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
	26

2. CONTRACT NUMBER	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			15M10226QA4700285	08/08/2026

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (*No collect calls*)	8. OFFER DUE DATE / LOCAL TIME
	Renee Leaman renee.leaman@usdoj.gov		08/13/2026 10:00 CT

9. ISSUED BY — CODE 15M102
U.S MARSHALS SERVICE
PROCUREMENT APC
Austin Processing Center
903 San Jacinto Blvd, Suite 1210
Austin, TX 78701

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): 811490
SIZE STANDARD: 9,000,000

11. DELIVERY FOR FREE ON BOARD (FOB) DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER THE DEFENSE PRIORITIES AND ALLOCATIONS SYSTEM - DPAS (15 CFR 700)	13b. RATING
[ ] SEE SCHEDULE		[ ]	14. METHOD OF SOLICITATION: [X] REQUEST FOR QUOTE (RFQ) [ ] INVITATION FOR BID (IFB) [ ] REQUEST FOR PROPOSAL (RFP)

15. DELIVER TO — CODE

16. ADMINISTERED BY — CODE 15M032
UNITED STATES MARSHAL-E/KY
EASTERN DISTRICT OF KENTUCKY
162 FEDERAL BUILDING
101 BARR STREET
LEXINGTON, KY 40507-1357
Melissa Smith
(O) 859-753-7202
Melissa.smith6@usdoj.gov

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

18a. PAYMENT WILL BE MADE BY — CODE 15M032
UNITED STATES MARSHAL-E/KY
EASTERN DISTRICT OF KENTUCKY
162 FEDERAL BUILDING
101 BARR STREET
LEXINGTON, KY 40507-1357
Melissa Smith
(O) 859-753-7202
Melissa.smith6@usdoj.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
	EO 14398 FY26-27 D32 Lex Remodel Phase II Install CONTRACT FILE: APC-FY26-000250 MISSION CRITICAL 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
		renee leaman	

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	Description	Page Number
	Solicitation/Contract Form	1
1	Commodity or Services Schedule	4
2	Contract Clauses	5
	52.203-17 Contractor Employee Whistleblower Rights (Nov 2023)	5
	52.212-4 Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2023)	5
	52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders-Commercial Products and Commercial Services (Mar 2026)	5
	52.213-2 Invoices (Apr 1984)	5
	52.217-8 Option to Extend Services (Nov 1999)	5
	52.217-9 Option to Extend the Term of the Contract (Mar 2000)	5
	52.222-3 Convict Labor (June 2003)	5
	52.222-21 Prohibition of Segregated Facilities (Apr 2015)	5
	52.222-26 Equal Opportunity (Sept 2016)	5
	52.222-36 Equal Opportunity for Workers with Disabilities (Jun 2020)	5
	52.222-40 Notification of Employee Rights Under the National Labor Relations Act (Dec 2010)	5
	52.222-50 Combating Trafficking in Persons (Oct 2025)	5
	52.223-18 [Reserved]	6
	52.225-1 Buy American-Supplies (Oct 2022)	6
	52.232-18 Availability of Funds (Apr 1984)	6
	52.232-25 Prompt Payment (Jan 2017)	6
	52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)	6
	52.233-1 Disputes (May 2014)	6
	52.243-1 Changes-Fixed-Price (Aug 1987)	6
	52.247-34 F.o.b. Destination (Nov 1991)	6
	52.249-2 Termination for Convenience of the Government (Fixed-Price) (Apr 2012)	6
	52.222-90 Addressing DEI Discrimination by Federal Contractors (APR 2026)	6
	DOJ-02 Contractor Privacy Requirements (JAN 2022)	7
	DOJ-05 Security of Department Information and Systems (APR 2026)	12
	USMS-0002 Release of Residual Funds (Greater Than $100)	19
	USMS-0003 Acceleration of Payments to Small Businesses	19
	USMS-0009 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT	19
	USMS-0010 CONTRACT/ORDER CLOSEOUT - FIXED-PRICE, TIME-AND-MATERIALS, OR LABOR HOURS	21
	USMS-0011 RELEASE OF CLAIMS	21
	USMS-0012 Contracting Officer's Representative (COR)	21
	USMS-0013 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2018)	22
3	List of Attachments	23
	USMS-0015 Item Specification, Statement of Work, Performance Work Statement of Statement of Objectives	23
4	Solicitation Provisions	25
	52.212-2 Evaluation-Commercial Products and Commercial Services (Nov 2021)	25

Section 1 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	FY26 D32 Lex Remodel Phase II Install See Statement of Work PSC: Z1AA **Line Period of Performance:** 08/21/2026 - 08/20/2027 Base Period	1	LT	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	FY27 D32 Lex Remodel Phase II Install DO NOT PRICE *Will be priced at the time of the bona-fide need. Must fall within the statement of work. PSC: Z1AA **Line Period of Performance:** 08/21/2027 - 08/20/2028 Unexercised Option	1	LT	$_____	$_____

EO 14398
FY26-27 D32 Lex Remodel Phase II Install
CONTRACT FILE: APC-FY26-000250
MISSION CRITICAL

Section 2 - Contract Clauses

A.1 ADDENDUM TO FAR 52.212-4, Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2023)

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)	
52.212-4	Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2023)	
52.212-5	Contract Terms and Conditions Required To Implement Statutes or Executive Orders-Commercial Products and Commercial Services (Mar 2026)	
52.213-2	Invoices (Apr 1984)	
52.217-8	Option to Extend Services (Nov 1999)	Period of Time: "5"
52.217-9	Option to Extend the Term of the Contract (Mar 2000)	(a) Period of Time: "5" (a) Days: "5" (c): "6 Months"
52.222-3	Convict Labor (June 2003)	
52.222-21	Prohibition of Segregated Facilities (Apr 2015)	
52.222-26	Equal Opportunity (Sept 2016)	
52.222-36	Equal Opportunity for Workers with Disabilities (Jun 2020)	
52.222-40	Notification of Employee Rights Under the National Labor Relations Act (Dec 2010)	

Clause	Title	Fill-ins (if applicable)
52.222-50	Combating Trafficking in Persons (Oct 2025)	
52.223-18	[Reserved]	
52.225-1	Buy American-Supplies (Oct 2022)	
52.232-18	Availability of Funds (Apr 1984)	
52.232-25	Prompt Payment (Jan 2017)	
52.232-33	Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)	
52.233-1	Disputes (May 2014)	
52.243-1	Changes-Fixed-Price (Aug 1987)	
52.247-34	F.o.b. Destination (Nov 1991)	
52.249-2	Termination for Convenience of the Government (Fixed-Price) (Apr 2012)	

Clauses By Full Text

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

(a) *Definitions*. As used in this clause—
Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.
Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.

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

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

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

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

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

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

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

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

(End of clause)

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)

USMS-0002 Release of Residual Funds (Greater Than $100)

If funds greater than $100 remain on this contract after the final invoice, the Government will issue a bilateral modification to authorize release of those funds. The contractor's signature on the modification will constitute understanding and agreement that all outstanding obligations incurred on this contract have been satisfied. The Government shall not be held liable for the payment of any further invoices submitted under this contract. The contractor will have up to 30 calendar days after issuance of the modification to sign and return it. Further, failure to sign and return the modification within the stated time period shall be considered acceptance of the government's intent to deobligate the residual funds; and releases the Government from any future liability stemming from or related to this contract. (Applies to all contracts.) (End of Clause)

USMS-0003 Acceleration of Payments to Small Businesses

In order for the United States Marshals Service Payment Office to comply with OMB Memorandum M-11-32, all invoices from any small business must include the following statement of self-certification of its small business status:
"I hereby certify that _____ is a small business concern as defined in Federal Acquisition Regulation (FAR) subpart 2.101."
This requirement for certification is in addition to any other invoicing instructions for this contract. Failure to include this certification on invoices may result in delayed payment.

USMS-0009 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

Non-Disclosure and Confidentiality Agreement

This Non-Disclosure/Confidentiality Agreement is a standard agreement designed for use by____and its employees and subcontractors assigned to work as a/an_____ for the Department of Justice, United States Marshals Service (USMS), under _____

The use of this agreement is designed to protect non-public information from disclosure and to prevent violations of federal statutes and regulations.

The contract and the employees working on the contract will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4705, 41 U.S.C. 4712, and FAR 3.908.

During your assignment, you agree to:

1. Use only for Government purposes any and all confidential business, procurement, and/or other sensitive information to which you are given direct or indirect access.
2. Not to disclose non-public information by any means (in whole or in part, alone or in combination with other information, directly or indirectly or derivatively) to any person except to a Contracting Officer's Representative (COR), Contracting Officer (CO), or other U.S. Government official with a need to know. All distribution of information will be controlled by the CO.
3. Not to use no-public information for any non-governmental purpose including but not limited to: the preparation of bids and proposals, or the development or execution of other business or commercial venture.

The signatory will not disclose any classified information received in the course of such intelligence or intelligence-related activity unless specifically authorized to do so by the United States Government;

and this NDA does not bar disclosures to Congress. Or to an authorized office of an executive agency or the Department of Justice, which are essential to report a substantial violation of law.

Except as necessary in the performance of your work assignment, you will not, without the written approval of the COR, CO or USMS Manager:

a. Disseminate any oral, written or electronic information which constitutes non-public information co vered under this Agreement, and that is obtained as a result of the accomplishment of work perf ormed under the aforementioned contract/task order; or,

b. Remove any documents or electronic media containing non-public information under this Agreement from the place of your work assignment.

c. Non-public information, as used herein, includes trade secrets, confidential or proprietary business information as defined under the Freedom of Information Act, 5 U.S.C. 552, procureme nt and any other proprietary information in any form, whether drawings, designs, schedules, plans, s tudies, software, prototypes, samples, or formulas, whether by verbal, electronic or written commun ication.

These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights or liabilities created by existing statues 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 controlling Executive orders and statutory provisions are incorporated into the agreement and are controlling.

By signing this agreement, you agree that:

1. You have been advised that all data covered by this Agreement that is furnished by the Government, including any copies, notes or working papers derived or produced therefrom, are the property of the Government.
2. You understand that any unexcused failure to surrender such materials promptly, or improper conversion of such materials for use not called for by your work assignment (e.g., delivery of a document, or a copy thereof, or notes containing information taken from the document, to someone not authorized by the Government to receive such information), may be in violation of18 U.S.C. 461(theft of Government property).
3. In accordance with the aforementioned contract/task order provisions, this Agreement may be formally modified or changed by the Government in those instances in which the courts (e.g., civil investigative demands), or specific circumstances dictate such a modification or change. You will be afforded an opportunity to review and concur with such changes.
4. You further acknowledge that you understand the provisions of the sections above and will continue to comply with the provisions herein even after your work assignment is completed. Additionally, you understand that you may be required to disclose the information subject to this agreement pursuant to the provisions of a valid court order.

It is understood that this Non-Disclosure/ Confidentiality Agreement is used to ensure that Contractors and con tractor’s employees are aware of and commit to comply with the confidentiality requirements described above.

AGREED:

Name (Print)

Name (Signature) Date

Title

Company

USMS-0010 CONTRACT/ORDER CLOSEOUT - FIXED-PRICE, TIME-AND-MATERIALS, OR LABOR HOURS

Timely contract closeout is a priority under this contract/order. The Contractor shall submit a final invoice within thirty (30) calendar days after the expiration of this contract/order, unless the Contractor requests and is granted an extension by the Contracting Officer, in writing. In addition, and concurrent with the submission of the final invoice, the Contractor shall notify the Contracting Officer of the amount of any excess funds that can be de-obligated from this contract/order so the closeout process can begin as soon as possible upon expiration of this contract/order.
A unilateral contract/order closeout modification will be issued for firm-fixed price actions under the Simplified Acquisition Threshold (SAT) where the Government has evidence that the supplies or services have been received or completed, the final invoice has been both submitted and paid, there are no funds remaining on the contract to be disbursed, and a release of claims has been obtained.
For all other acquisitions, a bilateral contract/order closeout modification will be forwarded to the Contractor by the Contracting Officer and must be signed by the Contractor and returned to the Contracting Officer within thirty (30) calendar days of issuance of the modification. A Contractor's failure to respond and/or sign the bilateral closeout modification within thirty (30) calendar days of receipt will constitute approval of the terms of the modification and the modification will subsequently be processed unilaterally by the Contracting Officer to de-obligate excess funds and close this contract/order.
If this contract/order contains option periods, the Contractor is required to submit an invoice within sixty (60) calendar days after expiration of the base period of performance and the expiration of each exercised option period of performance to allow for de-obligation of any excess funds that were obligated in those respective periods of performance.
(End of Clause)

USMS-0011 RELEASE OF CLAIMS

At the conclusion of the contract (or task order), the Contractor shall submit with the Final Invoice a release of claims against the United States arising out of the contract (or task order), other than claims specifically excepted from the operation of the release. Copies of the required form may be obtained from the Contracting Officer.

USMS-0012 Contracting Officer's Representative (COR)

CONTRACTING OFFICER'S REPRESENTATIVE (COR) (AUG 2017)
Rodney Baugh is hereby designated as the Contracting Officer's Representative (COR). The COR may be changed at any time by the Government without prior notice to the contractor by a unilateral modification to the contract. The COR is located at:
Phone Number:606-864-6993
E-mail: Rodney.Baugh3@usdoj.gov
(b) The responsibilities and limitations of the COR are as follows:
(1) The COR is responsible for the technical aspects of the contract and serves as technical liaison with the contractor. The COR is also responsible for the final inspection and acceptance of all deliverables and such other responsibilities as may be specified in the contract.
(2) The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract price, terms or conditions. Any contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the express written prior authorization of the Contracting Officer. The Contracting Officer may designate assistant or alternate COR(s) to act for the COR by naming such assistant/alternate(s) in writing and transmitting a copy of such designation to the contractor.

(End of clause)

USMS-0013 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2018)

Payment requests must be submitted electronically through the U.S. Department of the Treasury's Invoice Processing Platform System (IPP).

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions - Commercial Items included in commercial item contracts. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice .

The Contractor must use the IPP website to register access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from IPP Customer Support within 3 - 5 business days of the contract award date. The IPP website will enforce a Multifactor Authentication (MFA) login beginning on August 28, 2023 to strengthen account security. The Contractor must use the IPP website to register access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from IPP Customer Support within 3 - 5 business days of the contract award date. The IPP website will enforce a Multifactor Authentication (MFA) login beginning on August 28, 2023 to strengthen account security. The MFA login will require the use of ID.me or Login.gov for the multifactor authentication. Contractor assistance with enrollment and login can be obtained by contacting the ID.me Help Center at https://help.id.me/hc/en-us or the Login.gov Help Center at https://login.gov/help/.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the Contracting Officer with its proposal or quotation.

(End of Local Clause)
[END OF ADDENDUM TO FAR 52.212-4]

Section 3 - List of Attachments

USMS-0015 Item Specification, Statement of Work, Performance Work Statement of Statement of Objectives (DEVIATION)

U.S. Department of Justice

U.S. Marshals Service, Eastern District of Kentucky

STATEMENT OF WORK (SOW)

FY26 D32 Lex Remodel Phase II Install

Statement of Work

Introduction

Eastern District of Kentucky Lexington office has a requirement for the final installation of various items such as tv's, dry erase marker boards, and changing cell locks to complete the recent remodel at that location.

Delivery Date:

Work is to be completed within 90 days of the notice of award.

1. Place of Performance

2. Background/Current Environment

The Eastern District of Kentucky Lexington office has recently undergone a remodel and needs to have various items installed to complete the remodel for use.

3. Objectives and Tasks

Vendor will install the following items:	

MOUNT 4 TVs IN VARIOUS OFFICE LOACTIONS (LABOR)	EA	4
HANG 20 POSTER FRAMES IN VARIOUS LOACTIONS	EA	1
CHANGE OLD CELL LOCKS IN PRISONER CELLS WITH NEW LOCKS	EA	3
MATERIALS SUCH AS TV MOUNTS AND SUPPLIES HARDWARE	EA	1
HANGING THREE DRY ERASE BOARDS IN VARIOUS SPACES	EA	3

4. Key Deliverables

CONTRACTOR GUARANTEES THEIR WORK AND WILL REPAIR OR RESOLVE ANY ISSUES AS A RESULT OF POOR WORKMANSHIP

5. Government Furnished Equipment/Information (GFE/GFI)

E/KY LEXINGTON OFFICE IS PROVIDING TVs, POSTER FRAMES, DRY ERASE BOARDS TO BE MOUNTED AND CELL LOCKS

6. Constraints

NOTE: Compact Parking Area

NOTE: Work Must be completed between 8:30AM - 5:00PM EST Monday - Friday

7. Security

WORKS WILL BE ESCORTED BY USMS STAFF WHILE IN SECURE AREAS ON PREMISES

Section 4 - Solicitation Provisions

Provisions By Full Text

52.212-2 Evaluation-Commercial Products and Commercial Services (Nov 2021)

(a) 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 shall be used to evaluate offers:

Lowest Price Technically Acceptable

[*Contracting Officer shall insert the significant evaluation factors, such as (i) technical capability of the item offered to meet the Government requirement; (ii) price; (iii) past performance (see FAR 15.304); and include them in the relative order of importance of the evaluation factors, such as in descending order of importance.*]

Technical and past performance, when combined, are n/a [*Contracting Officer state, in accordance with FAR 15.304, the relative importance of all other evaluation factors, when combined, when compared to price.*]

(b) *Options*. 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. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise 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)

No substitutions allowed.
Evaluation Criteria:

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 shall be used to evaluate offers:

1. Technical Acceptability 2. Price The lowest priced offer will be evaluated for technical acceptability.

Therefore, each proposal will be evaluated first for lowest price/technical acceptable.

If found technically acceptable award will be made without further consideration. If found technically unacceptable the government will evaluate the next lowest offer for technical acceptability until award can be made to the lowest priced technically acceptable offeror.

This will be a lowest price technically acceptable purchase. Technical acceptability - at a minimum - will consist of meeting all characteristics, including those in the Technical Specifications Document and following the solicitation instructions.

INSTRUCTIONS TO OFFERORS

Volume 1: Quote

Quotes shall be provided on company letterhead, single page with company name, logo, address, Point of Contact, contact info, etc…. Cage Code, Tax ID number and **GSA Schedule Contract Number** must be included, if applicable. **The Government seeks additional discounts**. All prospective offerors must be a Commercial and Government Entity (CAGE) code and be registered with the System for Award Management at https://www.sam.gov /porta 1/public/SAM.

Volume 2: SF-1449

The SF-1449 shall be returned signed and with pricing. Fill in required Clauses.

Vendor shall enroll in IPP See Terms and Conditions USMS 0013, ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2018)

NOTES TO VENDOR:

1. Sign Page 1
2. Fill Section 1 - Schedule of Supplies/Services

3. Fill in required CLAUSES

SUBMIT ONE PDF ONLY. FRONT PAGE IS THIS SF1449 COMPLETED AND SIGNED. THEN ALL SUPORTING DOCUMENTS YOU REQUIRE TO PRESENT YOUR COMPANY.

ONE PDF FILE, COMBINED ALL DOCUMENTS TO ONE PDF FILE. And use the correct format in the SUBJECT when emailing your quote.

FAILURE TO COMPLY WILL SHOW AS UNRESPONSIVE and your quote will not be considered.