

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

32a. QUANTITY IN COLUMN 21 HAS BEEN

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

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

34. VOUCHER NUMBER

35. AMOUNT VERIFIED
CORRECT FOR

36. PAYMENT

☐ 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

<u>Section</u>	<u>Description</u>	<u>Page Number</u>
	Solicitation/Contract Form.....	1
1	Commodity or Services Schedule.....	4
2	Contract Clauses.....	6
	52.212-4 Contract Terms and Conditions-Commercial Products and Commercial Services (Nov 2023).....	6
	52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders-Commercial Products and Commercial Services (Jan 2025).....	6
	52.213-2 Invoices (Apr 1984).....	6
	52.217-8 Option to Extend Services (Nov 1999).....	6
	52.217-9 Option to Extend the Term of the Contract (Mar 2000).....	6
	52.222-3 Convict Labor (June 2003).....	6
	52.222-21 Prohibition of Segregated Facilities (Apr 2015).....	6
	52.222-26 Equal Opportunity (Sept 2016).....	6
	52.222-36 Equal Opportunity for Workers with Disabilities (Jun 2020).....	6
	52.222-40 Notification of Employee Rights Under the National Labor Relations Act (Dec 2010).....	6
	52.222-50 Combating Trafficking in Persons (Nov 2021).....	6
	52.223-18 [Reserved].....	6
	52.225-1 Buy American-Supplies (Oct 2022).....	7
	52.232-18 Availability of Funds (Apr 1984).....	7
	52.232-25 Prompt Payment (Jan 2017).....	7
	52.232-33 Payment by Electronic Funds Transfer-System for Award Management (Oct 2018).....	7
	52.233-1 Disputes (May 2014).....	7
	52.243-1 Changes-Fixed-Price (Aug 1987).....	7
	52.247-34 F.o.b. Destination (Nov 1991).....	7
	52.249-2 Termination for Convenience of the Government (Fixed-Price) (Apr 2012).....	7
	DOJ-05 Security of Department Information and Systems DOJ-05 (OCT 2023).....	7
	DOJ-02 Contractor Privacy Requirements (JAN 2022).....	7
	USMS-0002 Release of Residual Funds (Greater Than \$100).....	12
	USMS-0003 Acceleration of Payments to Small Businesses.....	12
	USMS-0009 NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT.....	12
	USMS-0010 CONTRACT/ORDER CLOSEOUT - FIXED-PRICE, TIME-AND-MATERIALS, OR LABOR HOURS.....	14
	USMS-0011 RELEASE OF CLAIMS.....	15
	USMS-0012 Contracting Officer's Representative (COR).....	15
	USMS-0013 ELECTRONIC INVOICING AND PAYMENT REQUIREMENTS - INVOICE PROCESSING PLATFORM (IPP) (JAN 2018).....	15
3	List of Attachments.....	17
	USMS-0015 Item Specification, Statement of Work, Performance Work Statement of Statement of Objectives.....	17
4	Solicitation Provisions.....	26
	52.212-2 Evaluation-Commercial Products and Commercial Services (Nov 2021).....	26

Section 1 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	10-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2025 - 12/21/2026 Base Period	2,000	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	3-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2025 - 12/21/2026 Base Period	500	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	10-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2026 - 12/21/2027 Unexercised Option	2,000	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002	3-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2026 - 12/21/2027 Unexercised Option	500	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001	10-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2027 - 12/21/2028 Unexercised Option	2,000	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002	3-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2027 - 12/21/2028 Unexercised Option	500	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001	10-Day Delivery Verbatim Transcription	2,000	EA	\$_____	\$_____

	SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2028 - 12/21/2029 Unexercised Option				
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002	3-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2028 - 12/21/2029 Unexercised Option	500	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001	10-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2029 - 12/21/2030 Unexercised Option	2,000	EA	\$_____	\$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002	3-Day Delivery Verbatim Transcription SEE STATEMENT OF WORK FOR DETAILS PSC: 7B22 Line Period of Performance: 12/22/2029 - 12/21/2030 Unexercised Option	500	EA	\$_____	\$_____

FY26-30 A45 Transcription Services
Contract File Folder: APC-FY26-000013
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)
52.212-4	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 (Jan 2025)	
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)	
52.222-50	Combating Trafficking in Persons (Nov 2021)	

Clause	Title	Fill-ins (if applicable)
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)	
DOJ-05	Security of Department Information and Systems DOJ-05 (OCT 2023)	

Clauses By Full Text

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)

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 non-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 covered under this Agreement, and that is obtained as a result of the accomplishment of work performed 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, procurement and any other proprietary information in any form, whether drawings, designs, schedules, plans, studies, software, prototypes, samples, or formulas, whether by verbal, electronic or written communication.

These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights or liabilities created by existing statutes 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 of 18 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 contractor'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)

(a) Demetria Leslie 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: 703-740-4209

E-mail: Demetria.Leslie@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)

The SCHEDULE OF SUPPLIES/SERVICES is hereby incorporated into the contract instrument.

See SCHEDULE OF SUPPLIES/SERVICES for Technical Specifications and to insert pricing

DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

UNITED MARSHAL SERVICE

U.S. Marshals Service Office of Employee and Labor Relations For Transcription Service for recorded Interviews

The contractor will provide completed transcripts of the United States Marshals Service (USMS), Office of Employee and Labor Relations (OELR), interviews and evidence. The contractor will transcribe digital audio, audio cassette tapes, digital video files, VHS tapes, and include translation services from Spanish to English. The contractor will provide USMS with the software application needed to access the contractor established file transfer protocol (FTP) website. FTP website should contain an application area for USMS to upload digital recordings (audio/visual). Transcripts are to be sent via e-mail to the submitting USMS employee's Department of Justice email account. The USMS may also send the contractor standard or micro- cassette, compact disk, and/or VHS recorded interviews via secure mail or Federal Express. All electronic media will be encrypted, and password protected prior to providing it to the contractor.

To ensure Offerors have the capacity to handle this requirement, OELR estimates it will submit approximately 10 transcripts per month totaling approximately 10 hours of recorded interviews per month to the contractor. The contractor will proofread and correct transcripts prior to submission to OELR. Typed transcripts will be in an editable Microsoft Word document, on pleading paper lined and numbered format. All return documents from the contractor must be encrypted and password protected.

The contractor is prohibited from disseminating or making duplicates of magnetic or digital media, or any documents for which transcription is requested by OELR. The contractor will maintain a secure electronic archive of transcripts for a period of six months and then purge the files.

Written notification of any archive file deletion (purge) must be provided to the Contracting Officer's Representative (COR) 30 days prior to the date the file is to be deleted.

In the event USMS mails a physical copy of an audio/video file, the vendor will return such file to USMS via US Mail at the completion of the transcription. The contractor will delete all electronic file copies of that physically mailed audio/video file in accordance to the previous paragraph and notify the COR 30 days prior to the date the file is to be deleted.

The contractor is required to provide completed transcripts within ten business days after receipt of recorded interviews. The contract rate will be reduced by 10% for each day after the tenth day, down to a minimum of 10% of the contract price. An extension to the "10-day period" can be granted by the COR if the contractor makes a request in writing and provides evidence the delay is caused by excessive OELR volume prior to the expiration of the ten days. The same 10% reduction applies to "3 day" period request delays.

PERSONNEL SECURITY REQUIREMENTS. The Government anticipates the work to be performed under this

contract will involve access to sensitive but unclassified information. The selected vendor must undergo a minimum HACL or other background investigation as determined by the USMS Security Programs Manager (SPM), or designee. The selected vendor will be required to submit information to the USMS Office of Security Programs (OSP) electronically to schedule his background investigation. The selected vendor must have access to the internet to submit this information online.

CONTRACTOR RESPONSIBILITIES. The contractor is responsible for pre-screening all prospective employees for suitability of work on any resulting contract and for assuring that all such persons have a Government-performed background investigation completed prior to assignment to the contract.

As part of this screening procedure, the contractor shall also perform a credit check for each employee to ascertain whether the employee has significant recent debt problems prior to submitting the employee's name to the COR.

The contractor is responsible for providing the COR the full name, Social Security Number, Date of Birth, Place of Birth, and e-mail address of the company's primary Point of Contact (POC). The COR will submit the information to OSP. Upon receipt, OSP will create an on-line account for the prospective contract employee and transmit instructions via e-mail regarding the on-line completion of any required security forms. The contractor shall assure the primary POC furnishes all required

data in the form and format determined by the SPM or his duly authorized representative.

All security forms shall be submitted a minimum of sixty (60) days before the contractor plans to assign an employee to work under this contract. The contractor shall have their assigned personnel working on the contract to have passed the appropriate background investigation and to not disclose the information contained in the audio/video files to anyone. OSP will notify the COR of the results of the background investigations and authorize the use of the contractor employee.

During the life of the contract, the contractor shall report any significant incidents involving employees previously cleared and assigned to this contract to the COR. Significant incidents includes, but are not limited to, arrests, convictions, adverse civil judgments, personal bankruptcy, and administrative disciplinary actions. Based on the information provided, OSP will decide whether an employee may continue to work on the contract.

The contractor has an affirmative obligation to report negative employee background findings to the USMS. If the contractor fails to report past findings or current significant incidents, and the USMS subsequently uncovers such information, the contractor may be terminated for default.

The contractor will submit their invoice for transcription/translation services on a monthly basis.

The invoice package will be sent electronically to the COR by the tenth day of the following month, e.g., January's invoice package is due no later than February 10. The invoice package

will consist of three parts, listed on separate pages and must be provided in one completed PDF document:

1. Formal invoice indicating the total number of pages per rate;
2. Activity report listing each requested transcript by name and the total pages/rate; and
3. Detail reconciliation report listing each transcription requested, the OELR employee who made the request, the case number, the name of the person interviewed, and the pages/rate.

DATA SECURITY

A. Security of Systems and Data, Including Personally Identifiable Information (PII).

The following must be used in any contract where the contractor handles data that originated within the Department of Justice, the Department data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel. Additional guidance is provided in Appendix A of this SOW.

Security of Systems and Data, Including Personally Identifiable Data.

a. Systems Security:

The work to be performed under this contract requires the handling of data that originated within the Department, data that the contractor manages or acquires for the Department, and/or data that is acquired in order to perform the contract and concerns Department programs or personnel.

For any system handling such data, the contractor shall comply with all security requirements applicable to Department of Justice systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by OMB and NIST), DOJ IT Security Standards, and DOJ Order 0904. The contractor shall provide DOJ access to and information regarding

the contractor's systems when requested by the Department in connection with its efforts to ensure compliance with all such security requirements and shall otherwise cooperate with the Department in such efforts. DOJ access shall include independent validation testing of controls, system penetration testing by DOJ, FISMA data reviews, and access by the DOJ Office of the Inspector General for its reviews.

The use of contractor-owned laptops or other media storage devices to process or store data covered by this clause is prohibited until the contractor provides a letter to the contracting officer (CO) certifying the following requirements:

1. Laptops must employ encryption using a NIST Federal Information Processing Standard (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. Mobile computing devices will utilize anti-viral software and a host-based firewall mechanism;

4. The contractor shall log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is sensitive information unless designated as non-sensitive by the Department;

5. Contractor owned removable media, such as removable hard drives, flash drives, CDs, and floppy disks, containing DOJ data, shall not be removed from DOJ facilities unless encrypted using a NIST FIPS 140-2 approved product;

6. When no longer needed, all removable media and laptop hard drives shall be processed (sanitized, degaussed, or destroyed) in accordance with security requirements applicable to DOJ;
7. Contracting firms shall keep an accurate inventory of devices used on DOJ contracts;
8. Rules of Behavior must be signed by users. These rules shall address at a minimum: authorized and official use; prohibition against unauthorized users; and protection of sensitive data and personally identifiable information'; and
9. All DOJ data will be removed from contractor-owned laptops upon termination of contractor work. This removal must be accomplished in accordance with DOJ IT Security Standard requirements. Certification of data removal will be performed by the contractors' project manager and a letter confirming certification will be delivered to the CO within 15 days of termination of contractor work.

b. Data Security:

By acceptance of, or performance on, this contract, the contractor agrees that with respect to the data identified in paragraph a, in the event of any actual or suspected breach of such data (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the contractor will immediately, (and in no event later than within one hour of discovery) report the breach to the DOJ CO and the Contracting Officer's Representative (COR).

If the data breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, the contractor shall call the DOJ Computer Emergency Readiness Team (DOJCERT) at 1-866-US4-CERT (1-866-874-2378) within one hour of discovery of the breach. The contractor shall also notify the CO as soon as possible during regular business hours.

c. PII Notification Requirement:

The contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose PII (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with the Department and shall not

proceed until the Department has decided that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor shall be coordinated with, and be subject to the approval of, the Department. The contractor assumes full responsibility for taking corrective action consistent with the

Department's Data Breach Notification Procedures, which may include offering credit monitoring when

appropriate.

d. Pass-through of Security Requirements to Subcontractors:

The requirements set forth in Paragraphs a through c, above, apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the contractor.

B. Information Resellers or Data Brokers.

For contracts where the Department obtains PII from a contractor (such as an information reseller or data broker), but the contractor does not handle the data described in Section A of this guidance document, the following clause must be used:

Information Resellers or Data Brokers:

Under this contract, the Department obtains personally identifiable information about individuals from the contractor. The contractor hereby certifies that it has a security policy in place which contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, lost or acquired by an unauthorized person while the data is under control of the contractor. In any case in which the data that was lost or improperly acquired reflect or consists of data that originated with the Department or reflects sensitive law enforcement or national security interest in the data, the contractor shall notify the Department contracting officer so that the Department may determine whether notification would impede a law enforcement investigation or jeopardize national security. In such cases, the contractor shall not notify the individuals until it receives further instruction from the Department.

Prepared by: Signature : Date: Appendix A – Security Standards Guide

Federal Information Technology Standards Guide

Background:

The United States Marshals Service, Information Technology Division, Security Branch provides this synopsis of federal compliance requirements pertaining to the processing, storage, transmission,

and protection of government information when non-government organizations are involved. This document is not intended to be all encompassing; rather a reference to provide an overview of the key concepts and direction on where more detailed information is to be gained. It is recommended that program managers, project leads, and contract personnel familiarize themselves with the information provided within this document to assist in the protection of agency information from unauthorized disclosure, facilitate construction of a realistic timeline, and assist in establishing contractual requirements for Information Technology (IT) projects involving our contracting partners and vendors.

Federal IT Systems Regulations & Policies

Federal Information Security Management Act (FISMA) , 44 U.S.C. 3541:

The United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The purpose of this act is to provide a comprehensive framework of information security controls, provide management and oversight, development, and maintenance of minimum required controls, acknowledge commercial industry expertise, and recognize individual agency discretion of security product procurement.

FISMA has brought attention within the federal government to cyber security and explicitly emphasized a risk-based policy for cost-effective security. FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act.

Federal Acquisition Regulation (FAR) Clause 39.101(c):

The FAR System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. This clause provides some contractually binding language.

"In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's Web site at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

Note: This provision to the FAR was included as directed from the OMB Memo M-08-22 of August 11, 2008 and last updated on May 26, 2022.

Department of Justice (DOJ) Order 0904:

Within USMS we reference the DOJ Order 0904, to define the specifics of compliance with Federal and

DOJ information technology security policies and requirements. Specifically, to the protection of USMS data within a contracted IT system, DOJ 0904 pages 26 and 27 provides:

“Contractors may process DOJ information on contractor-owned equipment, either within or outside DOJ space. In all of these situations, the contractors and their sub-contractors, including all personnel, information systems, and devices, are required to comply with this Order, and the contract must include the language required by PGD 15-03 (or its latest iteration), unless waived, in whole or in part, by the DOJ SPE or any other terms and conditions as deemed necessary by the CPCLO and/or DOJ's SPE.

When the contract requires or allows contractor information systems to be used (whether to access DOJ information systems and information or to process or store DOJ information), the contract must require that the information systems be assessed, authorized, and operated pursuant to a valid Authority to Operate (ATO). The ATO must be issued in accordance with the ATO requirements in this

document and in the Security Assessment & Authorization Handbook for unclassified and national security systems. Contractors who use individual devices under the contract must provide an inventory of such devices to the Contracting Officer's Representative (COR) and operate such devices pursuant to the requirements explicated in this Order, including all incident response requirements. Contractor systems used in this manner are subject to the same data calls as other DOJ systems.

Upon termination of contract work, all DOJ data must be removed from contractor-owned IT equipment.

Certification of data removal must be performed by the contract's project manager and a letter confirming certification must be delivered to the contracting officer within 15 business days of the termination of the contract, unless otherwise extended by the Contracting Officer or COR.”

Key Concepts Security Controls

Federal information systems must meet the minimum security requirements. These requirements are defined in Federal Information Processing Standards Publication (FIPS) 200. Organizations must meet

the minimum security requirements by selecting the appropriate security controls and assurance requirements as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve adequate security is a multifaceted, risk-based activity involving management and operational personnel within the organization. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in SP 800-53. This allows agencies to adjust the security controls to fit their mission requirements and operational environments more closely. The

controls selected or planned must be documented in the System Security Plan (SSP), further explained below.

Risk Assessment

The combination of FIPS 200 and NIST SP 800-53 requires a foundational level of security for all federal information and information systems. The agency's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations, assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a baseline for the federal agency and its contractors. A risk assessment essentially identifies potential threats and vulnerabilities and calculates the likelihood and impact to determine the overall risk to the agency. A determination is then made to either accept the given risk or mitigate the possibility of exploitation.

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 LPTA

[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/porta1/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