REQUEST FOR QUOTATION
(THIS IS NOT AN ORDER)

THIS RFQ [ ] IS [X] IS NOT A SMALL BUSINESS SET-ASIDE

PAGE OF PAGES: 1 | 34

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/ OR DMS REG. 1	RATING
15M10225QA4700302	08/01/2025			

5a. ISSUED BY

U.S MARSHALS SERVICE
PROCUREMENT APC
Austin Processing Center
903 San Jacinto Blvd, Suite 1210
Austin, TX 78701

6. DELIVER BY (Date)

7. DELIVERY
[ ] FOB DESTINATION [X] OTHER *(See Schedule)*

5b. FOR INFORMATION CALL (NO COLLECT CALLS)

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
Kate Oravitz Weeks kathryn.oravitz-weeks@usdoj.gov		Ext.:

8. TO:

a. NAME	b. COMPANY

c. STREET ADDRESS

9. DESTINATION

a. NAME OF CONSIGNEE

b. STREET ADDRESS

c. CITY

d. CITY	e. STATE	f. ZIP CODE	d. STATE	e. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS (Date)

07/01/2030 10:00 ET

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or service. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotation must be completed by the quoter.

11. SCHEDULE (Include applicable Federal, State and local taxes)

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	Aviation Security Office fill in block 13 a-f. Return within three (3) days to USMS at (e-mail): _____ ASO E-MAIL:_____ ASO USMS Vendor Code:_____ MISSION CRITICAL: Transporting and producing prisoners for court proceedings Labor Hours See Continuation Sheet(s)				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE
	0.00 %	0.00 %	0.00 %	0	0.00

NOTE: Additional provisions and representations [X] are [ ] are not attached.

13. NAME AND ADDRESS OF QUOTER			14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION	15. DATE OF QUOTATION
a. NAME OF QUOTER				
b. STREET ADDRESS			16. SIGNER	
			a. NAME (Type or print)	b. TELEPHONE AREA CODE
c. COUNTY				
d. CITY	e. STATE	f. ZIP CODE	c. TITLE (Type or print)	NUMBER

Section 1 - Commodity or Services Schedule

SCHEDULE OF SUPPLIES/SERVICES

CONTINUATION SHEET

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	40-hour work week Not to exceed 2,080 hours per year PSC: S206 **Line Period of Performance:** 10/01/2025 - 09/30/2026 Base Period	2,080	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	Above 40-hour work week Not to exceed 500 hours on a yearly basis PSC: S206 **Line Period of Performance:** 10/01/2025 - 09/30/2026 Base Period	500	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	40-hour work week Not to exceed 2,080 hours per year Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2026 - 09/30/2027 Unexercised Option	2,080	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002	Above 40-hour work week Not to exceed 500 hours on a yearly basis Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2026 - 09/30/2027 Unexercised Option	500	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001	40-hour work week Not to exceed 2,080 hours per year Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year PSC: S206 **Line Period of Performance:** 10/01/2027 - 09/30/2028 Unexercised Option	2,080	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002	Above 40-hour work week Not to exceed 500 hours on a yearly basis Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2027 - 09/30/2028	500	HR	$_____	$_____

	Unexercised Option				
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001	40-hour work week Not to exceed 2,080 hours per year Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2028 - 09/30/2029 Unexercised Option	2,080	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002	Above 40-hour work week Not to exceed 500 hours on a yearly basis Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2028 - 09/30/2029 Unexercised Option	500	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001	40-hour work week Not to exceed 2,080 hours per year Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2029 - 09/30/2030 Unexercised Option	2,080	HR	$_____	$_____
ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002	Above 40-hour work week Not to exceed 500 hours on a yearly basis Cost of living adjustment is at the discretion of the USMS and will be negotiated at time of Option Year. PSC: S206 **Line Period of Performance:** 10/01/2029 - 09/30/2030 Unexercised Option	500	HR	$_____	$_____

CCFM: ASO-FY25-000002 FY26-30 Aviation Security Officer

Statement of Work District Security Officer (DSO)

United States Marshals Service

STATEMENT OF WORK (SOW)

Aviation Security Officers (ASO)

1. Introduction

This Statement of Work (SOW) sets forth the Aviation Security Officers (ASO) requirements to provide detention service in various contexts in support of the United States Marshals Service (USMS) districts and Justice Prisoner Air Transportation System (JPATS).

JPATS mission is to coordinate and transport prisoners and detainees safely, securely, and humanely in a timely and economical manner. All ASO's will serve at the discretion of the Assistant Director (AD), JPATS or his/her designee. This is a personal services contract where the Government will exercise supervision over the ASOs performing the services herein.

2. Period of Performance

Option Year	Start Date	End Date
Base Year	1 OCTOBER 2025	30 SEPTEMBER 2026
Option Year 1	1 OCTOBER 2026	30 SEPTEMBER 2027
Option Year 2	1 OCTOBER 2027	30 SEPTEMBER 2028
Option Year 3	1 OCTOBER 2028	30 SEPTEMBER 2029
Option Year 4	1 OCTOBER 2029	30 SEPTEMBER 2030

3. Place of Performance

The Place of Performance supports the JPATS mission located throughout the 94 USMS Districts or other locations at the discretion of the Assistant Director (AD), JPATS or his/her designee.

4. Background/Current Environment

ASOs engaged under personal services contracts are not employees of the United States Government, the Department of Justice (DOJ), or the USMS. The authority and jurisdiction extended to, or provided by, the personal services contract is strictly limited to the period-of-time the services are directly provided by the ASO to the USMS.

Services performed pursuant to this contract do not entitle the ASO to pensions, health benefits, injury compensation, or other related federal employee benefits and services.

ASOs engaged under personal service contracts are considered employees for the purposes of the Federal Tort Claims Act and personal liability suits, and for the purposes of workers' compensation under the Federal Employees Compensation Act, 5 U.S.C. § 8101, et seq.

Work Locations:
ASOs may perform duties as described in this Statement of Work (SOW) in the following locations:

1. Oklahoma City, Oklahoma.
2. Kansas City, Missouri.
3. Other locations as required.

Assistant Director (AD), JPATS/designee may authorize qualified ASOs to carry and use firearms and less than lethal devices. The authority to carry a concealed weapon is extended to the ASOs to the extent necessary to meet the objectives of this written SOW. No authority is extended to carry a concealed weapon beyond duty assignments.

When handling prisoners, ASOs can work independently under the supervision of JPATS operational personnel. ASOs will not be teamed with other types of contract guards.

5. Scope

The ASO shall augment the JPATS staff in the:

Safe and secure custody of USMS prisoners while transporting, guarding, handling, or processing them in or between courthouses, detention facilities, medical facilities, aircraft, JPATS airlift sites, and other USMS secured spaces as needed.

Securing of federal, seized, or forfeited property (including entry control, roving patrol, fixed posts, and emergency response).

ASOs may be used to transport prisoners by commercial air if accompanied by a USMS operational employee(s). Professional Conduct: ASOs will adhere to the USMS Code of Professional Responsibility Policy Directive while on duty.

6. Key Personnel Qualifications

Each ASO is identified as key personnel for the USMS. As such, these are the minimum qualifications and shall be provided in a resume type format:

Experience:
Experience is in accordance with USMS Policy 9.37(A)(2)(a-d).

Must be actively employed state, local, or reserve, law enforcement officers with arrest authority and a minimum of one-year experience; or

Actively employed state, local, or reserve, corrections or detention officers with a minimum of one-year experience in prisoner handling or detention; or

Former or retired law enforcement, corrections, detention, or military police officers who have not been separated or retired for more than five years prior to contracting with the USMS**.**

Current ASO experience may be credited toward meeting the mandatory experience.

Medical Examination:
The ASO's MUST pass a medical examination prior to any contract award.

The JPATS shall pay expenses associated with medical examination directed by JPATS management at medical facilities identified by JPATS. JPATS shall provide the medical facility with the relevant forms necessary for the medical evaluation. The Medical Reviewing Official shall provide final determination of medical examination results to JPATS, indicating the permissibility of full execution of job requirements. Authorization to work/duty is when the Medical Reviewing Officials finds "Fit-for-Duty" without restrictions.

Any/all medical restrictions of the ASO shall be disclosed and explained so that the medical facility may properly assess the work restriction and determine to and if what extent such restrictions may or may not prevent the ASO from performing certain duties.

Travel time and/or mileage incurred by the ASO for the physical exam are not the responsibility of the government and are not reimbursable. Any treatment or other medical services provided to the ASO beyond the required medical examination is the responsibility of the ASO.

Drug Test:
The ASO MUST pass a drug test prior to any contract award.

Drug tests shall be administered in conjunction with the medical exam at the medical facility at no cost to the ASO (JPATS shall pay for the test). The Medical Reviewing Official shall ensure that a drug test has been conducted and test results provided to JPATS for review.

Vaccinations:
Tuberculin (TB) - USMS Policy 3.33, Tuberculosis Screening for USMS Employees. All employees who handle prisoners or who work in the cellblock area shall have Mantoux TB skin test using Purified Protein Derivative (PPD) with repeat screening on at least an annual basis following the recommendation of the Centers for Disease Control (CDC), American Thoracic Society and, the Infections Disease Society of America (see Exposure Control Plan for Occupational Exposure Airborne Pathogens directive for testing protocol). This test shall be administered during the annual medical exam and at the government's expense. JPATS is only responsible for the cost of the test. Any follow-on medical services required shall be received at the ASO's individual health care provider and at the ASO's expense.
ASO contracts shall be modified should any federal mandate with respect to requiring vaccinations as it could impose obligations with safety measures in the contractor's workplace. The Government reserves the right to terminate the contract if the contractor does not comply.

Injuries:
Injury/impairment that occur while engaged in JPATS Operations shall be reported immediately to JPATS management. In the event of the work-related injury/impairment JPATS Supervisors will coordinate with the USMS Workers Compensation Program Specialist for guidance.

Incapacitations:
Any ASOs incapacitated while under contract due to serious illness, injury, surgery/operation or disease, shall provide medical documentation regarding recovery and ability to resume duties without restrictions. Prior to resumption of such duties, JPATS will direct the ASO to be re-examined in accordance with the Medical Examination. JPATS shall pay for the examination cost.

7. Personnel Security Requirements

The Government shall designate the ASO's "Unescorted" or "Escorted."

Unescorted
ASO's may be granted access to USMS controlled spaces.

Escorted
ASO's are required to be in the presence of USMS personnel when in USMS controlled spaces.
The division may provide Escorted ASOs with a standard identification card (USM230A, Contract Guard Credential Card).

ASOs will be escorted while in USMS-controlled space unless they have a current background investigation or a waiver that has been favorably adjudicated by the Tactical Operations Division (TOD). After the division receives a favorable determination through either a completed investigation or waiver, the division may issue a physical access card to the ASO based on their internal policies.

The contractor shall ensure that the person(s) to be utilized under the performance of this contract shall have submitted to the federal Government a completed background investigation request. The intent and purpose of the investigation is to preclude the assignment of any individual who poses a threat or unacceptable risk to the USMS due to past unlawful/ inappropriate behavior or any issues which negatively affect his/her fitness to work for, or on behalf of, the USMS. The contractor shall ensure that each prospective employee furnishes all required data in the form and format determined by the USMS OSP Personnel Security Branch (PSB).

All contractor personnel performing under this contract are designated as moderate risk and shall be subject to a Tier 2 background investigation.

The Government reserves the right to reject any individual proposed to work under this contract if any derogatory information is discovered during or after the background investigation. The Government also reserves the right to reinvestigate any individual working under this contract, as deemed necessary.

After completion of the background investigation, the Government will review the results and determine if the individual is fit to perform work for, or on behalf of, the USMS. The contractor is prohibited from allowing or directing any individual to perform work under this contract prior to the authorization of PSB.

When an individual has been the subject of a prior background investigation conducted by another Federal Agency and meets the standards prescribed by the current position designation and other reciprocity guidance, approval may be granted based on reciprocity.

The contractor shall immediately provide the USMS with the name(s) of any employee who resigns, retires, has been terminated, or is otherwise no longer assigned to work under this contract. In addition, the contractor is required to notify the USMS of all self-reported criminal activities and/or law enforcement actions involving any employees previously cleared to perform service under this contract within 48 hours of preliminary disclosure.

8. Tasks needed to Accomplish the Objectives

The authority and jurisdiction extended to, or provided by, the personal services contract is strictly limited to the period of time the services are directly provided by the ASO to the USMS. No authority to enforce federal laws or to carry a concealed weapon is extended to the ASO unless performing official duties for the USMS. All ASOs are required to read, understand, and comply with current USMS Policy Directives and Standard Operating Procedures (SOP) annually or as directed by JPATS Management. USMS Policy Directives and SOP will be addressed during ASO Initial Training and made available upon request of the ASO for reference.

The ASO shall provide services in accordance with this SOW upon the direction of JPATS Management. Request for these services may be made at any time of the day or night, and the ASO must be capable of providing the services. ASOs shall participate and successfully complete all JPATS mandated training programs as well as medical certifications.

ASOs are responsible for the secure custody of any federal, state, or local detainee in the custody of JPATS. ASOs must maintain continuous observation of the detainee. In the event of an escape or attempted escape, the ASO must notify the Aviation Enforcement Officer-in-Charge (AEOIC) and/or JPATS Management.

Travel will be performed as required and compensable according to the rules for reimbursement of the Department of Justice and JPATS SOP. ASOs who volunteer to support international missions must have a U.S. Passport and comply with all USMS policies and directives pertaining to international travel. The ASO will be reimbursed for actual hours worked and travel expenses; however, the ASO will not be reimbursed for any costs involved in obtaining the U.S. Passport. International travel on JPATS missions is strictly voluntary.

JPATS Management will inform ASOs of inmates or detainees with any special handling instructions.

The ASO shall maintain all JPATS personally identifiable information (PII), classified materials and records in accordance with DOJ, USMS Policy Directives and JPATS SOP. Any questions may be directed to JPATS Management and/or the USMS Operational Security (OPSEC) Coordinator.

9. Quality Assurance

The JPATS Contracting Officer Representative (COR) shall evaluate the ASO performance using USM-601, District/ Aviation Security Officer Personnel Certification, at a minimum of least once every Fiscal Year.

Reviews will be done on a more frequent basis if performance is found to be substandard. The review will document any significant and relevant problems or areas needing improvement.

Performance reviews that cannot be completed due to a lack of cooperation from the ASO will result in an At-Risk or unacceptable which can result in contract termination.

ASOs must return all USMS-issued equipment/property to include any badging to the COR prior to termination of the contract. Any/all expense(s) incurred in returning the equipment shall be paid by the terminated ASO.
ASO's shall immediately report the use of illegal narcotics, violations of prescribed rules, regulations and any violations of statute or law to the USMS.

Termination shall be in accordance with (IAW) the terms and conditions shall be the convenience of the Government and in accordance with (IAW) the Federal Acquisition Regulation (FAR).

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

The Government will provide equipment, supplies, facilities, transportation vehicles, and in some instances firearms and Less Than Lethal (LTL) devices necessary to perform duties as defined in this SOW. The Government shall provide the ASO with applicable documents (e.g., Policies, SOPs, Post Orders), forms, and training materials upon contract award.

ASOs will maintain proper care, custody, and accountability of issued government property pursuant to applicable USMS property management and firearms Policy Directives.

With the exception of firearms, LTL devices, and body armor, accountable USMS property will be issued in accordance with Policy Directive 7.1 Management of Personal Property and will be returned to USMS custody at the end or termination of the ASO contract unless otherwise authorized by the USM/designee or AD, JPATS/designee.
Lost, stolen, or damaged USMS and/or government property or identification will be immediately reported to the COR pursuant to applicable USMS Property Management Policy Directives.

Firearms
ASOs are designated officials of the USMS and if qualified, can be authorized to carry and use firearms (handguns and long-guns) when performing their duties based upon the situation and assessment of the threat level. All USMS issued firearms shall be issued in accordance with USMS Policy and shall be returned to USMS custody at the end of the shift.

Less-Than-Lethal Devices
ASOs are designated officials of the USMS and if qualified, can be authorized to carry and use less-than-lethal devices when performing their duties based upon the situation and assessment of the threat level. All USMS issued less-than-lethal devices shall be issued in accordance with USMS Policy and shall be returned to USMS custody at the end of the shift.

Body Armor
All USMS issued body armor shall be issued in accordance with USMS Policy and shall be returned to USMS custody at the end of the shift.

Uniforms

ASOs shall be issued and wear duty uniforms in accordance with JPATS Standard Operating Procedure (SOP) 1410.6B. All uniform items that are issued to ASOs are government property for official use only and are not to be sold.

Contractor Furnished Equipment/Information (GFE/GFI)

Contractor shall not furnish any GFE/GFI.

1. Other Pertinent Information/Special Considerations

Travel

ASOs may be required to travel to include, but not limited to, overnight stays and offsite missions. Travel is in accordance with the Federal Travel Regulation.

Type of Contract

This is a labor hours contract and IAW FAR 12.207, the ceiling price for the labor hours are:
40-hour work week – not to exceed 2080 hours on a yearly basis (exceeding the ceiling is at the ASO's own risk).
Above 40-hour work week – not to exceed 500 hours on a yearly basis (exceeding the ceiling is at the ASO's own risk).

The ASO must obtain written pre-approval for any hours worked above a 40-hour work week.

The Service Contract Act (SCA) does not apply to personal service contracts (PSC), and the ASO's shall not receive benefits required by the SCA.

Under the Department of Labor (DOL), Fair Labor Standards Action (FLSA), there is no payment for time not worked, such as vacations, sick leave, or holidays (Federal or others). The benefits agreed upon are ONLY the 40-hour work week, above 40-hour week pay, and any items identified by this SOW.

Timekeeping and Payment

The official timekeeping system is webTA for payment purposes. ONLY official webTA timekeepers will enter ASO hours into webTA. ASO's shall not enter their own time or have access to webTA.

ASOs will be required to track and maintain their actual hours worked on a JPATS approved form, spreadsheet, and/or web-based scheduling system, as directed by JPATS management and COR.

ASOs will be reimbursed for actual hours worked (from the time the ASO reports for duty until the time the ASO is released from duty). Travel time to for reporting to the duty location is not reimbursed.

ASOs will be reimbursed at the hourly negotiated rate for this labor hours contract, subject only to withholding of federal and state taxes as required by 26 U.S. Code § 3402(a).

Services provided will be rounded to the nearest quarter hour.

Duty Hours

Contracted hours are scheduled on an "on call/as needed" basis. Emergency work authorized on an as needed basis by the COR.

ASO shall not leave the assignment without notifying the Government designee, including for meals or rest breaks. ASOs will not visit the duty site during non-duty hours unless authorized to do so by the AD, JPATS/designee.

JPATS management will determine if a ASO is able to safely perform duties for the USMS on those occasions when the ASO has also worked a shift or specified hours with a local agency (e.g., working a double shift).

ASOs shall not be scheduled for more than sixteen (16) USMS duty hours per day. If the ASO also worked a shift or specified hours with a local agency (e.g. working a double shift), JPATS shall determine if ASO is safely able to perform the duties outlined in this SOW.

11. Appendix A: Personnel and Property Contractor Compliance Requirement

Appendix A - Personnel and Property Contractor Compliance Requirements shall apply to all Contractors and sub-contractors providing services for performance delivery. Sites maintained by the TO Contractor where work is performed for the Government must meet the minimum federal compliance standards. The Government reserves the right to request an inspection of compliance.

Protection of Property

Contractor's Responsibility - If due to the default, negligence (whether of action or omission) and/or dishonesty of the Contractor or its employees, any Government-owned or controlled property is lost or damaged as a result of the Contractor's performance of this contract, the Contractor shall be responsible to the Government for such loss or damage, and the Government at its option, may, in lieu of payment therefore, require the Contractor to replace at its own expense, all property lost or damaged. Protection - The Contractor shall protect materials in his/her custody against the transportation, fire, theft, weather, and other hazards avoidance in the exercise of the "highest degree of care."

Indemnification

Responsibility for Government-owned or -leased Property and Equipment during contract performance, the Contractor shall be responsible for all negligent acts or omissions of its employees or agents or the employees or agents of its subcontractor(s). In this regard, the contractor shall, at no cost to the Government and at the Government's option, replace or compensate the Government for any damage to or loss of Government owned or -leased property caused by such negligent acts or omissions.

Responsibility for Contractor or Third Party-owned or -leased Property and Equipment. The contractor shall indemnify the Government against any and all liability claims for loss or damage to any Contractor owned or leased property occurring as a result of negligence or omissions by employees or agents of the contractor or its subcontractor(s) in connection with the performance of work under the terms of this contract.
Responsibility for Property and Equipment Damaged or Lost through no fault of the Contractor or the Government. Property damage or loss that occurs through no fault of either the Contractor, their subcontractors or agents or the Government shall be the responsibility of the party holding title to or having leased the property.

Safeguarding Sensitive Data and Information Technology

In accordance with FAR 39.105, this section applies to all users of sensitive data and IT resources, including awardees, contractors, subcontractors, lessors, suppliers, and manufacturers.
The following USMS policies must be followed. These policies can be found at
http://www.usmarshals.gov/foia/directives/information_technology.pdf
DOJ 2421.1E, Use of Government Telecommunications Systems

DOJ Order 0904, Information Technology Security, Sep 15, 2016

DOJ 2880.1B, Information Resources Management Program

DOJ Order 2740.1A, Use and Monitoring of DOJ Computers and Computer Systems

DOJ Order 2420.2, Telecommunications Policy and Guidelines

USMS Directive 1.1 Delegation of Authority, Organization and Functions

Personal Information on DOJ Web Sites, May 2, 2006

DOJ Web Content Guidelines and Suggested Practices, May 10, 1999

DOJ Information Technology, Security Staff (ITSS) Standards, as amended

DOJ Order 2600.2C, Security Programs and Responsibilities

DOJ Security Program Operating Manual (SPOM)

DOJ Order 2610.2A, Employment Security Regulations

DOJ Security and Privacy Assessment and Authorization Handbook v9 (2018), as amended

Department of Justice Information Technology (IT) Security Rules of Behavior (ROB) for General Users (2018), as amended
Department of Justice Information Technology (IT) Security Rules of Behavior (ROB) for Privileged Users (2018), as amended

In addition to the above, a DOJ USMS Non-Disclosure and Confidentiality Agreement (Appendix B) is inclusive of this SOW. As directed by the Government, annual rules of behavior shall be signed, account recertification, asset inventory, and Cyber training shall be required and completed by all contract support staff providing services on this contract.

Confidential Information
All information received by the Contractor as a result of performance of this contract is confidential and subject to the Privacy Act. The Contractor and Contractor personnel shall maintain this information in strict confidence and shall not disclose this information, or any information obtained as the result of its performance of this contract, to any person or entity, other than employees or bona fide Contractors of the USMS, without the prior written approval of the USMS.

The Contractor and Contractor personnel shall not disclose this information to any person or entity or otherwise make any improper use of this information during or after the performance period of this contract. The Contractor and Contractor personnel shall maintain this information in strict confidence and shall make no changes to the information except as necessary in the performance of the contract. The Contractor and Contractor personnel and their successors are prohibited forever from using this information for their personal or business gain, personally or for any other reason, directly or indirectly, without prior written approval from GPO. This provision, or a provision with an identical effect, shall also be placed in any subcontracts.

OSHA
The Contractor is solely responsible for compliance with all federal, state and local laws, the Occupational, Safety and Health Act (OSHA) (Public Law 91-596) and the resulting standards, OSHA Standards 29 CFR 1910 and 1926, as applicable, and the protection of their employees. Additionally, the Contractor is responsible for the safety and health of all subcontractor employees.

Department Policy on Domestic Violence, Sexual Assault, and Stalking
It is the Department's policy to enhance workplace awareness of and safety for victims of domestic violence, sexual assault, and stalking. This policy is summarized in DOJ Policy Statement 1200.02 (Policy Statement), available in full for public viewing at http://www.justice.gov/sites/default/files/ovw/legacy/2013/12/19/federal-workplace-responses-to-domesticviolence-sexualassault-stalking.pdf. Vendor agrees, upon contract award, to provide notice of this Policy Statement, including at a minimum the above-listed URL, to all of Vendor's employees and employees of subcontractors who will be assigned to work on Department premises.

Point of Contact for victims of Domestic Violence, Sexual Assault, and Stalking. Upon contract award, the Department will notify contractor of the name and contact information for the Point of Contact for Victims of domestic violence, sexual assault, and stalking for the component or components where Contractor will be performing. Contractor agrees to inform its employees and employees of subcontractors who will be assigned to work on Department premises of the name and contact information for the Victim Point of Contact.

Representation Regarding Felony Conviction Under Any Federal Law or Unpaid Delinquent Tax Liability (Deviation 2012-02) (January 2012)
(In accordance with sections 543 and 544 of Title V, Division B of the Further Continuing Appropriations Act, 2012 (Pub. L. 112-55), none of the funds made available by that Act may be used to enter into a contract, memorandum of understanding, or cooperative agreement with a corporation convicted of a felony criminal violation of any Federal law within the preceding 24 months, unless an agency has considered suspension and debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government; or

With an unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, unless an agency has considered suspension and debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

By accepting this award or order, in writing or by performance, the offeror/contractor represents that the offeror/contractor is not a corporation convicted of a felony criminal violation under any Federal law within the preceding 24 months; and the offeror/contractor is not a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

Liability
Includes, but is not limited to: services necessary to the installation systems (from design through start-up), maintain the system (including maintenance agreements), training, and travel.

The prime contractor shall be responsible, accountable and liable for all work performed, including work performed by subcontractors (at all tiers), and for ensuring the work performed is completed in accordance with the statement of work.

The prime contractor and subcontractors shall be licensed and bonded.

The prime contractor shall be responsible for insuring that the scope of work is completed and all warranties are honored.

The prime contractor shall insure compliance with all local laws, regulations, and ordinances.

The Government reserves the right to apply liquidated damages whenever the required delivery date is not met.

Publicity
Contractor shall not make publicity releases, including media interviews, in connection with this contract unless prior written approval has been received from the Contracting Officer.

Freedom of Information Act (FOIA) Requests
With respect to a Freedom of Information Act (FOIA) request for any part of the contractor's proposal that is either set forth or incorporated by reference in this task order, before responding to the FOIA requests the Government will afford the contractor an opportunity to explain why it believes some or all of the relevant parts of the proposal may be exempt from release under the FOIA.

Contract Personnel Security Requirements
The contractor and all subcontractors must maintain the required background investigations and site clearance levels required throughout the life of the contract. The contractor shall comply with all security requirements. Security clearance levels may range from Public Trust to Top Secret (TS) with Sensitive Compartmented Information (SCI) levels.

The Government requires that contract personnel obtain and maintain a DOJ security clearances to perform work where access to data or systems is involved. It is the expectation of the Government that the contractor has performed the requisite background checks to ensure that the individuals submitted by the contractor can be successfully adjudicated by the Department.

Security paperwork for proposed personnel shall be submitted upon award to initiate the clearance process. The following issues will require extended security processing time and shall be avoided by the contractor so that contract personnel onboarding will not be delayed: Past due/unpaid loans (student debt, mortgages, credit cards); unpaid IRS taxes/back taxes; arrests; bankruptcies; fired from a job; reporting drug use; and a previously revoked clearance.

Contractor personnel must present two original forms of identification prior to badge issuance. Acceptable documents are listed in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification." At least one document must be a valid State of Federal issued photo identification.
Contractor personnel must appear in person at least once before a USMS official who is responsible for verifying the identification documents. This verification must be completed prior to issuance of a badge.

Contractor personnel must possess a current, favorably adjudicated Background Investigation (BI) commensurate with the designated risk level associated with the duties of each position. The BI requirements for each risk level are outlined below:

National Security Positions: Single Scope Background Investigation (SSBI); 5-year scope

High Risk: Background Investigation (BI); 5-year scope

Moderate Risk: Limited background Investigation (LBI) and/or Minimum Background Investigation (MBI).

Low Risk: National Agency Check with Inquiries (NACI)

The risk associated with this contract is categorized Low Risk; therefore all contractors must possess either a NACI or higher level BI prior to commencing duties at USMS.

Pre-appointment BI waiver requirements for all positions, regardless of sensitivity are:

Favorable review of the security questionnaire

Favorable fingerprint results

Favorable credit report
Waiver request memorandum including both the Office of Personnel

Management interview schedule date and position risk level

Favorable review of the National Agency Check portion of the BI

Badge re-validation will occur once the BI has been completed and favorably adjudicated. If the BI results justify, the badge issued under waiver request will be suspended or revoked.

12. Appendix B: Information Technology Division Non-Disclosure Agreement

This Non-Disclosure/Confidentiality Agreement is a standard agreement designed for use its employees and subcontractors assigned to work as ASO for the DOJ, USMS. 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:

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.

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.

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:

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,

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

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.

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.

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.

13. Appendix C: Department of Justice (DOJ) Cybersecurity and Privacy Rules of Behavior (ROB) for General Users Version 12 January 1, 2019

Introduction

These Rules of Behavior (ROB) for General Users pertain to the use, security, and acceptable level of risk for Department of Justice (DOJ) systems and applications. Each DOJ user is responsible for helping to ensure the security and privacy of DOJ information systems and data. As a user of the DOJ information systems and data, each user serves as the first line of defense in support of DOJ's cyber security protections and enforcement of appropriate privacy protections of Personally Identifiable Information (PII).

The intent of this ROB is to acknowledge receipt and understanding by DOJ users of applicable cybersecurity requirements and responsibilities (as detailed in Federal and DOJ policies and procedures). These requirements include, but are not limited to, the Office of Management and Budget (OMB) Circular A-130, OMB M-17-12, OMB M-16-24, the Privacy Act of 1974, DOJ Order 0904 Cybersecurity Program, DOJ Order 0601 Privacy and Civil Liberties, DOJ Order 2740.1 (series), and the DOJ Cybersecurity Standard.

Who is covered by these rules?

These rules apply to all personnel (government employees, interns, and contractors) who have logical access to DOJ information on DOJ information systems or provide information services to DOJ — hereafter referred to as users. All users are required to review and provide signature or electronic verification acknowledging compliance with these rules to their respective Component cybersecurity representative.

When authorized, users may obtain limited exemptions from particular terms of these ROB for specific occurrences when necessary for performance of official duties. These individual exemption requests must document why a particular rule prevents or hinders mission operations. The information system Authorizing Official (AO) has the ability to issue an exemption if the accepted risk(s) and justification are appropriate, substantiated and documented.[1]

In addition to this ROB, users with escalated privileges on an information system (e.g., administrator) must also agree to and provide signature or electronic verification acknowledging compliance for the Privileged User ROB.
Users will be held responsible for compromising Government information through negligence or willful acts. Users must use caution and follow all statutory and regulatory access, use, maintenance, and disclosure restrictions, as well as adhere to Department and Component level policies regarding the exchange of access-restricted information such as taxpayer, personally identifiable, controlled unclassified, and grand jury information. Failure to comply with the rules and responsibilities listed in this ROB may result in appropriate sanctions, including but not limited to: remedial training; loss of access to information; loss of a security clearance; verbal or written warning; termination of employment; or civil or criminal prosecution.

User Responsibilities - General

Comply with all Federal laws and Department and Component policies and requirements, including DOJ Orders, Policy Statements, and Standards. Use DOJ information and information systems for lawful, official use, and authorized purposes only.
Ensure individuals have the proper clearance, authorization, and need-to-know before providing access to any DOJ information.

Read and accept the DOJ security warning banner that appears prior to logging onto the system or mobile device. Acknowledgment of this ROB also indicates consent to monitoring, recording, and collection of data on all DOJ devices for law enforcement purposes.

Consent to the monitoring and search of any IT equipment brought into, networked to, or removed from DOJ owned, controlled, or leased facilities consistent with employee and contractor consent obtained through logon banners and DOJ policies.

Screen-lock or log off, and remove the personal identity verification (PIV) card from your computer when leaving the work area.

Always keep your PIV card secure. When not in use for authentication and when away from the work area, keep your PIV card on your person and out of sight.

Do not generate, view, download, store, copy, or transmit offensive or inappropriate information in any DOJ medium, to include email messages, documents, images, videos, and sound files (e.g., graphic violence, pornography, hateful language, etc.), unless authorized for official purposes.

Do not access continuous data streams such as viewing streaming video or listening to streaming audio/radio on a website (e.g., YouTube, Netflix, Spotify) on Department computers and computer systems during working or nonworking hours, unless authorized for official purposes.

Adhere to Separation of Duties principles. Avoid conflict of interest in responsibilities, roles, and functions within a system or application (e.g., duties of the System Administrator and Database Administrator should not be combined).

Do not use anonymizer sites on the internet and bypass the Department security mechanisms designed to protect systems from malicious internet sites unless authorized for official purposes.

Do not use Peer-to-Peer (P2P) technology (e.g., BitTorrent) on the internet unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy.

Do not post Department information on cloud-based services unless approved by the Component CIO or designee.

Do not use cloud-based services that have not been approved for use by the Department (e.g., DropBox, iCloud, Google Drive/Docs); use the Department's approved file sharing solutions (e.g., Justice Enterprise File Sharing)

Do not post Department official business information on public websites or social media unless in accordance with applicable Departmental and Component level policies and explicitly authorized for your official duties (e.g., Public Affairs Office).

Do not post information on social media or public websites which allows unauthorized users to infer or obtain non-public information (e.g., system account information, sensitive personally identifiable information (PII), project status, etc.).

Upload only the user's picture as a profile picture in Outlook. User's picture must be in a professional pose from the shoulders up with the U.S. flag or a neutral background.

Protect and safeguard all DOJ information commensurate with the sensitivity and value of the data at risk, including encrypting all sensitive PII (as defined below) before sending to third parties outside of DOJ.

Protect and safeguard all DOJ information and information systems from unauthorized access; unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service; and improper sanitization or use.

Ensure that all DOJ data on authorized removable media (e.g., thumb drives, removable hard drives, and CD/DVD), laptops, tablets, and mobile devices (e.g., smartphones and netbooks) is encrypted with a Department-approved solution unless the Department's CIO or designee approves a waiver from the Department policy. For classified environments, follow the procedures required for those networks for data storage and transport.

Handle all Department data as Sensitive unless designated as Non-Sensitive by the Component Head or Office Director.

Report any anomalous or unusual behavior, and discovered or suspected security incidents to an appropriate point of contact (POC) (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor, or Justice Security Operations Center (JSOC), jsoc@usdoj.gov).

Ensure that you complete any required training in accordance with current Department policies.

Follow all Department level and Component level policies related to user responsibilities for the recording of information into the Department's recordkeeping systems, and comply with applicable records retention schedules.

<u>Classified Systems/Information</u>

Do not use portable electronic devices (e.g., smart watches, fitness trackers, laptops, mobile devices, and removable media except CD-R for music) in sensitive compartmented information facilities or areas where classified information processing is authorized.[2]

Properly mark and label classified and sensitive documents, electronic equipment, and media.[3]

Do not process classified information on an unclassified system.

Send classified email only on systems or authorized devices with the appropriate level of security classification.

Operate information systems only in areas certified for the highest classification or sensitivity level of the information being processed. When not in use, classified items should be stored and contained in an approved security facility.[4]

Receive the proper security training before handling classified removable media. Transport classified removable media only when authorized.

Passwords

Comply with Department and Component password policies (e.g, must be at least 12 characters, contains upper-case, lower-case, numeric, and special characters (e.g. ~ ! @ # $ % ^ & * ( ) _ + = -‘ [] / ? > <)).

Change the default password upon receipt from a system administrator.

Do not share account passwords with anyone.

Avoid using the same password for multiple accounts.

Hardware

Do not add, modify, or remove hardware, or connect unauthorized accessories or communications connections to DOJ resources unless specifically authorized.

Do not access the internal components of the computer or its hard drive from DOJ facilities, unless specifically authorized.

Software

Do not copy or distribute protected intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). Use only DOJ-licensed and authorized software.

Do not install or update any software unless specifically authorized. Submit requests for system changes through the appropriate help desk or configuration management process.

Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized.

Do not change any configurations or settings of the operating system and security-related software, or circumvent and test the security controls of the system unless authorized through the documented configuration management procedures.

Email Use

Limit distribution of email only to those who are authorized and need to know the information to perform their job duties.

Do not open emails from suspicious sources (e.g., people you do not recognize, know, or normally communicate with) and do not visit untrusted or inappropriate websites, unless authorized for official purposes. Download permissible files only from known and reliable sources and use virus-checking procedures prior to file use.

Do not auto-forward emails from your DOJ email account to or through a non-DOJ email system (e.g., Gmail, Yahoo, Outlook.com).

Comply with DOJ Policy Statement 0801.04, Electronic Mail and Electronic Messaging Policy Statement, on the appropriate capture of email.

Do not use personal email accounts for DOJ business except under exigent circumstances and in accordance with Policy Statement 0801.04, Electronic Mail and Electronic Messaging Policy Statement, and any Component-level policy related to the use of personal email accounts.

Mobile Computing and Remote Access[5]

Use mobile Government Furnished Equipment (GFE) (e.g., laptop, tablet, smartphone) for official business and authorized use in accordance with the *de minimis* rule. Mobile GFE is for use by DOJ personnel only and shall connect to DOJ networks only through an approved DOJ remote access method.

Always keep GFE mobile devices, portable electronic devices and removable media secure. When not in use, keep GFE mobile devices, portable electronic devices and removable media in your physical presence and out of sight.

Do not bypass native mobile device operating system controls to gain increased privileges (e.g., jailbreaking or rooting the device).

Download and/or install only authorized applications and software on DOJ mobile devices, and only from DOJ-authorized sources.

Update all mobile devices, including applications and operating systems (e.g., iOS 12 .1. 3 +) to the latest versions and in the timely manner.

Install DOJ-provided removable media, including memory (such as SD cards) and subscriber identity module cards, only on GFE mobile devices.

Immediately report lost or stolen devices (e.g., laptop, phone, tablet, thumb drive) to your appropriate POC (e.g., Help Desk, Incident Response Representative, Security Manager, Supervisor, or JSOC (jsoc@usdoj.gov)).

Do not associate a personal gift or credit card with a government app store account (e.g., iTunes or Google Play). Authorized mobile application purchases should be made by the appropriate contracting officer or official designee (e.g., government purchase card holder).

Unless explicitly authorized by the AO for mobile devices follow these rules:
Do not connect non-DOJ mobile devices and/or accessories to DOJ networks, with the exception of Guest Networks.

Do not connect mobile GFE to non-DOJ information systems, to include personal computers.

Follow your organization's telework guidelines when working remotely and/or remotely accessing DOJ information remotely.

Ensure the confidentiality of government information when using remote access from a non-GFE device (public or private). As per the DOJ Strong Authentication Plan,[6] this includes the following: Device cannot be joined to the DOJ network domain via VPN.

Virtual Conferencing
Hosts and presenters must provide participants with advance notice if the virtual conference session is being recorded.

Do not access a virtual conference presentation using a privileged user account.

Limit presentation information to only that which is authorized for dissemination.

Delete all DOJ information on a provider's web site immediately upon the end of a virtual conference.

Do not install any agents or other software designed to enhance or aid in virtual conferencing. Submit requests for system and software changes through the appropriate help desk or configuration management process.

Employ strong participant authentication mechanisms (e.g., multi-factor authentication, PIN creation, unique login credentials).

Users are provided with logging, auditing, and the appropriate/authorized meeting functions (e.g., upload, download, desktop sharing).

Traveling Users

Adhere to the Department requirements and recommendations regarding foreign travel and mobile devices in the *DOJ Mobile Device and Mobile Application Security Policy*.[9]

Your Component CIO/AO, or equivalent, shall notify the appropriate Component POC in advance of foreign travel with the dates and location(s) of travel when you intend to bring a mobile device to a general-risk country. Your Component POC will then notify JSOC (jsoc@usdoj.gov). The DOJ Chief Information Security Officer must approve the use of laptops for any foreign travel and mobile devices to countries designated as high-risk.[10] The user's Component CIO/AO, or equivalent, shall notify the appropriate Component POC (in advance) of foreign travel. Dates and location(s) of travel will be provided for when the user intends to bring a mobile device to a general-risk country. The user's Component POC will then notify JSOC (jsoc@usdoj.gov). The DOJ Chief Information Security Officer (CISO) must approve the use of laptops and mobile devices in countries designated as high-risk.

64. Inspect computers, smartphones, and any other media that have been transported outside the United States for compromise prior to any physical or logical connection to any DOJ system.

Minimize the information on your information system to what is required to perform a particular mission while traveling and destroy copies of sensitive data when no longer needed.

Shut down devices when not in use or no longer needed. If the device is needed but not the associated network capability, turn off/disable the network/wireless network functionality.

Assume all communications (including cellular services) are intercepted and read when on travel in a foreign country.

Keep your remote access token separate from the laptop/tablet (preferably on you) when possible.

Personally Identifiable Information (PII)

TRAINING:

Complete mandatory privacy training as part of the on-boarding process and annually thereafter, as required by and within the timeframe set by applicable component policy.

Complete role-based privacy training as required by applicable policy, including when the staff member performs specialized privacy roles and responsibilities.

Complete Cybersecurity Awareness Training or similar security training at least annually.

Adhere to all PII training and procedures that are specific to your position.

NO EXPECTATION OF PRIVACY:

Know that DOJ information systems include computers, computer networks, and all devices and storage media attached to a(n) DOJ network or to a computer on such network.

Understand and consent to having no expectation of privacy regarding any communications transiting, stored on, or traveling to or from DOJ information systems.

Understand and consent that the Government routinely monitors communications occurring on DOJ information systems for any lawful government purpose including, but not limited to, monitoring network operations, quality control, employee misconduct investigations, law enforcement investigations, and counterintelligence investigations.

Understand and consent that, at any time, the Government may for any lawful government purpose monitor, intercept, search, and seize communications or information transiting, stored on, or traveling to or from DOJ information systems.

Understand and consent that any communications or information transiting, stored on, or traveling to or from DOJ information systems may be disclosed or used for any lawful government purpose.

COLLECTION OF PII:

Know that “PII” 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. PII can be in any medium or form, including paper, oral, and electronic.

Limit the collection of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of your responsibilities.

Know that Social Security numbers (SSNs) are singular personal identifiers, and their use poses unique privacy risks, including the risk of identity theft. Special procedures apply to the collection, use, and disclosure of SSNs in some instances; for example, you need to coordinate any disclosure of SSNs outside DOJ with your Senior Component Official for Privacy (SCOP)[11] to ensure that such disclosure is authorized by law. See DOJ Memo on *Minimizing the Use and Disclosure of Social Security Numbers and Protecting Personally Identifiable Information in Motion* (2012).

Collect no information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the information is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.

Follow applicable Department and Component-level policies related to responsibilities for the recording or inputting of information into the Department’s official recordkeeping systems.

ACCESS AND USE OF PII:
Limit the access and use of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of your responsibilities.

MAINTENANCE OF PII:
Protect and safeguard PII from loss, compromise, or unauthorized access commensurate with the sensitivity and value of the information and applicable policy. For example, encrypt Social Security numbers when sending via email to any email address outside of the Department.[12]

Comply with applicable records retention schedules including requirements to destroy, delete, or purge information, and requirements to preserve or produce it.[13]

Use only authorized and appropriate techniques to erase, delete, or purge PII, or dispose of media containing PII.

Do not use personally owned information technology such as computers or removable media to store government related work or Department PII.

DISCLOSURE OF PII:
When considering whether to disclose PII (including PII within emails) to a DOJ recipient, ensure the recipient has a need-to-know that information to perform his or her job duties, and that such sharing complies with DOJ policy and the law.

When considering whether to disclose PII (including PII within emails) to a non-DOJ recipient, follow applicable DOJ and/or component policy and the law, which may also involve keeping an accounting of the date, nature, and purpose of the disclosures, and the name and address of the person or agency to whom the PII is disclosed. Need-to-know may not be sufficient justification, by itself, for PII disclosure to a non-DOJ recipient.

Disclose PII to members of the public including individuals or the media only as allowed by the scope of duties, applicable DOJ and/or component policy, and the law.

Do not post information, including PII, on any social media or public website that allows unauthorized user(s) to infer or obtain non-public information.

BREACH:
Know a “breach” is 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.

Report all suspected or confirmed breaches of PII to your supervisor and component-level Security Operations Center or DOJ Justice Security Operations Center (jsoc@usdoj.gov) as applicable, as soon as possible without unreasonable delay, but no later than 1 hour after discovery, and consistent with DOJ Instruction 0900.00.01, *Reporting and Response Procedures for a Breach of Personally Identifiable Information.*

[1] For additional information on mobile device exemptions, please refer to the *Department of Justice Mobile Device and Mobile Application Security* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile-DeviceMobile-Appl-Sec-Supp-2017A.pdf).

[2] For additional information on authorized use of PEDs when working in spaces authorized to process classified information, please refer to *DOJ Order 0904* (https://portal.doj.gov/sites/dm/dm/Directives/0904.pdf), DOJ Security Program Operating Manual (*SPOM) Chapter 8* (http://dojnet.doj.gov/jmd/seps/spom/chapter8.pdf), and *Intelligence Community Directive 503* (http://www.dni.gov/files/documents/ICD/ICD_503.pdf).

[3] For additional instruction on proper markings, please refer to the *DOJ Security Program Operating Manual (SPOM)*

[4] For additional information on removable media, please refer to the *DOJ Removable Media Requirements for Classified Systems* (https://dojnet.doj.gov/jmd/seps/docs/removable_media_requirements.pdf).

[5] For additional information, please refer to the *DOJ Mobile Device and Mobile Application Security Policy* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile-Device-Mobile-ApplSec-Supp-2017A.pdf).

[6] https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/doj-strong-authentication-plan.pdf

[7] PIV card readers must be tested and approved by GSA, and therefore listed on the Approved Products List on the Federal ICAM site -https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage

[8] Procurement of PIV card readers must comply with DOJ Procurement Guidance (PGD) 14-03 a. User must authenticate to a VDI solution with an approved LOA-4 credential.

[9] For additional information on traveling with a mobile device, please refer to *the DOJ Mobile Device and Mobile Application Security Policy* (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/Mobile-Device-MobileAppl-Sec-Supp-2017A.pdf). [10] For additional information on foreign travel requirements, please refer to the *DOJ IT Resources Outside U.S. Territory Waiver Request* form (https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/2-DOJ_Policy_Instruction/foreign_travel_it_resources_1_2.pdf).

[11] to ensure that such disclosure is authorized by law. See DOJ Memo on *Minimizing the Use and Disclosure of Social Security Numbers and Protecting Personally Identifiable Information in Motion* (2012).

[12] See Department policy memoranda from DOJ CIO and CPCLO regarding protecting PII and sensitive PII at https://dojnet.doj.gov/jmd/ocio/ocio-document_library/cs/4 DOJ_%20IT_Memoranda/Data_Loss/Safeguarding%20PII%20Memo.pdf, and https://dojnet.doj.gov/privacy/docs/safeguarding sens-pii.pdf.

[13] For disposal guidance, please refer to Record Management, DOJ Order 0801 (https://portal.doj.gov/sites/dm/dm/Directives/0801.pdf).

Section 2 - Contract Clauses

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)
52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2011)	
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)	
52.222-50	Combating Trafficking in Persons (Nov 2021)	
52.223-18	[Reserved]	
52.232-7	Payments under Time-and-Materials and Labor Hour Contracts (Nov 2021)	(h)(2): "30th"
52.243-3	Changes-Time-and-Material or Labor-Hours (Sept 2000)	
DJAR-PGD-15-03	Security of Department Information and Systems	
DOJ-03	Personnel Security Requirements For Contractor Employees (Nov 2021)	
USMS-0002	Release of Residual Funds (Greater Than $100)	
USMS-0007	Federal Workplace Responses to Domestic Violence, Sexual Assault and Stalking (2014)	
USMS-0009	NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT	
USMS-0010	CONTRACT/ORDER CLOSEOUT - FIXED-PRICE, TIME-AND-MATERIALS, OR LABOR HOURS	
USMS-0011	RELEASE OF CLAIMS	
DOJ-05	Security of Department Information and Systems DOJ-05 (OCT 2023)	

Clauses By Full Text

52.213-4 Terms and Conditions-Simplified Acquisitions (Other Than Commercial Products and Commercial Services) (Jan 2025)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses that are incorporated by reference:

(1) The clauses listed below implement provisions of law or Executive order:

(i) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(ii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (Dec 2023) (Section 1634 of Pub. L. 115-91).

(iii) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(iv) 52.204-27, Prohibition on a ByteDance Covered Application (Jun 2023) (Section 102 of Division R of Pub. L. 117-328), unless the agency grants an exception--see paragraph (b) of 52.204-27.

(v) 52.204-30, Federal Acquisition Supply Chain Security Act Orders-Prohibition. (Dec 2023) (Pub. L. 115-390, title II).

(vi) 52.222-3, Convict Labor (Jun 2003) (E.O. 11755).

(vii) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(viii) 52.222-26, Equal Opportunity (Sept 2016) (E.O. 11246).

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

(x) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801).

(xi) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(xii) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Pub. L. 108-77 and 108-78 (19 U.S.C. 3805 note)).

(2) Listed below are additional clauses that apply:

(i) 52.232-1, Payments (Apr 1984).

(ii) 52.232-8, Discounts for Prompt Payment (Feb 2002).

(iii) 52.232-11, Extras (Apr 1984).

(iv) 52.232-25, Prompt Payment (Jan 2017).

(v) 52.232-39, Unenforceability of Unauthorized Obligations (Jun 2013).

(vi) 52.233-1, Disputes (May 2014).

(vii) 52.244-6, Subcontracts for Commercial Products and Commercial Services (Jan 2025).

(viii) 52.253-1, Computer Generated Forms (Jan 1991).

(b) The Contractor shall comply with the following FAR clauses, incorporated by reference, unless the circumstances do not apply:

(1) The clauses listed below implement provisions of law or Executive order:

(i) 52.203-17, Contractor Employee Whistleblower Rights (Nov 2023) (41 U.S.C. 4712); this clause does not apply to contracts of DoD, NASA, the Coast Guard, or applicable elements of the intelligence community--see FAR 3.900(a).

(ii) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note) (Applies to contracts valued at or above the threshold specified in FAR 4.1403(a) on the date of award of this contract).

(iii) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2025) (E.O. 13126) (Applies to contracts for supplies exceeding the micro-purchase threshold, as defined in FAR 2.101 on the date of award of this contract).

(iv) 52.222-20, Contracts for Materials, Supplies, Articles, and Equipment (Jun 2020) (41 U.S.C. chapter 65) (Applies to supply contracts over the threshold specified in FAR 22.602 on the date of award of this contract, in the United States, Puerto Rico, or the U.S. Virgin Islands).

(v) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212) (Applies to contracts valued at or above the threshold specified in FAR 22.1303(a) on the date of award of this contract).

(vi) 52.222-36, Equal Employment for Workers with Disabilities (Jun 2020) (29 U.S.C. 793) (Applies to contracts over the threshold specified in FAR 22.1408(a) on the date of award of this contract, unless the work is to be performed outside the United States by employees recruited outside the United States). (For purposes of this clause, "United States" includes the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, and Wake Island.)

(vii) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212) (Applies to contracts valued at or above the threshold specified in FAR 22.1303(a) on the date of award of this contract).

(viii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67) (Applies to service contracts over $2,500 that are subject to the Service Contract Labor Standards statute and will be performed in the United States, District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, Johnston Island, Wake Island, or the outer Continental Shelf).

(ix)(A) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O 13627) (Applies to all solicitations and contracts).

(B) Alternate I (Mar 2015) (Applies if the Contracting Officer has filled in the following information with regard to applicable directives or notices: Document title(s), source for obtaining document(s), and contract performance location outside the United States to which the document applies).

(x) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022) (Applies when 52.222-6 or 52.222-41 are in the contract and performance in whole or in part is in the United States (the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, Johnston Island, Wake Island, and the outer Continental Shelf as defined in the Outer Continental Shelf Lands Act (43 U.S.C. 1331, et seq.))).

(xi) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706) (Applies when 52.222-6 or 52.222-41 are in the contract and performance in whole or in part is in the United States (the 50 States and the District of Columbia.))

(xii) 52.223-5, Pollution Prevention and Right-to-Know Information (May 2024) (42 U.S.C. 11001-11050 and 13101-13109) (Applies to services performed on Federal facilities).

(xiii) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (May 2024) (42 U.S.C. 7671, *et seq*.) (Applies to contracts for products as prescribed at FAR 23.109(d)(1)).

(xiv) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (May 2024) (42 U.S.C. 7671, *et seq*.) (Applies to maintenance, service, repair, or disposal of refrigeration equipment and air conditioners).

(xv) 52.223-20, Aerosols (May 2024) (42 U.S.C. 7671, et seq.) (Applies to contracts for products that may contain high global warming potential hydrofluorocarbons as a propellant or as a solvent; or contracts for maintenance or repair of electronic or mechanical devices).

(xvi) 52.223-21, Foams (May 2024) (42 U.S.C. 7671, et seq.) (Applies to contracts for products that may contain high global warming potential hydrofluorocarbons or refrigerant blends containing hydrofluorocarbons as a foam blowing agent; or contracts for construction of buildings or facilities.

(xvii) 52.223-23, Sustainable Products and Services (May 2024) (E.O. 14057, 7 U.S.C. 8102, 42 U.S.C. 6962, 42 U.S.C. 8259b, and 42 U.S.C. 7671l) (Applies to contracts when the agency identifies in the statement of work, or elsewhere in the contract, the sustainable products and services that apply to the acquisition).

(xviii)(A) 52.225-1, Buy American-Supplies (Oct 2022) (41 U.S.C. chapter 67) (Applies to contracts for supplies, and to contracts for services involving the furnishing of supplies, for use in the United States or its outlying areas, if the value of the supply contract or supply portion of a service contract exceeds the micro-purchase threshold, as defined in 2.101 on the date of award of this contract, and the acquisition--

(1) Is set aside for small business concerns; or

(2) Cannot be set aside for small business concerns (see 19.502-2), and does not exceed $50,000).

(B) *Alternate I* (Oct 2022) (Applies if the Contracting Officer has filled in the domestic content threshold below, which will apply to the entire contract period of performance. Substitute the following sentence for the first sentence of paragraph (1)(ii)(A) of the definition of domestic end product in paragraph (a) of 52.225-1:

(A) The cost of its components mined, produced, or manufactured in the United States exceeds N/A percent of the cost of all its components. [*Contracting officer to insert the percentage per instructions at 13.302-5(d)(4)*.])

(xix) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792) (Applies to contracts greater than the threshold specified in FAR 26.404 on the date of award of this contract, that provide for the provision, the service, or the sale of food in the United States).

(xx) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct 2018) (Applies when the payment will be made by electronic funds transfer (EFT) and the payment office uses the System for Award Management (SAM) as its source of EFT information).

(xxi) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (Applies when the payment will be made by EFT and the payment office does not use the SAM database as its source of EFT information).

(xxii) 52.240-1, Prohibition on Unmanned Aircraft Systems Manufactured or Assembled by American Security Drone Act-Covered Foreign Entities (Nov 2024). (Sections 1821-1826, Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

(xxiii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305) (Applies to supplies transported by ocean vessels (except for the types of subcontracts listed at 47.504(d)).

(xxiv) 52.247-69, Reporting Requirement for U.S.-Flag Air Carriers Regarding Training to Prevent Human Trafficking (Jan 2025) (49 U.S.C. 40118(g)). (Applies to contracts with a U.S.-flag carrier for the transportation by air of passengers; does not apply to contracts awarded by the Department of Defense or contracts for commercial products).

(2) Listed below are additional clauses that may apply:

(i) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Nov 2021) (Applies to contracts when the contractor or a subcontractor at any tier may have Federal contract information residing in or transiting through its information system.)

(ii) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded (Jan 2025) (Applies to contracts over the threshold specified in FAR 9.405-2(b) on the date of award of this contract).

(iii) 52.211-17, Delivery of Excess Quantities (Sept 1989) (Applies to fixed-price supplies).

(iv) 52.247-29, F.o.b. Origin (Feb 2006) (Applies to supplies if delivery is f.o.b. origin).

(v) 52.247-34, F.o.b. Destination (Jan 1991) (Applies to supplies if delivery is f.o.b. destination).

(c) *FAR 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):

https://www.dau.edu/tools/dau-provision-and-clause-matrix
[*Insert one or more Internet addresses*]

(d) *Inspection/Acceptance*. The Contractor shall tender for acceptance only those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. The Government must exercise its postacceptance rights--

(1) Within a reasonable period of time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(e) *Excusable delays*. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence, such as acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(f) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges that the Contractor can demonstrate to the satisfaction of the Government, using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.

(g) *Termination for cause*. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(h) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(End of clause)

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 5 days [*insert the period of time within which the Contracting Officer may exercise the option*].

(End of clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 2 days [*insert the period of time within which the Contracting Officer may exercise the option*]; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 5 day days [*60 days unless a different number of days is inserted*] before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 4 year, 6 months (months)(years).

(End of clause)

52.249-12 Termination (Personal Services) (Apr 1984)

The Government may terminate this contract at any time upon at least 15 days' written notice by the Contracting Officer to the Contractor. The Contractor, with the written consent of the Contracting Officer, may terminate this contract upon at least 15 days' written notice to the Contracting Officer.

(End of clause)

DOJ-02 Contractor Privacy Requirements (JAN 2022)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

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

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

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

(3) Prior Approval Required to Hire Subcontractors

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

(4) Separation Checklist for Contractor Employees

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

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

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

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

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

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

(2) Safeguarding PII Requirements

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

(3) Non-Disclosure Agreement Requirement

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

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

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

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

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

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

(5) Reporting Actual or Suspected Data Breach

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

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

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

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

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

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

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

(6) Victim Remediation

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

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

(1) Records Management Training and Compliance

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

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

(2) Records Creation, Ownership, and Disposition

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

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

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. The Agency and its contractors are responsible for preventing the alienation or unauthorized

destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. § 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the Agency records schedules.

D. Data Privacy and Oversight

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

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

(2) Requirements for Contractor IT Systems Hosting Government Data

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

(3) Requirement to Support Privacy Compliance

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

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

[1] “[T]he term ‘record’ means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.” 5 U.S.C. § 552a(a)(4). “[T]he term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” 5 U.S.C. § 552a(a)(5).
[2] As stated in FAR 52.224-3 and Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource (2016), “’personally identifiable information’ means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” Regarding “sensitive PII,” “[t]he sensitivity level of the PII will depend on the context, including the purpose for which the PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed. For example, the sensitivity level of a list of individuals’ names may depend on the source of the information, the other information associated with the list, the intended use of the information, the ways in which the information will be processed and shared, and the ability to access the information.” OMB Circular A-130, at App. II-2.
[3] The DOJ OPCL Resources page is available at https://www.justice.gov/opcl/resources.

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

(End of Clause)

USMS-0012 Contracting Officer's Representative (COR)

CONTRACTING OFFICER'S REPRESENTATIVE (COR) (AUG 2017)
(a) [Name] 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:[Phone]
E-mail:[Email]
(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)

Section 3 - List of Attachments

This Section Is Intentionally Left Blank

Section 4 - Solicitation Provisions

Provisions By Reference

52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)		
This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): www.acquisition.gov		
Provision	Title	Fill-ins (if applicable)
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Nov 2021)	(d)(1) will not: "X" (d)(2) Does not: "X"
52.209-11	Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)	
52.225-25	Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran--Representation and Certifications (Jun 2020)	