SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

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

1. REQUISITION NUMBER	PAGE 1 OF
15B41826PR000696	34

2. CONTRACT NUMBER	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			15B41826Q00000004	09/11/2026

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (*No collect calls*)	8. OFFER DUE DATE / LOCAL TIME
	C. Livingston C1livingston@bop.gov		09/16/2026 11:00 ET

9. ISSUED BY — CODE 15B418
Federal Bureau of Prisons
FCC Terre Haute
4700 Bureau Road South
Contracting Office
Terre Haute, IN 47802

10. THE ACQUISITION IS
- [X] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB)
- [ ] UNRESTRICTED OR [X] SET ASIDE: 100.00 % FOR
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB)
- [ ] ECONOMICALLY DISADVANTAGED WOMEN-OWNED SMALL BUSINESS (EDWOSB)
- [ ] 8(A)

NORTH AMERICAN INDUSTRY CLASSIFICATION STANDARD (NAICS): 333413
SIZE STANDARD: 500 Employees

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 — CODE 15B418
Federal Bureau of Prisons
FCC Terre Haute
4700 Bureau Road South
Contracting Office
Terre Haute, IN 47802

16. ADMINISTERED BY — CODE 15B418
Federal Bureau of Prisons
FCC Terre Haute
4700 Bureau Road South
Contracting Office
Terre Haute, IN 47802
Carl Livingston
C1livingston@bop.gov

17a. CONTRACTOR/ OFFEROR — CODE — FACILITY CODE
TELEPHONE NUMBER

18a. PAYMENT WILL BE MADE BY — CODE 15B418
Federal Bureau of Prisons
FCC Terre Haute
4700 Bureau Road South
Contracting Office
Terre Haute, IN 47802
N. Kelly
Nkelly@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
	Delivery Date: 10/26/2026 Exhaust Fans for FCC Terre Haute Camp Roof SEE LINE ITEMS FOR DETAILS 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 1 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*)	31c. DATE SIGNED
		Carl Livingston	

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

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(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 1 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	Belt Driven Upblast Centrifugal Roof Exhaust Fans with grease traps, heat baffles, hinged roof curbs, V-belt drives, and 1 ½ H.P. ODP 208/60/3 motors.The full load amp draw will be 6.6 amps Standard Curb Cap Size (in): 34 x 34 Roof Opening(in): 30.5 x 30.5 PSC: 4140 **Line Period of Performance:** 09/11/2026 - 10/26/2026 **Delivery Schedule:** **Delivery Description:** Delivery Number: 1 Delivery Requested By: 10/26/2026 Quantity: 7.000000 Delivery Address: Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	7	EA	$_____	$_____

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Belt Driven Propeller Hooded Roof Exhaust Fans with gravity backdraft dampers. These fans will have 2 H.P. 208/60/3 motors. The full load amp draw will be 7.5 amps Roof Opening (in.): 62.5 x 62.5 PSC: 4140 **Line Period of Performance:** 09/11/2026 - 10/26/2026 **Delivery Schedule:** **Delivery Description:** Delivery Number: 1 Delivery Requested By: 10/26/2026 Quantity: 8.000000 Delivery Address: Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	8	EA	$_____	$_____

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003	16 x 33 Fresh Air Intakes with galvanized construction, and birdscreens. 16 x 33 Fresh Air Intakes with galvanized construction, and birdscreens. PSC: 4140 **Line Period of Performance:** 09/11/2026 - 10/26/2026 **Delivery Schedule:** **Delivery Description:** Delivery Number: 1 Delivery Requested By: 10/26/2026 Quantity: 2.000000 Delivery Address: Federal Bureau of Prisons FCC Terre Haute	2	EA	$_____	$_____

	4700 Bureau Road South Contracting Office Terre Haute, IN 47802				
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004	Belt Driven Centrifugal Roof Exhaust Fan with aluminum birdscreen, disconnect switch, gravity backdraft damper, V-belt drive, and½ H.P. ODP 115/60/1 motor. The full load amp draw is 9.8 amps. Roof Opening (in.) 26.5 x x26.5 PSC: 4140 **Line Period of Performance:** 09/11/2026 - 10/26/2026 **Delivery Schedule:** **Delivery Description:** Delivery Number: 1 Delivery Requested By: 10/26/2026 Quantity: 1.000000 Delivery Address: Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	1	EA	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005	Belt Driven Centrifugal Roof Exhaust Fans with aluminum bird screens, disconnect switches, gravity backdraft dampers, V-belt drives, and½ H.P. ODP 208/60/3 motors. The full load amp draw is 2.4 amps. Roof Opening (in.): 26.5 x 26.5 PSC: 4140 **Line Period of Performance:** 09/11/2026 - 10/26/2026 **Delivery Schedule:** **Delivery Description:** Delivery Number: 1 Delivery Requested By: 10/26/2026 Quantity: 3.000000 Delivery Address: Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	3	EA	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0006	Belt Driven Centrifugal Roof Exhaust Fans with aluminum birdscreens, disconnect switches, gravity backdraft dampers, V-belt drives, curb cap adapters for 30" x 30" roof curbs, and ¼ H.P. ODP 115/60/1 motors. The full load amp draw is 5.8 amps. Roof Opening (in.): 30.5 x 30.5 PSC: 4140 **Line Period of Performance:** 09/11/2026 - 10/26/2026 **Delivery Schedule:** **Delivery Description:** Delivery Number: 1 Delivery Requested By: 10/26/2026 Quantity: 4.000000 Delivery Address: Federal Bureau of Prisons FCC Terre Haute 4700 Bureau Road South Contracting Office Terre Haute, IN 47802	4	EA	$_____	$_____

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 Reference

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)		
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov		
Clause	Title	Fill-ins (if applicable)
52.203-17	Contractor Employee Whistleblower Rights (Nov 2023)	
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)	
52.204-13 (DEV)	System for Award Management-Maintenance (Oct 2018) (DEVIATION NOV 2025)	

Clause	Title	Fill-ins (if applicable)
52.209-6 (DEV)	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (Jan 2025) (DEVIATION NOV 2025)	
52.209-10 (DEV)	Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015) (DEVIATION NOV 2025)	
52.212-4 (DEV)	Terms and Conditions-Commercial Products and Commercial Services (Nov 2023) (DEVIATION NOV 2025)	
52.219-6 (DEV)	Notice of Total Small Business Set-Aside (Nov 2020) (DEVIATION DEC 2025)	
52.222-19 (DEV)	Child Labor-Cooperation with Authorities and Remedies (Jan 2025) (DEVIATION MAR 2026)	
52.222-36 (DEV)	Equal Opportunity for Workers with Disabilities (Jun 2020) (DEVIATION DEC 2025)	
52.222-50 (DEV)	Combating Trafficking in Persons (Oct 2025) (DEVIATION DEC 2025)	
52.222-90	Addressing DEI Discrimination by Federal Contractors (APR 2026)	
52.223-23 (DEV)	Sustainable Products (May 2024) (DEVIATION DEC 2025)	
52.226-8	Encouraging Contractor Policies To Ban Text Messaging While Driving (May 2024)	
52.232-33	Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)	
52.233-3 (DEV)	Protest after Award (Aug 1996) (DEVIATION NOV 2025)	
52.233-4 (DEV)	Applicable Law for Breach of Contract Claim (Oct 2004) (DEVIATION NOV 2025)	

Clauses By Full Text

52.222-3 (DEV) Convict Labor (June 2003) (DEVIATION DEC 2025)

(a) Except as provided in paragraph (b) of this clause, the Contractor must not employ in the performance of this contract any person undergoing a sentence of imprisonment imposed by any court of a State, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, or the U.S. Virgin Islands.

(b) The Contractor is not prohibited from employing persons—

(1) On parole or probation to work at paid employment during the term of their sentence;

(2) Who have been pardoned or who have served their terms; or

(3) Confined for violation of the laws of any of the States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, or the U.S. Virgin Islands who are authorized to work at paid employment in the community under the laws of such jurisdiction, if-

(i) The worker is paid or is in an approved work training program on a voluntary basis;

(ii) Representatives of local union central bodies or similar labor union organizations have been consulted;

(iii) Such paid employment will not result in the displacement of employed workers, or be applied in skills, crafts, or trades in which there is a surplus of available gainful labor in the locality, or impair existing contracts for services;

(iv) The rates of pay and other conditions of employment will not be less than those paid or provided for work of a similar nature in the locality in which the work is being performed; and

(v) The Attorney General of the United States has certified that the work-release laws or regulations of the jurisdiction involved are in conformity with the requirements of Executive Order11755, as amended by Executive Orders 12608 and 12943.

(End of clause)

52.225-1 (DEV) Buy American-Supplies (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 60 percent of the cost of all its components, except that the percentage will be 65 percent for items delivered in calendar years 2024 through 2028 and 75 percent for items delivered starting in calendar year 2029. Components of foreign origin of the same class or kind as those that the agency determines are not mined, produced, or manufactured in sufficient and reasonably available commercial quantities of a satisfactory quality are treated as domestic. Components of unknown origin are treated as foreign. Scrap generated, collected, and prepared for processing in the United States is considered domestic; 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)

DOJ-02 Contractor Privacy Requirements (JAN 2022)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

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

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

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

(3) Prior Approval Required to Hire Subcontractors

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

(4) Separation Checklist for Contractor Employees

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

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

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

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

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

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

(2) Safeguarding PII Requirements

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

(3) Non-Disclosure Agreement Requirement

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

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

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

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

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

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

(5) Reporting Actual or Suspected Data Breach

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

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

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

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

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

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

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

(6) Victim Remediation

At DOJ's request, the Contractor is responsible for notifying victims and providing victim remediation services in the event of a breach of PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose PII was lost or compromised. When DOJ requests notification, the Department Chief Privacy and Civil Liberties Officer and SCOP will direct the Contractor on the method and content of such notification to be sent to individuals whose

PII was breached. By performing this work, the Contractor agrees to full cooperation in the event of a breach. The Contractor should be self-insured to the extent necessary to handle any reasonably foreseeable breach, with another source of income, to fully cover the costs of breach response, including but not limited to victim remediation.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

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

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

(2) Records Creation, Ownership, and Disposition

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

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

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

D. Data Privacy and Oversight

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

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

(2) Requirements for Contractor IT Systems Hosting Government Data

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

(3) Requirement to Support Privacy Compliance

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

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

[1] “[T]he term ‘record’ means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” 5 U.S.C. § 552a(a)(4). “[T]he term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” 5 U.S.C. § 552a(a)(5).
[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), “’personally identifiable information’ means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” Regarding “sensitive PII,” “[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals’ names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information.” OMB Circular A-130, at App. II-2.
[3] The DOJ OPCL Resources page is available at https://www.justice.gov/opcl/resources.
[4] As stated in DOJ Instruction 0900, “Contractors must notify the Contracting Officer, the Contracting Officer’s Representative, and JSOC (or component-level SOC) within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines.”
[5] https://www.justice.gov/file/4336/download
[6] As stated in DOJ Instruction 0900, the description should include the type of information that constitutes PII; purpose for which PII is collected, maintained, and used; extent to which PII identifies a peculiarly vulnerable population; the determination of whether the information was properly encrypted or rendered partially or completely inaccessible by other means; format of PII (e.g., whether PII was structured or unstructured); length of time PII was exposed; any evidence confirming that PII is being misused or that it was never accessed.
[7] As stated in DOJ Instruction 0900, the report should include the nature of the cyber threat (*e.g.*, Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents.
[8] As stated in DOJ Instruction 0900, the report should include analysis on whether the data is accessible, usable, and intentionally targeted.
[9] As defined in 40 U.S.C. § 11101, the term “information technology” means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive

agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.
[10] In this instance, the term “project” is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL.

(End of Clause)

DOJ-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

This Section Is Intentionally Left Blank

Section 4 - Solicitation Provisions

52.212-1 (DEV) Instructions to Offerors-Commercial Products and Commercial Services (Sep 2023) (DEVIATION NOV 2025)

(a) *Submission of offers*. Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. As a minimum, offers shall include—

(1) The solicitation number;

(2) The name, address, telephone number of the Offeror;

(3) The Offeror's Unique Entity Identifier (UEI) and, if applicable, Electronic Funds Transfer (EFT) indicator;

(4) Information necessary to evaluate the factors contained in the provision at 52.212-2 or as described in the solicitation;

(5) Responses to provisions that require Offeror completion of information, representations, and certifications (other than those collected via the System for Award Management (SAM)); and

(6) A statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation and any solicitation amendments.

(b) *Period for acceptance of offers*. The Offeror agrees to hold the prices in its offer firm for 60 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

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

(1) Offerors are responsible for submitting offers and any modifications or revisions to the Government office designated in the solicitation by the time specified in the solicitation.

(2) Any offer, modification, or revision received after the time specified for receipt of offers is "late" and will not be considered unless it is received before award is made and the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition. However, a late modification of an otherwise successful offer that makes its terms more favorable to the Government will be considered at any time it is received and may be accepted.

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

(4) Offerors may withdraw their offers by written notice to the Government received at any time before award.

(d) *Contract award (not applicable to Invitation for Bids)*. The Government intends to evaluate offers and award a contract without discussions with Offerors. Therefore, the Offeror's initial offer should contain the Offeror's best terms. However, the Government reserves the right to conduct discussions, if necessary. The Government may reject any or all offers if such action is in the public interest, accept other than the lowest offer, and waive informalities and minor irregularities in offers received.

(e) *Debriefings*. If a postaward debriefing is given to requesting Offerors, the Government will disclose the following information, if applicable:

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

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

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

(4) A summary of the rationale for award.

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

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

(End of provision)

A.2 ADDENDUM TO FAR 52.212-1, Instructions to Offerors-Commercial Products and Commercial Services (Sep 2023) (DEVIATION NOV 2025)

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

Provisions By Full Text

52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements--Representation (Jan 2017)

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

"Internal confidentiality agreement or statement, subcontract, and *subcontractor*", are defined in the clause at 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements.

(b) 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), Government agencies are not permitted to use funds appropriated (or otherwise made available) for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(c) The prohibition in paragraph (b) of this provision 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.

(d) *Representation*. By submission of its offer, the Offeror represents that it will 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).

(End of provision)

52.204-7 (DEV) System for Award Management-Registration (Nov 2024) (DEVIATION NOV 2025)

The Offeror shall have an active Federal Government contracts registration in the System for Award Management (SAM) when submitting an offer or quotation in response to this solicitation and at the time of award. As part of the SAM registration process, the Government collects information, as described in paragraphs (b) through (d) of this provision, that is necessary to identify the Offeror and for the Offeror to be awarded Federal Government contracts. To register in SAM, go to https://www.sam.gov. Allow for processing time when registering in SAM. If the Offeror is not registered in SAM, it should register immediately after receiving this solicitation.

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

Commercial and Government Entity (CAGE) code has the meaning provided in the clause at the Federal Acquisition Regulation (FAR) 52.204-13, System for Award Management—Maintenance, of this solicitation.

Electronic Funds Transfer (EFT) indicator means a bank account identifier to establish additional System for Award Management records for identifying alternative EFT accounts (see part 32) for the same entity.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest-level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees. There may be more than one immediate owner (e.g., joint ventures).

Predecessor means an entity whose assets were acquired by the offeror or another entity (most often through merger or acquisition) and whose affairs are now carried out by the offeror or the other entity under a new name.

Taxpayer identification number means the number required by the Internal Revenue Service (IRS) to be used by the offeror to report income tax and other returns. It may be either a Social Security Number or an Employer Identification Number.

Unique entity identifier (UEI) has the meaning provided in the clause at FAR 52.204-13, System for Award Management—Maintenance, of this solicitation.

(b) *Identifiers*. The Offeror shall obtain and provide the following identifying information:

(1) *Unique entity identifier (UEI)*.

(i) The Offeror shall obtain a UEI to register in SAM. The Government will independently validate the existence and uniqueness of the Offeror before assigning a UEI to the Offeror. Go to https://www.sam.gov for instructions on obtaining a UEI.

(ii) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation “Unique Entity Identifier” followed by the UEI that identifies the Offeror's name and address exactly as stated in the offer. The Offeror shall also enter its EFT indicator, if applicable.

(iii) The Contracting Officer will use the UEI to verify that the Offeror has an active Federal Government contracts registration in SAM.

(2) *Taxpayer identification number (TIN)*.

(i) The Offeror shall provide its TIN or related information to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d); reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M; and implementing regulations issued by the IRS. The Offeror shall consent for TIN validation; and

(3) *Commercial and Government Entity (CAGE) code*.

(i) The Offeror shall provide a CAGE code and legal business name (Do not use a “doing business as” name) for—

(A) Itself;

(B) Its immediate owner(s), if any;

(C) Its highest-level owner, if any; and

(D) Any predecessor(s), or predecessor of an Offeror’s predecessor, that held a Federal contract or grant within the last three years.

(ii) If the Offeror is in the United States or its outlying areas and does not already have a CAGE code assigned, the DLA CAGE Branch will assign a CAGE code to the Offeror as a part of the SAM registration process. For information on obtaining a CAGE code go to https://cage.dla.mil/.

(iii) The Offeror shall get from any immediate and/or highest-level owner(s) their respective CAGE code(s) to provide the code(s) as part of the registration (FAR 52.204-7(b)(3)(i)).

(iv) If the Offeror is located outside of the United States or its outlying areas, and does not already have a CAGE code assigned, the Offeror may obtain a CAGE code as indicated in the following table.

If the Offeror is…	**Then…**
Located in a country that is a member of the North Atlantic Treaty Organization (NATO) or a sponsored nation	Contact the appropriate National Codification Bureau (https://www.nato.int/structur/ac/135/about/contacts)
Located in a country that is not a member of NATO or a sponsored nation	Contact the NATO Support and Procurement Agency (NSPA) (https://eportal.nspa.nato.int/AC135Public/scage/CageList.aspx)

(c) *Representations and certifications*.

(1) The following FAR solicitation provisions contain entity-level representations and certifications that the Offeror shall submit as part of their Federal Government contracts registration in SAM:

Provision	**Title**	**Date**
52.204-5	Women-Owned Business (Other Than Small Business)	Oct 2014
52.209-2	Prohibition on Contracting with Inverted Domestic Corporations—Representation	Nov 2015
52.209-5	Certification Regarding Responsibility Matters	Aug 2020
52.209-11	Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law	Feb 2016
52.219-1	Small Business Program Representations	Feb 2024
52.219-1 Alt I	Small Business Program Representations, with its Alternate I	Feb 2024
52.219-1 Alt II	Small Business Program Representations, with its Alternate II	Mar 2023
52.226-2	Historically Black College or University and Minority Institution Representation	Oct 2014

(2) By submitting its offer, the Offeror verifies that, as of the date of its offer, its representations and certifications posted electronically in SAM for the provisions listed in paragraph (c)(1) of this provision are current, accurate, and complete. The Offeror’s representations and certifications in SAM are hereby incorporated by reference into its offer.

(d) *Other information*. The Offeror shall provide more information on its business operations and type that is necessary to be considered for award of certain contracts and financial information necessary to receive payment under contracts.

(End of provision)

52.240-90 (DEV) Security Prohibitions and Exclusions Representations and Certifications (DEVIATION NOV 2025)

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

Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.

Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce

Marginalized populations of Sudan means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and

(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) *Procedures*.

(1) *Covered telecommunications and video surveillance*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.gov for entities excluded from receiving federal awards for "covered telecommunications equipment or services."

(2) *FASCSA Orders*.

(i) The Offeror shall search in SAM for the phrase "FASCSA order" for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.

(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).

(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.

(c) *Covered telecommunications equipment or services representations*. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror’s possession but does not need to include an internal or third-party audit)—

(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and

(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).

(d) *FASCSA Representation*. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror’s possession but does not need to include an internal or third-party audit.

(e) *Sudan certification*. By submission of its offer, the offeror certifies, after conducting a reasonable inquiry (that looks at any information in the offeror’s possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.

(f) *Iran Representation and Certifications*.

(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror’s possession but does not need to include an internal or third-party audit), by submission of its offer—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum

products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)

(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—

(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.

(iii) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(g) *Disclosure*.

(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:

(i) Contract number and order number, if applicable;

(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);

(vii) Whether alternative products or services are available that would be compliant with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions undertaken or recommended.

(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:

(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at https://dibnet.dod.mil.

(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.

(3) If the disclosure provided does not contain any of the information required by paragraph (1), and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.

(h) *Executive agency review of disclosures*. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.

(End of provision)

[END OF ADDENDUM TO FAR 52.212-1]

52.212-2 (DEV) Evaluation-Commercial Products and Commercial Services (Nov 2021) (DEVIATION NOV 2025)

Evaluation—Commercial Products and Commercial Services (Nov 2025)

(a) Evaluation factors. The Government will award a contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors will be used to evaluate offers:Price, Past Performance and Delivery time considered *[Insert evaluation factors in the relative order of importance. For requests for proposals, state: Evaluation factors other than price when combined are [significantly more important than price/approximately equal to price/significantly less important] than price. For invitations for bids, list only price and price-related factors.]*

(b) *Options (if applicable)*. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. The evaluation of options does not obligate the Government to exercise the option(s).

c) *Notice of award*. A written notice of award or acceptance of an offer furnished to the successful Offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)