURCHASE AGREEMENT TO PROVIDE PHARMACY TECHNICIAN SERVICES IN ACCORDANCE WITH THIS DOCUMENT AND STATEMENT OF WORK Firm Fixed Price See Continuation Sheet(s) (*Use Reverse and/or Attach Additional Sheets as Necessary*)				

25. ACCOUNTING AND APPROPRIATION DATA

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

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

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

[ ] 29. AWARD OF CONTRACT: REFERENCE _____ 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*): Jessica L Hutchison
31c. DATE SIGNED

19. ITEM NUMBER	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

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

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

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

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

Table of Contents

Section	Description	Page Number
	Solicitation/Contract Form	1
1	Commodity or Services Schedule	4
2	Contract Clauses	6
	2852.212-4 Contract Terms and Conditions, Commercial Items (FAR Deviation) (NOV 2020)	6
	52.203-17 Contractor Employee Whistleblower Rights (Nov 2023)	9
	52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)	10
	52.204-13 (DEV) System for Award Management-Maintenance (Oct 2018) (DEVIATION NOV 2025)	10
	52.204-13 Alt I (DEV) System for Award Management-Maintenance (Oct 2018) - Alternate I (DEVIATION NOV 2025)	12
	52.204-19 Incorporation by Reference of Representations and Certifications (Dec 2014)	13
	52.219-6 Alt I (DEV) Notice of Total Small Business Set-Aside (Nov 2020) - Alternate I (Mar 2020) (DEVIATION DEC 2025)	13
	52.222-90 Addressing DEI Discrimination by Federal Contractors (APR 2026)	13
	52.223-23 (DEV) Sustainable Products (May 2024) (DEVIATION DEC 2025)	14
	52.225-1 Alt I (DEV) Buy American-Supplies (Oct 2022) - Alternate I (Oct 2022) (DEVIATION DEC 2025)	15
	52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)	16
	BOP 2852.237-72 DOJ CONTRACTOR RESIDENCY REQUIREMENT BUREAU OF PRISONS (JUNE 2004)	18
	DJAR-PGD-05-08 Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractor	18
	DJAR-PGD-15-02-2A Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - Award (DEVIATION 2015-02) (March 2015)	19
	DJAR-PGD-15-02-2B Contractor Internal Confidentiality Agreements or Statements Prohibiting or Restricting Reporting of Waste, Fraud, and Abuse - Award - (DEVIATION 2015-02) (March 2015)	20
	DOJ-01 Whistleblower Information Distribution (Oct 2021)	20
	DOJ-02 Contractor Privacy Requirements (JAN 2022)	20
	DOJ-03 Personnel Security Requirements For Contractor Employees (Nov 2021)	25
	DOJ-05 Security of Department Information and Systems (APR 2026)	30
3	List of Attachments	38
4	Solicitation Provisions	39
	52.215-1 Alt II (DEV) Instructions to Offerors-Competitive Acquisition (Nov 2021) - Alternate II (DEVIATION DEC 2025)	39

Section 1 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Pharmacy Technician services to be provided in accordance with the statement of work. Funds to be obligated by individual delivery orders. PSC: Q999 **Delivery Schedule:** Quantity: 0.000000 Place of Performance Address: Federal Bureau of Prisons FCI Gilmer 201 FCI LANE Glenville, WV 26351	0		$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Base Year: Date of Award through 12 months, Estimated number of Sessions 1820 (35 hours per week x 52 weeks) PSC: Q999 **Delivery Schedule:** Quantity: 1,820.000000 Place of Performance Address: Federal Bureau of Prisons FCI Gilmer 201 FCI LANE Glenville, WV 26351	1,820		$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003	Option Year 1: 13-24 months from Effective Date of Award (EDOA) PSC: Q999 **Delivery Schedule:** Quantity: 1,820.000000 Place of Performance Address: Federal Bureau of Prisons FCI Gilmer 201 FCI LANE Glenville, WV 26351	1,820		$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004	Option Year 2: 25-36 months from Effective Date of Award (EDOA) PSC: Q999 **Delivery Schedule:** Quantity: 1,820.000000 Place of Performance Address: Federal Bureau of Prisons FCI Gilmer 201 FCI LANE Glenville, WV 26351	1,820		$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT

0005	Option Year 3: 37-48 months from Effective Date of Award (EDOA) PSC: Q999 **Delivery Schedule:** Quantity: 1,820.000000 Place of Performance Address: Federal Bureau of Prisons FCI Gilmer 201 FCI LANE Glenville, WV 26351	1,820		$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0006	Option Year 4: 47-60 months from Effective Date of Award (EDOA) PSC: Q999 **Delivery Schedule:** Quantity: 1,820.000000 Place of Performance Address: Federal Bureau of Prisons FCI Gilmer 201 FCI LANE Glenville, WV 26351	1,820		$_____	$_____

DECISION WILL BE BASED ON BEST VALUE TO THE GOVERNMENT
Estimated contract award 11/01/2026.

Section 2 - Contract Clauses

2852.212-4 Contract Terms and Conditions, Commercial Items (FAR Deviation) (NOV 2020)

When a commercial item is contemplated (using FAR part 12 procedures or otherwise) and the contract will include FAR 52.212-4, the following replaces subparagraph (g)(2); paragraph (h); subparagraph (i)(2); paragraph (s); and paragraph (u), Unauthorized Obligations, of the basic FAR clause, and adds paragraph (w), as follows:
(g)(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment act regulations at 5 CFR part 1315, as modified by subparagraph (i)(2), *Prompt payment,* of this clause.
* * * * *
(h) *Patent indemnity.* Contractor shall indemnify and hold harmless the Government and its respective affiliates, officers, directors, employees, agents, successors and assigns (collectively, “Indemnities”) from and against any and all liability and losses incurred by the Indemnities that are (i) included in any settlement and/or (ii) awarded by a court of competent jurisdiction arising from or in connection with any third party claim of infringement made against Indemnities asserting that any product or service supplied under this contract constitutes infringement of any patent, copyright, trademark, service mark, trade name or other proprietary or intellectual right. This indemnity shall not apply unless Contractor shall have been informed within a reasonable time by the Government of the claim or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. This indemnity also shall not apply to any claim unreasonably settled by the Government which obligates Contractor to make any admission or pay any amount without written consent signed by an authorized officer of Contractor, unless required by final decree of a court of competent jurisdiction.
* * * * *
(i)(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations (5 CFR part 1315), with the following modification regarding the due date: For the sole purpose of computing an interest penalty due the Contractor, the Government agrees to inspect and determine the acceptability of any supply delivered or service performed specified in the invoice within thirty (30) days of receipt of a proper invoice from the Contractor, after which time, if no affirmative action has been taken by the Government to accept such supply or service, the supply or service will be deemed accepted and payment due thirty (30) days from the date of deemed acceptance. If the Government makes the determination that the item delivered or service performed is deficient or otherwise unacceptable, or the invoice is otherwise determined not to be a proper invoice, the terms and conditions of this paragraph regarding prompt payment will apply to the date the Contractor corrects the deficiency in the item delivered or service performed or submits a proper invoice. If actual acceptance occurs within the constructive acceptance period, the Government will base the determination of an interest penalty on the actual date of acceptance. The constructive acceptance requirement does not, however, compel Government officials to accept supplies or services, perform contract administration functions, or make payment prior to fulfilling their responsibilities.
* * * * *
(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:
(1) The schedule of supplies/services.
(2) The Assignments, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts provisions of the basic FAR clause at 52.212-4, and the Unauthorized Obligations and Contractor's Commercial Supplier Agreements—Unenforceable Clauses provisions of JAR 2852.212-4.
(3) FAR 52.212-5.
(4) Other paragraphs of the basic FAR clause at 52.212-4, with the exception of paragraph (o), Warranty, and those paragraphs identified in this deviation of 52.212-4.
(5) Addenda to this solicitation, contract, or order, including contractor's Commercial supplier agreements incorporated into the contract.
(6) Solicitation provisions if this is a solicitation.
(7) Paragraph (o), Warranty, of the basic FAR clause at 52.212-4.
(8) The Standard Form 1449.
(9) Other documents, exhibits, and attachments.
(10) The specification.
* * * * *
(u) *Unauthorized obligations.*
(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract or order is subject to any Commercial supplier agreement that includes any language, provision, or clause requiring the Government

to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (see 31 U.S.C. 1341), the following shall govern:
(i) Any such language, provision, or clause is unenforceable against the Government.
(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an "I agree" click box or other similar mechanism (*e.g.,* "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.
(iii) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement and have no effect.
(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.
* * * * *
(w) *Commercial supplier agreements—unenforceable clauses.* When any supply or service acquired under this contract or order is subject to a contractor's commercial supplier agreement, the following shall be deemed incorporated into such agreement and modifies and replaces any similar language, provision, or clause in such agreement. As used herein, "this agreement" means any contractor commercial supplier agreement:
(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:
(i) *Applicability.* This agreement is a part of a contract between commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR part 12).
(ii) *End user.* This agreement shall bind the Government as end user but shall not operate to bind the Government employee or person acting on behalf of the Government in his or her personal capacity.
(iii) *Law and disputes.* This agreement is governed by Federal law.
(A) Any language, provision, or clause purporting to subject the U.S. Government to the laws of any U.S. state, territory, district, or municipality, or the laws of a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted and shall have no effect.
(B) Any language, provision, or clause requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted and shall have no effect.
(C) Any language, provision, or clause prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted and shall have no effect.
(iv) *Continued performance.* Notwithstanding any other provision in this agreement, if the Contractor believes the Government to be in breach of this contract, order, or agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in subparagraph (d), Disputes, of FAR 52.212-4.
(v) *Arbitration; equitable or injunctive relief.* In the event of a claim or dispute arising under or relating to the contract, order, or this agreement, (A) binding arbitration shall not be used unless otherwise specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the Government only when explicitly provided by statute.
(vi) *Updating terms.*
(A) After award, the contractor may unilaterally revise terms if they are not material. Material terms are defined as:
(1) Terms that change Government rights or obligations;
(2) Terms that increase Government prices;
(3) Terms that decrease the overall level of service; or
(4) Terms that limit any other Government right addressed elsewhere in this contract.
(B) For revisions that materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.
(C) Any agreement terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provisions of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.
(vii) *Order of precedence.* Any Order of Precedence clause in any commercial supplier agreement is not enforceable against the Government. The applicable Order of Precedence for this contract, order, or agreement is FAR 52.212-4(s), as revised by JAR 2812.302 and 2852.212-4(s).
(viii) *No automatic renewals.* If any license or service tied to period payment is provided under this agreement (*e.g.,* annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by a properly warranted contracting officer, and any provision or term of any license or service purporting to provide for automatic renewal is unenforceable against the Government.
(ix) *Indemnification by the Government or end-user.* Any language, provision, or clause of this commercial supplier agreement requiring the Government or End-user to indemnify the commercial supplier or licensor is not enforceable against the Government.

(x) *Indemnification by the commercial supplier or licensor.* Any clause of this agreement requiring or permitting the commercial supplier or licensor to defend the Government as a condition of indemnifying the Government for any claim of infringement is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.
(xi) *Audits.* Any language, provision, or clause of this commercial supplier agreement permitting Contractor to audit the end user's compliance with this agreement is not enforceable against the Government. To the extent any language, provision or clause of this agreement permits Contractor to audit the Government's compliance under this contract, order, or agreement, such language, provision, or clause of this agreement is hereby stricken and replaced as follows:
"(A) If Contractor reasonably believes that the Government has violated the terms of this agreement with regard to the restrictions on authorized use and/or the number of authorized users, upon written request from Contractor, including an explanation of the basis for the request, DOJ will provide a redacted version of the Government's most recent Security Assessment and Authorization package (SAA) to Contractor on a confidential basis, so that Contractor may reasonably verify the Government's compliance with its obligations under this agreement. Contractor understands and agrees that the Government will remove or redact any information from the SAA that it reasonably believes may compromise (a) the security of the Government's information technology environment; (b) the confidentiality of any third-party proprietary or confidential information; (c) any confidential, sensitive law enforcement information; and (d) any other information that the Government believes may compromise a past, current, or prospective investigation, prosecution, or litigation. Notwithstanding the preceding, and subject to the Government's policies and procedures for such review, including but not limited to complying with all Government security requirements prior to being granted access to the Government's facilities, including the execution of appropriate confidentiality and/or non-disclosure agreements, the Government will arrange, upon Contractor's written request, for Contractor to view an un-redacted version of the SAA on Government premises. Contractor understands that Contractor will be provided a copy of the un-redacted SAA on Government premises only and that no un-redacted copy of the SAA, or any medium containing information relating to it, will be permitted to be removed from Government premises.
(B) The Contractor also understands and agrees that the Contractor shall make a request under this paragraph no more than on an annual basis and only during the period of the contract, and that any activities performed by Contractor under this clause will be performed at Contractor's expense, without reimbursement by the Government.
(C) Discrepancies found with regard to the restrictions on authorized use and/or the number of authorized users may result in a charge by Contractor to the Government. Any resulting invoice must comply with the proper invoicing and payment requirements specified in the contract. This charge, if disputed by the Government, will be resolved through the Disputes clause at 52.212-4(d); no payment obligation shall arise on the part of the Government until the conclusion of the dispute process."
(xii) *Taxes or surcharges.* Any taxes or surcharges which the Contractor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.
(xiii) *Non-assignment.* This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under FAR 52.212-4 (b), Assignment.
(xiv) *Confidential information.*
(A) During the term of this contract or order, either party may identify information as "confidential information," and there shall be no disclosure, dissemination, or publication of any such information except to the extent required for the performance of this contract or order and otherwise provided in this clause or by statute or regulation. Specifically, the parties agree that the party receiving confidential information may only disclose such information to its employees and contractors on a "need-to-know" basis to carry out the obligations of this contract or order, and that subcontractors performing under this Agreement are subject to the same stipulations provided in this provision. The parties also agree that this provision shall survive the termination of this contract or order, and any confidential information obtained or received which comes within these restrictions shall remain confidential, provided that the obligation to treat information as confidential shall not apply to information which is or becomes publicly available through no improper action of the receiving party; is or comes to be in the receiving party's possession independent of its relationship with the disclosing party; is developed by or becomes known to the receiving party without use of any confidential information of the disclosing party; or is obtained rightfully from a third party not bound by an obligation of confidentiality. Additionally, nothing in this contract or order shall restrict disclosure by the receiving party pursuant to any applicable law, including but not limited to the Freedom of Information Act, 5 U.S.C. 552, *et seq.,* or an order of any court of competent jurisdiction, provided that in either such case the receiving party gives prompt notice to the disclosing party to allow the disclosing party to interpose an objection to such disclosure, take action to assure confidential handling of the confidential information, or take such other action as it deems appropriate to protect its confidential information.
(B) The Government considers and hereby identifies as confidential any and all information related to any inquiries and/or searches performed by the Government or by contractor at the Government's direction under this contract or order, including the subject of any such inquiry or search and any and all search terms, regardless of whether provided in writing or orally to Contractor, and Contractor agrees that it may only disclose such information to its employees and contractors

on a “need-to-know” basis to carry out the obligations of this contract or order and that it will not share, reveal, divulge, disclose, disseminate, or publicize any such information to any third party except as provided in this provision without the prior written approval of the Contracting Officer. Contractor also understands and agrees that any subcontractors performing under this contract or order are subject to the same stipulations and that Contractor may be held responsible for any violations of confidentiality by a subcontractor.
(C) These provisions are consistent with and do not supersede, conflict with, or otherwise alter an employee's obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by Executive orders and statutory provisions relating to whistleblower protection are incorporated into this contract and are controlling.
(D) The Government may share the terms, conditions and prices set forth in this Order with, and provide a copy of the Order to, other Executive branch agencies of the U.S. Government, provided that the Government shall ensure that other Executive branch agencies to which it provides such information will be required to treat all such information consistent with terms and conditions set forth in this Order.
(E) Notwithstanding anything in this agreement, the Government may retain any confidential information as required by law, regulation, or its internal document retention procedures for legal, regulatory, or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this Order.
(xv) *Authorized users.* Authorized users may include full and part-time employees of the Government, including those working at or from remote locations, and contractors and contractor employees working within the scope of their contract with the Government, including those at or from remote locations.
(xvi) *Authorized use.* Authorized users are authorized to use the product or service acquired under this contract in performing business on behalf of the Government. Any information obtained or acquired by the Government under this contract may be used by the Government in the performance of Government business.
(2) If any language, provision, or clause of this agreement conflicts or is inconsistent with the preceding paragraph (w)(1), the language, provisions, or clause of paragraph (w)(1) shall prevails to the extent of such inconsistency.

A.1 ADDENDUM TO FAR 52.212-4, Contract Terms and Conditions, Commercial Items (FAR Deviation) (NOV 2020)

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 Full Text

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):

ACQUISITION.GOV

_____

_____

[Insert one or more Internet addresses]

(End of clause)

52.203-17 Contractor Employee Whistleblower Rights (Nov 2023)

(a) This contract and employees working on this contract will be subject to the whistleblower rights and remedies established at 41 U.S.C. 4712 and Federal Acquisition Regulation (FAR) 3.900 through 3.905.

(b) The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712, as described in FAR 3.900 through 3.905.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts.

(End of clause)

52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

(a) *Definitions*. As used in this clause--

"Internal confidentiality agreement or statement" means a confidentiality agreement or any other written statement that the contractor requires any of its employees or subcontractors to sign regarding nondisclosure of contractor information, except that it does not include confidentiality agreements arising out of civil litigation or confidentiality agreements that contractor employees or subcontractors sign at the behest of a Federal agency.

"Subcontract" means any contract as defined in subpart 2.1 entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.

"Subcontractor" means any supplier, distributor, vendor, or firm (including a consultant) that furnishes supplies or services to or for a prime contractor or another subcontractor.

(b) The Contractor shall not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (*e.g.,* agency Office of the Inspector General).

(c) The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any preexisting internal confidentiality agreements or statements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(d) The prohibition in paragraph (b) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(e) In accordance with 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) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(End of clause)

52.204-13 (DEV) System for Award Management-Maintenance (Oct 2018) (DEVIATION NOV 2025)

(a) *Definitions*. As used in this clause—

Commercial and Government Entity code means—

(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity by unique location (referred to as “CAGE code”); or

(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency to entities located outside the United States and its outlying areas that the DLA CAGE Branch records and maintains in the CAGE master file (referred to as “NCAGE code”).

Unique Entity Identifier (UEI) means an identifier used to identify a specific commercial, nonprofit, or Government entity.

(b) *Active registration*.

(1) The Contractor shall maintain an active Federal Government contracts registration in the System for Award Management (SAM) at https://www.sam.gov during contract performance and through final payment under this contract. To maintain an active registration in SAM, the Contractor shall review at least annually its registration in SAM and validate that the information is current, accurate, and complete.

(2) The Contractor is responsible for the currency, accuracy, and completeness of the information provided within SAM, and for any liability resulting from the Government’s reliance on inaccurate or incomplete information. Updating SAM does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(c) *Novation and change-of-name agreements*.

(1) If the Contractor has legally changed its business name or “doing business as” name (whichever is shown on the contract), or has transferred the assets used to perform the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in part 42 of the Federal Acquisition Regulation (FAR), the Contractor shall provide the responsible Contracting Officer a minimum of one business day’s written notification of its intention to —

(i) Change the legal business name in SAM;

(ii) Comply with the requirements of FAR part 42; and

(iii) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor shall provide with its written notification sufficient documentation to support the legally changed name.

(2) If the Contractor fails to comply with the requirements of paragraph (c)(1) of this clause, or fails to perform the agreement at paragraph (c)(1)(iii) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the “Suspension of Payment” paragraph of the electronic funds transfer (EFT) clause of this contract.

(d) *Assignees*.

(1) The Contractor shall not change the legal business name or address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see FAR part 32). Assignees shall be separately registered in SAM.

(2) Information provided to the Contractor’s SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be incorrect information within the meaning of the “Suspension of Payment” paragraph of the EFT clause of this contract.

(e) Unique entity identifier (UEI). The Contractor shall ensure that its UEI is maintained throughout the life of the contract.

(f) Commercial and Government Entity (CAGE) code. The Contractor shall ensure that the CAGE code is maintained throughout the life of the contract. To update a CAGE code, the Contractor shall initiate the change by updating its SAM registration.

(g) Communicating changes. The Contractor shall communicate any change to its UEI or CAGE code to the Contracting Officer within 30 days after the change, so a modification can be issued to update the UEI or CAGE code on this contract. A change in the UEI does not necessarily require a novation.

(End of clause)

52.204-13 Alt I (DEV) System for Award Management-Maintenance (Oct 2018) - Alternate I (DEVIATION NOV 2025)

(a) *Definitions*. As used in this clause—

Commercial and Government Entity code means—

(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity by unique location (referred to as “CAGE code”); or

(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency to entities located outside the United States and its outlying areas that the DLA CAGE Branch records and maintains in the CAGE master file (referred to as “NCAGE code”).

Unique Entity Identifier (UEI) means an identifier used to identify a specific commercial, nonprofit, or Government entity.

(b) *Active registration*.

(1) If the Contractor was unable to register for Federal Government contracts in the System for Award Management (SAM) at *https://www.sam.gov* before award, the Contractor shall register in SAM within 30 days after contract award or at least three days before submitting the first invoice, whichever occurs first.

(2) The Contractor shall maintain an active Federal Government contracts registration in SAM during contract performance and through final payment under this contract. To maintain an active registration in SAM, the Contractor shall review at least annually its registration in SAM and validate that the information is current, accurate, and complete.

(3) The Contractor is responsible for the currency, accuracy, and completeness of the information provided within SAM, and for any liability resulting from the Government’s reliance on inaccurate or incomplete information. Updating SAM does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(c) *Novation and change-of-name agreements*.

(1) If the Contractor has legally changed its business name or “doing business as” name (whichever is shown on the contract), or has transferred the assets used to perform the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in part 42 of the Federal Acquisition Regulation (FAR), the Contractor shall provide the responsible Contracting Officer a minimum of one business day’s written notification of its intention to —

(i) Change the legal business name in SAM;

(ii) Comply with the requirements of FAR part 42; and

(iii) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor shall provide with its written notification sufficient documentation to support the legally changed name.

(2) If the Contractor fails to comply with the requirements of paragraph (c)(1) of this clause, or fails to perform the agreement at paragraph (c)(1)(iii) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the SAM information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the “Suspension of Payment” paragraph of the electronic funds transfer (EFT) clause of this contract.

(d) *Assignees*.

(1) The Contractor shall not change the legal business name or address for EFT payments or manual payments, as appropriate, in the SAM record to reflect an assignee for the purpose of assignment of claims (see FAR part 32). Assignees shall be separately registered in SAM.

(2) Information provided to the Contractor's SAM record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be incorrect information within the meaning of the "Suspension of Payment" paragraph of the EFT clause of this contract.

(e) Unique entity identifier (UEI). The Contractor shall ensure that its UEI is maintained throughout the life of the contract.

(f) Commercial and Government Entity (CAGE) code. The Contractor shall ensure that the CAGE code is maintained throughout the life of the contract. To update a CAGE code, the Contractor shall initiate the change by updating its SAM registration.

(g) Communicating changes. The Contractor shall communicate any change to its UEI or CAGE code to the Contracting Officer within 30 days after the change, so a modification can be issued to update the UEI or CAGE code on this contract. A change in the UEI does not necessarily require a novation.

(End of clause)

52.204-19 Incorporation by Reference of Representations and Certifications (Dec 2014)

The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

52.219-6 Alt I (DEV) Notice of Total Small Business Set-Aside (Nov 2020) - Alternate I (Mar 2020) (DEVIATION DEC 2025)

(a) *Definition*. *Small business concern*, as used in this clause—

(1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.

(2) *Affiliates*, as used in paragraph (a)(1) of this clause, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

(b) *Applicability*. This clause applies only to-

(1) Contracts that have been set aside for small business concerns; and

(2) Orders set aside for small business concerns under multiple-award contracts as described in 8.4 and 16.5.

(c) *General*.

(1) Offers are solicited only from small business concerns and Federal Prison Industries, Inc. (FPI). Offers received from concerns that are not small business concerns or FPI shall be considered nonresponsive and will be rejected.

(2) Any award resulting from this solicitation will be made to either a small business concern or FPI.

(End of clause)

52.222-90 Addressing DEI Discrimination by Federal Contractors (APR 2026)

(a) *Definitions*. As used in this clause—
Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of clause)

52.223-23 (DEV) Sustainable Products (May 2024) (DEVIATION DEC 2025)

(a) *Definitions.* As used in this clause—

Sustainable product means—

(1) A product that contains recovered material designated by the EPA under the Comprehensive Procurement Guidelines (42 U.S.C. 6962) (40 CFR part 247) (https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program#products).

(2) An energy-efficient product or low standby power device (42 U.S.C. 8259b) (10 CFR part 436, subpart C) (https://www.energy.gov/eere/femp/search-energy-efficient-products, https://www.energystar.gov/products?s=mega, and https://www.energy.gov/femp/low-standby-power-product-list).

(3) A biobased product that meets the content requirements of the USDA under the BioPreferred® program (7 U.S.C. 8102) (7 CFR Part 4270) (https://www.biopreferred.gov/).

(4) A substance identified in the EPA’s Significant New Alternatives Policy (SNAP) program as a safe alternative to an ozone-depleting substance (42 U.S.C. 7671l) (40 CFR part 82, subpart G) (https://www.epa.gov/snap/unacceptable-and-acceptable-substitutes-tables).

(b) *Requirements*. The Government has identified in the statement of work or elsewhere in the contract the sustainable products that are required during the performance of this contract. The Contractor shall ensure that it provides sustainable products as required by this contract, when the products are—

(1) Delivered to the Government;

(2) Furnished for use by the Government;

(3) Incorporated into the construction of a public building or public work; or

(c) Furnished for use in performing services under this contract, where the cost of the products is a direct cost to this contract.

(End of clause)

52.225-1 Alt I (DEV) Buy American-Supplies (Oct 2022) - Alternate I (Oct 2022) (DEVIATION DEC 2025)

(a) *Definitions.* As used in this clause--

Commercially available off-the-shelf (COTS) item--

(1) Means any item of supply (including construction material) that is–

(i) A commercial product (as defined in paragraph (1) of the definition of "commercial product" at Federal Acquisition Regulation (FAR) 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and

(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

Component means an article, material, or supply incorporated directly into an end product.

Cost of components means--

(1) For components purchased by the Contractor, the acquisition cost, including transportation costs to the place of incorporation into the end product (whether or not such costs are paid to a domestic firm), and any applicable duty (whether or not a duty-free entry certificate is issued); or

(2) For components manufactured by the Contractor, all costs associated with the manufacture of the component, including transportation costs as described in paragraph (1) of this definition, plus allocable overhead costs, but excluding profit. Cost of components does not include any costs associated with the manufacture of the end product.

Critical component means a component that is mined, produced, or manufactured in the United States and deemed critical to the U.S. supply chain. The list of critical components is at FAR 25.105.

Domestic end product means--

(1) For an end product that does not consist wholly or predominantly of iron or steel or a combination of both-

(i) An unmanufactured end product mined or produced in the United States;

(ii) An end product manufactured in the United States, if-

(A) The cost of its components mined, produced, or manufactured in the United States exceeds _____ percent of the cost of all its components. [*Contracting officer to insert the percentage.*]; or

(B) The end product is a COTS item; or

(2) For an end product that consists wholly or predominantly of iron or steel or a combination of both, an end product manufactured in the United States, if the cost of foreign iron and steel constitutes less than 5 percent

of the cost of all the components used in the end product. The cost of foreign iron and steel includes but is not limited to the cost of foreign iron or steel mill products (such as bar, billet, slab, wire, plate, or sheet), castings, or forgings utilized in the manufacture of the end product and a good faith estimate of the cost of all foreign iron or steel components excluding COTS fasteners. Iron or steel components of unknown origin are treated as foreign. If the end product contains multiple components, the cost of all the materials used in such end product is calculated in accordance with the definition of "cost of components".

End product means those articles, materials, and supplies to be acquired under the contract for public use.

Fastener means a hardware device that mechanically joins or affixes two or more objects together. Examples of fasteners are nuts, bolts, pins, rivets, nails, clips, and screws.

Foreign end product means an end product other than a domestic end product.

Foreign iron and steel means iron or steel products not produced in the United States. Produced in the United States means that all manufacturing processes of the iron or steel must take place in the United States, from the initial melting stage through the application of coatings, except metallurgical processes involving refinement of steel additives. The origin of the elements of the iron or steel is not relevant to the determination of whether it is domestic or foreign.

Predominantly of iron or steel or a combination of both means that the cost of the iron and steel content exceeds 50 percent of the total cost of all its components. The cost of iron and steel is the cost of the iron or steel mill products (such as bar, billet, slab, wire, plate, or sheet), castings, or forgings utilized in the manufacture of the product and a good faith estimate of the cost of iron or steel components excluding COTS fasteners.

Steel means an alloy that includes at least 50 percent iron, between 0.02 and 2 percent carbon, and may include other elements.

United States means the 50 States, the District of Columbia, and outlying areas.

(b) 41 U.S.C. chapter 83, Buy American, provides a preference for domestic end products for supplies acquired for use in the United States. In accordance with 41 U.S.C. 1907, the domestic content test of the Buy American statute is waived for an end product that is a COTS item, except that for an end product that consists wholly or predominantly of iron or steel or a combination of both, the domestic content test is applied only to the iron and steel content of the end product, excluding COTS fasteners.

(c) Offerors may obtain from the Contracting Officer a list of foreign articles that the Contracting Officer will treat as domestic for this contract.

(d) The Contractor shall deliver only domestic end products except to the extent that it specified delivery of foreign end products in the provision of the solicitation entitled "Buy American Certificate."

(End of clause)

52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)

(a) *Method of payment*.

(1) All payments by the Government under this contract shall be made by electronic funds transfer (EFT), except as provided in paragraph (a)(2) of this clause. As used in this clause, the term "EFT" refers to the funds transfer and may also include the payment information transfer.

(2) In the event the Government is unable to release one or more payments by EFT, the Contractor agrees to either--

(i) Accept payment by check or some other mutually agreeable method of payment; or

(ii) Request the Government to extend the payment due date until such time as the Government can make payment by EFT (but see paragraph (d) of this clause).

(b) *Contractor's EFT information*. The Government shall make payment to the Contractor using the EFT information contained in the System for Award Management (SAM). In the event that the EFT information changes, the Contractor shall be responsible for providing the updated information to SAM.

(c) *Mechanisms for EFT payment*. The Government may make payment by EFT through either the Automated Clearing House (ACH) network, subject to the rules of the National Automated Clearing House Association, or the Fedwire Transfer System. The rules governing Federal payments through the ACH are contained in 31 CFR Part 210.

(d) *Suspension of payment*. If the Contractor's EFT information in the *SAM* is incorrect, then the Government need not make payment to the Contractor under this contract until correct EFT information is entered into the SAM; and any invoice or contract financing request shall be deemed not to be a proper invoice for the purpose of prompt payment under this contract. The prompt payment terms of the contract regarding notice of an improper invoice and delays in accrual of interest penalties apply.

(e) *Liability for uncompleted or erroneous transfers*.

(1) If an uncompleted or erroneous transfer occurs because the Government used the Contractor's EFT information incorrectly, the Government remains responsible for--

(i) Making a correct payment;

(ii) Paying any prompt payment penalty due; and

(iii) Recovering any erroneously directed funds.

(2) If an uncompleted or erroneous transfer occurs because the Contractor's EFT information was incorrect, or was revised within 30 days of Government release of the EFT payment transaction instruction to the Federal Reserve System, and--

(i) If the funds are no longer under the control of the payment office, the Government is deemed to have made payment and the Contractor is responsible for recovery of any erroneously directed funds; or

(ii) If the funds remain under the control of the payment office, the Government shall not make payment, and the provisions of paragraph (d) of this clause shall apply.

(f) *EFT and prompt payment*. A payment shall be deemed to have been made in a timely manner in accordance with the prompt payment terms of this contract if, in the EFT payment transaction instruction released to the Federal Reserve System, the date specified for settlement of the payment is on or before the prompt payment due date, provided the specified payment date is a valid date under the rules of the Federal Reserve System.

(g) *EFT and assignment of claims*. If the Contractor assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Contractor shall require as a condition of any such assignment, that the assignee shall register separately in SAM and shall be paid by EFT in accordance with the terms of this clause. Notwithstanding any other requirement of this contract, payment to an ultimate recipient other than the Contractor, or a financial institution properly recognized under an assignment of claims pursuant to Subpart 32.8, is not permitted. In all respects, the requirements of this clause shall apply to the assignee as if it were the Contractor. EFT information that shows the ultimate recipient of the transfer to be other than the Contractor, in the absence of a proper assignment of claims acceptable to the Government, is incorrect EFT information within the meaning of paragraph (d) of this clause.

(h) *Liability for change of EFT information by financial agent*. The Government is not liable for errors resulting from changes to EFT information made by the Contractor's financial agent.

(i) *Payment information*. The payment or disbursing office shall forward to the Contractor available payment information that is suitable for transmission as of the date of release of the EFT instruction to the Federal Reserve System. The Government may request the Contractor to designate a desired format and method(s) for delivery of payment information from a list of formats and methods the payment office is capable of executing. However, the Government does not guarantee that any particular format or method of delivery is available at any particular payment office and retains the latitude to use the format and delivery method most convenient to the Government. If the Government makes payment by check in accordance with paragraph (a) of this clause, the Government shall mail the payment information to the remittance address contained in SAM.

(End of clause)

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

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

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

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

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

DJAR-PGD-15-02-2A Corporate Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability - Award (DEVIATION 2015-02) (March 2015)

(a) None of the funds made available by the Department's current Appropriations Act may be used to enter into a contract, memorandum of understanding, or cooperative agreement with a corporation -

(1) convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government, or

(2) that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner

pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability ,
unless an agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(b) By accepting this award or order, in writing or by performance, the offeror/contractor represents that-

(1) the offeror is *not* a corporation convicted of a felony criminal violation under any Federal or State law within the preceding 24 months; and,

(2) the offeror is *not* a corporation that has any unpaid Federal or State tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.
(End of Clause)

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

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

(End of Clause)

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 3.906 & 52.203-17, and commits to distribution. Within 45 days of award, the contractor must provide confirmation to the contracting officer verifying that it has distributed the whistleblower information as required.

(End of Clause)

DOJ-02 Contractor Privacy Requirements (JAN 2022)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

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

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

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

these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

(3) Prior Approval Required to Hire Subcontractors

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

(4) Separation Checklist for Contractor Employees

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

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

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

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

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

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

(2) Safeguarding PII Requirements

Contractor employees must comply with DOJ Order 0904 and other guidance published to the publicly-available Office of Privacy and Civil Liberties (OPCL) Resources page[3] relating to the safeguarding of PII, including the use

of additional controls to safeguard sensitive PII (e.g., the encryption of sensitive PII). This requirement flows down from the Prime Contractor to all Subcontractors and lower tiered subcontracts.

(3) Non-Disclosure Agreement Requirement

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

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

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

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

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

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

(5) Reporting Actual or Suspected Data Breach

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

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

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

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

(i) Narrative or detailed description of the events surrounding the suspected loss or compromise of information.[6] Date, time, and location of the incident.
(ii) Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.
(iii) Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.[7]
(iv) Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.

(v) Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.[8]
(vi) Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
(vii) Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

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

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

(6) Victim Remediation

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

C. <u>Government Records Training, Ownership, and Management</u>

(1) Records Management Training and Compliance

(a) The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the *DOJ Records and Information Training for New Employees (RIM)* training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. The Contractor shall maintain copies of certificates as a record of compliance and must submit an email notification annually to the COR verifying that all employees working under this contract have completed the required records management training.

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

(2) Records Creation, Ownership, and Disposition

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

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

to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

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

D. Data Privacy and Oversight

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

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

(2) Requirements for Contractor IT Systems Hosting Government Data

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

(3) Requirement to Support Privacy Compliance

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

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor shall work with personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST 800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB Circular A-130.

[1] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).
[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), "'personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable

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

(End of Clause)

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

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

1. General Requirements

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

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

(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 penalties.

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. citizenship.

> (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) U.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 below.

(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 required.
(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 required.

(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 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 clause.

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 contract.

(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 badge. 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 submit.

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

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

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-05 Security of Department Information and Systems (APR 2026)

I. Applicability to Contractors and Subcontractors

Section 2839.102 of the Justice Acquisition Regulation (JAR), (48 C.F.R. § 2839.102), applies to this contract. Accordingly, all contractors are obligated to comply with all applicable DOJ security policies, directives, or guidance documents, including the security requirements in the provisions in this contract clause. This contract clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of the contractors and subcontractors (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. The security requirements set forth herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), and any other applicable laws, mandates, contract clauses, DOJ policies, directives or guidance documents and Executive Orders pertaining to the development and operation of Information Systems and/or the protection of Government Information. This clause does not alter or diminish any existing rights, obligations, 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. **Authorization to Operate** ("ATO"), as defined in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-37 Revision 2, is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.

B. **Cloud Computing**, as defined in DOJ Order 0904 Cybersecurity Program, is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models in accordance with NIST SP 800-145.

C. **Covered Contract** is any contract, order or other agreement under which the contractor, or a subcontractor at any tier, including a cloud service provider, may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information (as defined below) in the course of providing a product or service to the Department, with the exception of acquisitions under the micro-purchase threshold.

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

E. **Data** means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data, computer software, and personally identifiable information (PII) (defined below). The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

F. **DOJ Information**, as defined in DOJ Order 0904, 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 the Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired to perform the contract.

G. **Information**, as defined in DOJ Order 0904, is 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. This includes any communication or representation of knowledge in an electronic format that allows it to be stored, retrieved, or transmitted.

H. **Information System**, means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

I. **Personally Identifiable Information** ("PII"), as defined in the FAR 24.101, 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. It includes but is not limited to common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers or other government-issued identifiers, precise location information, medical history, and biometric records. This definition covers all PII that is created by or becomes available to the contractor, including its employees, subcontractors, or affiliates, as a result of performing under this contract. PII, as supplementally defined in DOJ Order 0904, also includes 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.

J. **Private Cloud**, as defined in NIST SP 800-145, is the deployment model for cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

K. **Security Breach** means any security incident (as defined below) that directly relates to the loss of control, compromise, exfiltration, manipulation, unauthorized disclosure, unauthorized acquisition, unauthorized exposure or unauthorized access or any similar occurrence of any Covered Information System or any DOJ Information or any PII accessed by, retrievable from, processed by, stored on, or transmitted within, to or from any such system. This includes incidents where (1) a person other than an authorized user accesses or potentially accesses PII or DOJ Information or (2) an authorized user accesses or potentially accesses PII or DOJ Information for an unauthorized purpose.

a. **Potential Security Breach** (hereinafter, "Potential Breach") means any suspected, but unconfirmed security breach (as defined above).
b. **Confirmed Security Breach** (hereinafter, "Confirmed Breach") means any confirmed security breach (as defined above).

L. **Security Incident** means any occurrence that (1) may actually or imminently jeopardize, without lawful authority, the availability, integrity, authentication, confidentiality, or nonrepudiation of DOJ Information or a Covered Information System; or (2) may constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

a. **Potential Security Incident** means any suspected, but unconfirmed security incident (as defined above).
b. **Confirmed Security Incident** means any confirmed security incident (as defined above).

M. **Vulnerability**, as defined in DOJ Vulnerability Management Plan, and the OCIO Information Security Management Procedure, means a weakness or flaw discovered in the design of a system that, when exploited, may result in a loss of confidentially, integrity, or availability of DOJ Information or an Information System.

III. Confidentiality and Non-Disclosure of DOJ Information

A. Preliminary and final contract deliverables and all associated working papers and material generated by the Contractor developed using DOJ Information, product, source code, and/or methods of operations, 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 (Rights in Data-General). The Contractor will define a method of monitoring the development activity to include any activity associated with DOJ Information, product, source code, and methods of operations. The data rights and development details shall be defined within the Contract.

If the Contractor intends to utilize its existing data, for which it has a patent or copyright, to develop a contract deliverable, it is incumbent upon the Contractor to negotiate with the CO the proper FAR Part 27 clauses in the contract to protect its existing data.

B. Pursuant to FAR 52.227-14(d)(2), all documents and data produced in the performance of this contract containing DOJ Information, product code, source code, and/or methods of operations are the property of the U.S. Government and, without the prior written permission of the CO, the Contractor shall neither reproduce nor release such information to any third-party at any time, including during performance or following expiration and/or termination of the contract.

C. Any DOJ Information made available to the 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, the Contractor assumes responsibility for the protection of the confidentiality of all DOJ Information processed, stored, or transmitted by the Contractor. The Contractor shall comply with information security responsibilities and duties throughout the contract and after expiration/ termination as appropriate per contract close-out activities. When requested by the CO (typically no more than annually), the Contractor shall provide a report to the CO identifying, to the best of the 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, in addition to any other applicable requirements, as set forth in Part I, the Contractor shall comply with the security requirements of the Federal Information Security Modernization 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, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards as amended, and OMB Memoranda relating to the security of information and/ or Federal Information Systems.

B. In addition, for all Covered Information Systems, the Contractor shall comply with the following requirements, which are listed here only to highlight certain specific applicable requirements from one of the sources identified in the first paragraph of this Section. This is not an exhaustive list of all such requirements with which the Contractor is obligated to comply, and the omission of a requirement from this list should not be construed as negating the materiality of that requirement. These requirements and those in the authorities in the prior paragraph should be read together.

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 at least annually to all Contractor employees and contractors involved with the Covered Contract. Such training shall include, but not be 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, in accordance with applicable requirements but in any event at least until the expiration of the contract, 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, to include but not be limited to, collecting, reviewing, and analyzing appropriate logs and timely investigating security alerts and potential security incidents.
6. Establishing and maintaining baseline configurations and current 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 Covered 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 as defined by NIST 800-63-3, Digital Identity Guidelines or current revision.
9. Establishing and maintaining an operational incident handling capability for Covered Information Systems that includes adequate and timely development, logging, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and timely reporting incidents to appropriate officials and authorities within the 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.
11. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media, and DOJ assets under Contractor control; protecting them from environmental impacts, access, and equipment positioning requirements defined; 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.
12. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized personnel according to DOJ 03.
13. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards including personnel background checks.
14. Continuously assessing the risk to DOJ Information in Covered Information Systems, including scanning and remediating vulnerabilities, or implementing appropriate mitigation in accordance with DOJ policy, and ensuring the timely removal of assets no longer supported by the Contractor.
15. Continuously monitoring the application of security controls of Covered Information Systems, assessing the efficacy of such controls, and developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Covered Information Systems.
16. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Covered Information Systems, and employing architectural designs, software development techniques, and systems engineering principles that promote effective security.
17. 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 and timely action in response.
18. Ensuring return of Government Furnished Equipment ("GFE") and/or PIV card assets within 10 business days of notification for end of use (contract end, staff change, etc.).
19. Complying with rights in data (FAR 52.227-14) as to the development, management, and protection of DOJ Information.
20. Reporting on risks or known issues impacting DOJ Services (staffing, hardware, process, changes, etc.) through the Contractor's CO or COR, DOJ Service Owner ("SO"), and Government Technical Manager ("GTM") including risk mitigation activities.
21. Reporting through the Contractor's CO or COR on any projected or planned changes in corporate ownership, covered information system design, and/or any technical changes that could impact the confidentiality, integrity or availability of DOJ Information, data, or systems. Changes to system design must be updated through the authorization process per NIST SP 800-37 Revision 2, Step 6 ('Continuous Monitoring") or current NIST revision.
22. When, as part of operating within the DOJ environment, the Contractor's covered information system is subject to review, audit, or assessment by third parties, facilitating DOJ access to information system resources, facilities, personnel, and documentation in a timely manner as required by the auditors. Should a third-party organization conduct a review of any Covered Information System, the Contractor must provide a copy of the report to DOJ, through the CO and COR.
23. To enhance software supply chain and transparency, upon request, the Contractor shall provide a current Software Bill of Materials (SBOM) for all software, software updates, modules, libraries, and container images delivered or operated in the performance of this contract, consistent with applicable federal policy such as the National Telecommunications and Information (NTIA)-established minimum elements for SBOM to the CO who will refer to the DOJ Cyber-Security Risk Management team (C-SCRM) [Authority: OMB M-26-05; EO 14028/ NTIA minimum requirements].
24. Reporting on outages impacting DOJ Services through the Contractor's CO, COR, and DOJ Service Owner (SO) to include event and mitigation details.

C. The Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an 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. (For Cloud Computing Systems, see Section V, below.)

D. The Contractor shall ensure compliance with DOJ-03 (Personnel Security Requirements for Contractor Employees) as to all Covered Information Systems.

E. When requested by the DOJ CO or COR as described below, the 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 the 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, the Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

F. The use of Contractor-owned laptops or other portable digital or electronic media to process or store DOJ Information covered by this clause or access a Covered Information System is prohibited unless the CO approves it in writing after the Contractor has provided a letter certifying compliance with the following requirements. For any requirements which include the use or storage of PII, the Senior Component Official for Privacy must also approve. Any additional requirements set forth for the use or storage of PII under DOJ-02, Contractor Privacy Requirements, are in addition to, not superseded by, the requirements set forth here.

1. Media must be encrypted using a NIST FIPS 140-2 approved product.
2. The 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. The 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 should be treated by the Contractor as sensitive information unless specifically designated as non-sensitive by the DOJ.
5. A Rules of Behavior (ROB) form must be signed and acknowledged annually 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 users that they have no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other portable digital or electronic media.
6. Cybersecurity Awareness Training (CSAT) shall be provided annually by Contractor for all users of Covered Information System. This training must be submitted to, and approved by, the CO or COR in advance of being provided to users. Users must complete and acknowledge having received CSAT each year. At a minimum, CSAT provided by contractors must include:
    a. Insider Threat Detection and Reporting – Importance of detecting, methodologies, indicators, and reporting
    b. Privacy Awareness – Privacy Act and PII
    c. General Cybersecurity – Information security, trends in advance persistent threats, social engineering/phishing, appropriate use, mobile devices, remote access, basic security best practices

G. Contractors shall not store DOJ information on Contractor-owned removable IT (e.g., media such as a thumb drive or external hard drive) unless expressly authorized in writing by the DOJ CO or COR in the performance of their contract.

H. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

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

J. The Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 10 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 in a format and form acceptable to DOJ. The

Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 10 business days of the removal and return of all DOJ Information.

K. DOJ, at its discretion, may suspend the Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that the Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident or Security Breach (see definitions above), 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. Any termination action taken because of the Contractor's suspected failure to comply with any security requirement will be conducted in accordance with the applicable termination clause governing the awarded contract. The Contractor understands that any suspension or termination in accordance with this provision shall be at no cost to DOJ, and that upon request by the CO, the Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at the Contractor's expense. The Contractor must comply with FAR 52.227-14 (Rights in Data), FAR 52.245-1 (Government Property), DOJ 2400.3A Chapter 1 (component property procedures), and FAR 4.804-5(a)(6) (Procedures for closing out contract files).

V. Cloud Computing

A. The Contractor may not utilize the Cloud system of any Cloud Service Provider ("CSP") unless:

1.
    1. All of the following has occurred: (a) the Cloud system and CSP have been evaluated by a Third Party Assessing Organization ("3PAO") certified under FedRAMP; (b) the Cloud system received FedRAMP authorization; (c) the Contractor has provided the most current System Security Plan ("SSP") and Security Assessment Report ("SAR") to the DOJ CO for consideration, and provides any subsequent SSPs and SARs within 30 days of issuance; and, (d) the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under the Covered Contract has issued an ATO; or,
    2. In cases where the CSP or its offering is not FedRAMP authorized, the COR approves utilization of the Cloud System after the CSP has worked with the authorizing official, the DOJ OCIO, and the FedRAMP Program Management Office to determine that the CSP is likely to seek and receive Agency/FedRAMP authorization within 1 year, or DOJ has authorized use as a Private Cloud or Contractor Owned, Contractor Operated system.

B. The 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.

C. The Contractor must ensure that the CSP provides access and information to support and enable DOJ's cloud security posture management, to include the current inventory of security management configuration data for services and information to confirm the Contractor has been monitoring accounts for compliance with security requirements. The DOJ Justice Security Operations Center (JSOC) must be able to access logs and events to investigate potential security breaches and perform security posture assessments associated with the Security Audit Identity Credential Access Management (ICAM) policies.

D. The Contractor must ensure that the CSP provides evidence of annual recertification of privileged user access management.

E. A C-SCRM review is mandatory for specified acquisitions in accordance with established process in EO 14028 and NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, or superseding document. All vendor products and solutions to be used on DOJ national security systems, enterprise-wide systems, or new FIPS-199 High and Moderate systems for the purpose of accessing, collecting, storing, processing, maintaining, using, sharing, retrieving, disseminating, transmitting, or disposing of DOJ Information must be submitted to DOJ OCIO for a C-SCRM review prior to contract award or ATO signature. Changes in corporate ownership or structure shall be reported to the CO for referral to C-SCRM. The Contractor shall notify the CO of any confirmed Supply Chain compromise affecting the Contractor's products or services within 1 hour of discovery.

__ The following C-SCRM requirements for acquisition of systems, hardware, or software which will be used in systems that are mission critical or process sensitive data apply to this award. **(CO check as appropriate in coordination with the Program Manager and/or System Owner)**

1. The Contractor shall develop and deliver a C-SCRM Plan. The C-SCRM Plan shall meet the format described in NIST SP 800-161, Appendix E. The C-SCRM plan shall address the following security controls from NIST SP 800-53 Rev 5: SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-10, and SR-11. Equivalent ISO 27000 series controls may be used if they are mapped to the NIST control(s).
2. The Contractor shall implement the required security controls as documented in the C-SCRM Plan. The requirements of the C-SCRM plan shall flow down to all subcontractors. Evidence of the certification and compliance is required.
3. For cloud platforms or managed services, upon request, the Contractor shall provide a current SBOM of the runtime production environment reflecting the software components and dependencies materially present in the service.
4. The Contractor shall provide evidence of compliance with the documented C-SCRM Plan. (CO select which applies)

__ Self-assessment by a contractor security team
__ External assessment by an independent auditor

VI. Information System Security Incident

A. Confirmed Security Incident. The Contractor shall immediately (and in no event later than 1 hour of discovery) report any Confirmed Security Incident to the DOJ CO and COR. If the Confirmed Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call JSOC at 1-202-357-7000 immediately (and in no event later than within 1 hour of discovery of the Confirmed Security Incident) and shall notify the CO and COR as soon as practicable.

B. Potential Security Incident.

1. If the Contractor suspects that DOJ information has been potentially disclosed or impacted, the Contractor shall promptly investigate to determine if a Security Incident has occurred. If the Contractor has not determined within 24 hours (i.e., 24 hours from detection of potential security incident and/or security breach) whether the Potential Security Incident was in fact a Security Incident, then it must immediately report the Potential Security Incident to the DOJ CO and the COR. If the time by which to report the Potential Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call or e-mail the JSOC Team at 1-202-357-7000 or JSOC@USDOJ.GOV and contact the DOJ CO and COR as soon as practicable. If the contract involves PII, the Contractor must comply with the notification requirements of DOJ-02 and Executive Order M-17-12 (Memorandum on Preparing for and Responding to a Breach of Personally Identifiable Information), Contractor Privacy Requirements, Section B.5, for an actual or suspected Security Incident.
2. The Contractor must limit sharing of Security Incident details to only those individuals involved in responding to the potential Security Incident. Any provisions of the Covered Contract regarding the citizenship or location of individuals working on the Covered Contract apply equally to individuals involved in responding to any potential Security Incidents. The Contractor may request assistance from the JSOC for advice, incident response, or FBI coordination. The Contractor must provide weekly updates to CO, COR and JSOC during the course of a Security Incident investigation.

C. Any report submitted in accordance with paragraphs (B) and (C), above, shall identify:

1. Both the Covered 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 the Contractor to minimize, remedy, and/or investigate the Security Incident.
3. Any and all other information as required by the CISA Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and

The Contractor may request assistance from the JSOC Team for advice, incident response, or FBI coordination, and must provide weekly updates to CO, COR, and JSOC during the course of an Incident investigation.

D. Except as otherwise required by Federal, State and local laws, executive orders, rules and regulations, all determinations regarding whether and when to notify other individuals and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials, the DOJ Core Management Team, or the COR at DOJ's discretion.

E. The Contractor must provide to DOJ full access to any facility and/or Covered Information System affected or potentially affected by any potential or confirmed Security Incident, 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.

F. DOJ, at its sole discretion, may obtain, and the Contractor will permit, the assistance of other federal agencies and/or third-party contractors or firms to aid in response activities related to any potential or confirmed Security Incident. Additionally, DOJ, at its sole discretion, may require the Contractor to retain, at the Contractor's expense, a 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 Covered Information Systems.

G. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by the 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. The 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. Pass-Through of Security Requirements to Subcontractors and CSPs

A. The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with the contract, including any CSP providing services for any other CSP under the contract, and the 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 the Contractor.

(End of Clause)

[END OF ADDENDUM TO FAR 52.212-4]

Section 3 - List of Attachments

Identifier	Title	Number of Pages
2	Statement of Work.pdf	5

Section 4 - Solicitation Provisions

Provisions By Full Text

52.215-1 Alt II (DEV) Instructions to Offerors-Competitive Acquisition (Nov 2021) - Alternate II (DEVIATION DEC 2025)

(a) *Definitions*. As used in this provision-

In writing, *writing*, or *written* means any worded or numbered expression that can be read, reproduced, and later communicated, and includes electronically transmitted and stored information.

Proposal modification is a change made to a proposal before the request for proposal closing date and time, or made in response to an amendment, or made to correct a mistake at any time before award.

Proposal revision is a change to material elements of a proposal made after the request for proposal closing date, at the request of or as allowed by a Contracting Officer, as the result of negotiations.

Time, if stated as a number of days, is calculated using calendar days, unless otherwise specified, and will include Saturdays, Sundays, and legal holidays. However, if the last day falls on a Saturday, Sunday, or legal holiday, then the period shall include the next working day.

(b) *Amendments to requests for proposals.* If this request for proposal (RFP) is amended, all terms and conditions that are not amended remain unchanged. Offerors shall acknowledge receipt of any amendment to this RFP by the date and time specified in the amendment(s).

(c) Submission, modification, revision, and withdrawal of proposals.(1)(i) Proposals and modifications to proposals shall be—

(A) Submitted using the method and the format specified in the RFP;

(B) Addressed to the office specified in the RFP; and

(C) Showing the time and date specified for receipt, the RFP number, and the name and address of the offeror.

(ii) Offerors using commercial carriers should ensure that the proposal is marked on the outermost wrapper with the information in paragraphs (c)(1)(i)(B) and (C) of this provision.

(2) The first page of the proposal must show—

(i) The RFP number;

(ii) The name, address, and telephone number of the offeror (and electronic address if available);

(iii) A statement specifying the extent of agreement with all terms, conditions, and provisions included in the RFP and agreement to furnish any or all items upon which prices are offered at the price set opposite each item;

(iv) Names, titles, and telephone number (and electronic addresses if available) of persons authorized to negotiate on the offeror’s behalf with the Government in connection with this RFP; and

(v) Name, title, and signature of person authorized to sign the proposal. Proposals signed by an agent shall be accompanied by evidence of that agent's authority, unless that evidence has been previously furnished to the issuing office.

(3)(i) Offerors are responsible for submitting proposals, and any modifications or revisions, so as to reach the Government office designated in the RFP by the time specified in the RFP. If no time is specified in the RFP, the time for receipt is 4:30 p.m., local time, for the designated Government office on the date that proposal or revision is due. (ii)(A) Any proposal, modification, or revision received at the Government office designated in the RFP 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-

(1) If it was transmitted through an electronic commerce method authorized by the RFP, 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 proposals; or

(2) 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

(3) It is the only proposal received.

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

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

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

(v) Proposals may be withdrawn by written notice received at any time before award. Oral proposals in response to oral RFPs may be withdrawn orally. Proposals may be withdrawn in person by an offeror or an authorized representative, if the identity of the person requesting withdrawal is established and the person signs a receipt for the proposal before award.

(4) Unless otherwise specified in the RFP, the offeror may propose to provide any item or combination of items.

(5) Offerors shall submit proposals in response to this RFP in English, unless otherwise permitted by the RFP, and in U.S. dollars, unless the provision at FAR 52.225-17, Evaluation of Foreign Currency Offers, is included in the RFP.

(6) Offerors may submit modifications to their proposals at any time before the RFP closing date and time, and may submit modifications in response to an amendment, or to correct a mistake at any time before award.

(7) Offerors may submit revised proposals only if requested or allowed by the Contracting Officer.

(8) Proposals may be withdrawn at any time before award. Withdrawals are effective upon receipt of notice by the Contracting Officer.

(9) Offerors may submit proposals that depart from stated requirements. Such proposals shall clearly identify why the acceptance of the proposal would be advantageous to the Government. Any deviations from the terms and conditions of the RFP, as well as the comparative advantage to the Government, shall be clearly identified and explicitly defined. The Government reserves the right to amend the RFP to allow all offerors an opportunity to submit revised proposals based on the revised requirements.

(d) *Offer expiration date*. Proposals in response to this RFP will be valid for the number of days specified on the RFP cover sheet (unless a different period is proposed by the offeror).

(e) *Restriction on disclosure and use of data*. Offerors that include in their proposals data that they do not want disclosed to the public for any purpose, or used by the Government except for evaluation purposes, shall-

(1) Mark the title page with the following legend:

Mark the title page with the following legend: This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of, or in connection with, the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]; and

(2) Mark each sheet of data it wishes to restrict with the following legend:

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

(f) Contract award.(1) The Government intends to award a contract or contracts resulting from this RFP to the responsible offeror(s) whose proposal(s) represents the best value after evaluation in accordance with the factors and subfactors in the RFP.

(2) The Government may reject any or all proposals if such action is in the Government’s interest.

(3) The Government may waive informalities and minor irregularities in proposals received.

(4) The Government intends to evaluate proposals and award a contract without negotiations with offerors (except clarifications as described in FAR 15.202(b)). Therefore, the offeror's initial proposal should contain the offeror's best terms from a cost or price and technical standpoint. The Government reserves the right to conduct negotiations if the Contracting Officer later determines them to be necessary. If the Contracting Officer determines that the number of proposals that would otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly evaluated proposals.

(5) The Government reserves the right to make an award on any item for a quantity less than the quantity offered, at the unit cost or prices offered, unless the offeror specifies otherwise in the proposal.

(6) The Government reserves the right to make multiple awards if, after considering the additional administrative costs, it is in the Government’s best interest to do so.

(7) The Government may determine that a proposal is unacceptable if the prices proposed are materially unbalanced between line items or subline items. Unbalanced pricing exists when, despite an acceptable total evaluated price, the price of one or more line items is significantly overstated or understated as indicated by the application of cost or price analysis techniques. A proposal may be rejected if the Contracting Officer determines that the lack of balance poses an unacceptable risk to the Government.

(8) If a cost realism analysis is performed, cost realism may be considered by the source selection authority in evaluating performance or schedule risk.

(9) A written award or acceptance of proposal mailed or otherwise furnished to the successful offeror within the time specified in the proposal shall result in a binding contract without further action by either party.

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

(i) The agency's evaluation of the significant weaknesses or deficiencies in the debriefed offeror's offer.

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

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

(iv) A summary of the rationale for award.

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

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

(vii) For DoD contracts in excess of $10 million but not in excess of $100 million with a small business or nontraditional defense contractor (10 U.S.C. 3014), an option for the contractor to request disclosure of the agency's written source selection decision document, redacted to protect the confidential and proprietary information of other offerors for the contract award.

(viii) For award of a DoD contract in excess of $100 million, disclosure of the agency's written source selection decision document, redacted to protect the confidential and proprietary information of other offerors for the contract award.

(End of provision)