This is a combined synopsis/solicitation for commercial services prepared in accordance with Part FAR Part 12, Acquisition of Commercial Products and Commercial Services, using FAR Part 15 Negotiated Procurement Procedures. This announcement constitutes the only solicitation. Offers are being requested and a separate written solicitation will not be issued.

Solicitation number 15JPSS26Q00000058 is issued as a request for proposal (RFP), for Legal Services.

This acquisition is not set aside for small business concerns. This solicitation incorporates provisions and clauses by reference. The full text of provisions and clauses may be accessed electronically at www.acquisition.gov.

The requirement will be awarded as a standalone Firm Fixed Price Contract Type. The Government reserves the right to award a contract without negotiations if the Contracting Officer determines that the initial offer provides the best value to the Government and negotiations are not necessary.

PART I – THE SCHEDULE

Section A - Continuation of Solicitation/ Contract Form

A1. Brief Description of Services

The U.S. Department of Justice, Executive Office for Immigration Review (EOIR), created the Legal Access Services for Reunified Families (LASRF) Program pursuant to the Settlement Agreement in Ms. L., et al. v. U.S. Immigration and Customs Enforcement, et al., 18-cv-00428 (S.D. Cal. Oct. 16, 2023) ("Settlement Agreement"). The LASRF Program is divided into two components: (1) federalized services, including group orientations and group workshops, that EOIR provides, and (2) individualized services, including legal advice and document preparation, that the Contractor provides under this Statement of Work (SOW). EOIR, through the federalized program, also operates a centralized email address and telephone number to receive requests for assistance and to connect eligible individuals to the full range of legal services that are available under the Settlement Agreement.

The Government seeks a contractor to satisfy the Government's obligations under the Settlement Agreement by delivering individualized legal services that complement the group orientations and workshops that EOIR provides to Program Participants. All work shall be performed in accordance with Section C, Statement of work, and shall meet the highest quality standards, consistent with industry best practices, to ensure timely performance, optimum agency satisfaction, and adequately protect the interests of the Government.

DOJ EOIR intends to enter into a standalone firm fixed price contract to obtain legal services. The contract shall have one twelve-month Base Period and four twelve-month Option Periods.

A2. NAICS Code and Size Standard

a. The North American Industry Classification System (NAICS) code for this acquisition is 541110: Offices of Lawyers.
b. The small business size standard is $15.5 Million.

A3. Solicitation

The Solicitation opens on 06/11/2026, and Closes on 07/13/2026 at 10:00AM Eastern Standard Time.

Section B – Services and Price

The Contractor shall provide all personnel, supplies, transportation, supervision, management, tools, materials, and other items necessary to perform non-personal legal services in accordance with the Statement of Work.

B1. Pricing Schedule and CLIN Structure

Contract Line Item (CLIN) pricing schedule for the Base Period and all Option Periods are in Attachment 2 - Pricing Schedule. The prices listed in the pricing schedule are completed as part of an Offeror's price proposal and used to evaluate an Offeror's proposal as stated in Section M of the solicitation. All CLINs are required.

B.2 Payment of Postage and Fees

All postage and fees related to distribution of deliverables including forms, reports, etc., shall be paid by the Contractor.

B.3 Travel

The Government will only provide payment for travel specifically authorized in the contract requirements. Reimbursement shall not exceed the rates and expenses allowed by the Federal Travel Regulation (FTR) which is available at http://www.gsa.gov/ftr. The Contractor will be reimbursed by the Government for actual travel which includes transportation, lodging, meals (per diem expenses) that are incurred by Contractor personnel specifically authorized to travel for contract purposes by the CO. Reimbursement shall not exceed the rates and expenses allowed by Government travel regulations to a Government employee traveling under identical circumstances and will not exceed maximum limits authorized in the Contract. Travel and per diem payments are intended as reimbursement to the Contractor employees and are not subject to profit, deduction, or set-aside by the Contractor.

B.4 Federal Holidays

The Firm fixed price shall include all costs associated with the contractor compensation for federal holidays, leave, overhead, and fringe benefits necessary to perform the required services.

i) The Government hereby provides "NOTICE," and the Contractor hereby acknowledges "RECEIPT" that Government personnel observe the listed days as holidays, see the list below, and this link Federal Holidays:

1. New Year's Day
2. Birthday of Martin Luther King, Jr.
3. Washington's Birthday
4. Memorial Day
5. Juneteenth National Independence Day
6. Independence Day
7. Labor Day
8. Columbus Day
9. Veterans Day
10. Thanksgiving Day
11. Christmas Day

ii) In addition to the days designated as holidays, the Government observes the following days:

(1) Any other day designated by Federal Statute
(2) Any other day designated by Executive Order
(3) Any other day designated by the President's Proclamation

iii) When any such day falls on a Saturday, the following Monday is observed. Except for designated around-the-clock or emergency operations, Contractor personnel will not be permitted to perform on-site under the contract on holidays set forth above. The Contractor shall not charge any holiday as direct cost to the contract. In the event Contractor personnel work during a holiday observed by the Contractor other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost. The provision does not preclude reimbursement for Government-authorized overtime if such overtime is allowable under the terms of the contract.

iv) The Government reserves the right to close the facilities due to weather conditions, safety, health, or medical emergencies as necessary. The Contractor personnel may be required to remain on duty to maintain the facility in the event of adverse weather conditions or emergencies. During these times, the Contractor program manager, or designee, must be available (on-site or by cell phone and email) to address DOJ operational shutdowns or emergencies. Contractor personnel should refer to the Contracting Officer Representative (COR) for early dismissal and closure procedures.

v) It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation, except as set forth within the contract.

vi) Nothing in the clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of the contract.

vii) The Contractor shall perform work in a manner that does not interfere with normal occurrence of Government business.

Section C – Statement of Work (SOW)

The Contractor shall perform work in accordance with the terms and conditions herein, see Attachment 1 - Statement of Work and Attachment 5 – Performance Requirement Standards.

Section D - Packaging and Marking

Packaging and marking requirements are not applicable to this service contract. Any deliverables submitted electronically shall identify the contract number, task order number (if applicable), deliverable title, and submission date. If hard copy materials are required or requested by the Government, all packages shall be clearly marked with: Contract Number, Contractor Name, Deliverable Title, Date of Submission.

All materials shall be packaged to prevent damage during shipment and handling.

Section E - Inspection and Acceptance

E.1 Inspections by the Government: The Government will inspect and make acceptance decisions for all materials, documents, and services provided under the contract, where applicable. The EOIR COR is the authorized representative of the CO. The COR will monitor the Contractor's performance, evaluate the quality of services, and perform the final inspection and acceptance of all deliverables where applicable.

The Government will review and verify all deliverables, invoices, and reports associated with the contract requirements under the contract, to ensure that the Contractor has fulfilled the requirements/standards, as stated in the contract. All deliverables, invoices, and reports will be inspected for content, completeness, accuracy, and conformance to the requirements (including any applicable standards). All deliverables, invoices, and reports will be accepted if they are completed in accordance with the contract specifications, schedules, or other acceptance criteria, as outlined in the contract. The following review procedures will be as follows:

a. The Government will perform an initial review of the deliverables, invoices, and reports. If problems are encountered during the review, the Contractor must correct them as stated in accordance with the SOW and elsewhere in the contract.

b. If necessary, a meeting and/or telephone conference may be held to resolve any differences. The Contractor shall make all required changes to achieve an acceptable deliverable (i.e., invoices, reports).

c. When the review of a deliverable, invoice or report results in necessary changes, the Contractor will, in accordance with the contract, correct the deliverable, invoice, or report as indicated by the Government. It will then be the responsibility of the Contractor to properly and consistently incorporate the comments into the final deliverable, invoice, and/or report.

d. These procedures shall not be construed to constitute a waiver on the part of the Government of its rights under FAR 52.212-4(m) Termination for Cause nor of any other rights or remedies provided by law or under the contract.

e. The Government has authority to make minor adjustments to contractor's submitted invoices to expedite payment due to current agency procedure.

E.2 Formal Acceptance by the Government: Formal acceptance of the performance of work is made by the Government's approving and accepting authority acknowledging such acceptance by a signature approval on the invoicing documents submitted for payment. No payment shall be made under this contract on any services without acceptance being made by the Government.

E.3 Inspections by the Contractor: The Contractor is responsible for the day-to-day inspection and monitoring of all work performed to ensure compliance with contract requirements. The Contractor shall ensure that the required services outlined in Attachment 1-Statement of Work (SOW), and elsewhere in the contract, meet the quality standards as outlined. All work performed under the contract shall be of the highest quality, consistent with best industry practices for legal services.

E.4 Corrective Actions: In the event work is performed by the Contractor unsatisfactorily, the Contractor will be requested to correct the deficiencies.

E.5 Unsatisfactory Performance: The Contractor shall correct all deficiencies, as defined in the contract, from the date of the Government's notification. If all deficiencies have not been corrected, the Government may terminate the contract in whole, or in part, for cause, in accordance with procedures outlined in FAR 52.212-4(m) Termination for Cause.

Section F – Deliveries or Performance

Satisfactory performance of the final contract shall be deemed to occur upon performance of the work described in the Attachment 1 - Statement of Work (SOW) of the contract and upon delivery and acceptance by the Contracting Officer, or the duly authorized representative, of the items in accordance with the stated SOW of the contract.

F.1 Period of Performance

The Base Period of Performance of the contract shall begin on September 01, 2026, and shall not extend beyond August 31, 2027, plus four (1) year Option Periods, which may be exercised at

the Government's discretion. In accordance with FAR 52.217-8, the Government may also extend services for a period not to exceed six (6) months beyond the final period of performance.

Periods	Dates
Base Period	09/01/2026 – 08/31/2027
Option Period One	09/01/2027 – 08/31/2028
Option Period Two	09/01/2028 – 08/31/2029
Option Period Three	09/01/2029 – 08/31/2030
Option Period Four	09/01/2030 – 08/31/2031

F.2 Place of Performance

The Contractor must provide the services described in Section 6.0 of this SOW from eight regional offices.[1] Services are currently provided from the following eight regional offices: 1) Annandale/Sterling, Virginia; 2) Chicago, Illinois; 3) Houston, Texas; 4) Los Angeles, California; 5) Miami, Florida; 6) New Orleans, Louisiana; 7) Newark, New Jersey; and 8) San Francisco, California. Based on the Contractor's assessment of the needs presented in this SOW, the Contractor may propose its own list of eight regional office locations that provide nationwide coverage.

The Contractor must arrange suitable space to provide the services described in this SOW at each designated regional office location. Suitable space may include a private office or other space that is appropriate for private discussions.

The Contractor must provide the services in Sections 6.1 and 6.2 of this SOW via remote technology to Program Participants who prefer remote services or are unable to receive in-person services at any of the regional offices. These remote services can be provided to Program Participants from private spaces via telephone, video-conferencing, or other multi-way remote communication. If remote services are inappropriate because of the Program Participant's language need or disability, the Contractor, with the Program Participant's consent, may submit a written request to the Contracting Officer's Representative (COR) for a transportation stipend from EOIR to allow the family to receive in-person legal services.

The Contractor must also provide pro bono mentorship, as described in Section 6.3 of this SOW, via remote technology. This pro bono mentorship must be available, upon request, to pro bono legal representatives anywhere in the United States who agree to provide free representation to Class Members who participate in the LASRF Program.

[1] Pursuant to the Settlement Agreement, the Government must implement the LASRF program in at least eight regional offices across the United States. The Government may select a single contractor to operate all eight regional offices or multiple contractors to individually operate one or more regional offices.

F.3 Hours of Operation

For deliverable/report submission purposes, normal hours of operation are Monday through Friday, 7:30AM through 4:30PM Eastern Standard Time (EST), excluding federal holidays.

F.4 Delivery of Reports

The Contractor shall submit monthly status reports no later than 11:59 p.m. Eastern Time fifteen (15) business days following the last day of each reporting period, see the SOW for more information.

Reporting Requirements, Data Management, Required Documents and Reports: The Contractor shall prepare and deliver all reports and documents to the CO and COR as specified in the contract. Unless specified otherwise herein, all reports shall be delivered electronically in spreadsheet or database format by email. The Contractor's reports shall be complete, accurate and prepared in a professional manner. Reports delivered by the Contractor(s) shall become a part of the DOJ's official records and subject to review by regulatory authorities and the general public. Unless otherwise specified herein, the format for all reports shall be subject to the approval of the CO and COR.

Ownership and Security of Data and Documents: All DOJ and Contractor collected, maintained, and delivered data files, reports, logs or other documents developed relative to contractual operations are the sole property of the DOJ. The Contractor shall take all measures necessary to secure and safely protect all hardware, software, data and documents from theft, destruction, and unauthorized access. The Contractor shall report any information security or privacy incidents/violations to CO and COR immediately when such incidents/violations occur.

508 Reporting Requirements: All reports required herein shall be submitted in electronic format. All electronic reports submitted shall be compliant with Section 508 of the Rehabilitation Act of 1973.

F.5 Government Closures

Contractor Personnel shall comply with closure procedures due to weather, emergencies, or Government-directed shutdowns.

Section G – Contract Administration Data

G.1 Contract Administration

Contracting Officer (CO)
The Contracting Officer is the only person with authority to act as agent of the Government under the contract. Only the Contracting Officer has authority to:

i) direct or negotiate any changes in a Task Order or contract;
ii) issuing, modifying, or terminating any terms of the contract or any issued TO;
iii) change the delivery schedule;

iv) appointing any Contracting Officer Representative (COR) in writing for the contract or any issued TO;
v) authorize reimbursement to the Contractor any costs incurred during the performance of the contract;
vi) executing final compliance and closeout for the contract or any issued TO;
vii) receiving and providing final approval for processing payments under any TO;
viii) authorize reimbursement to the Contractor any costs incurred during the performance of the contract; or
ix) otherwise change any terms and conditions of the contract.

Contracting Officer (CO):
Tracy-Ann Thomas-Arthur
Contracting Officer
Email: **Tracy-Ann.B.Thomas-Arthur@usdoj.gov**

All requests for information on matters related to the contract shall be submitted in writing via email to the CO.

Contracting Officer Representative (COR)
The COR (To Be Identified Upon Contract Award) is responsible for:
i) monitoring the Contractor's technical progress, including the surveillance and assessment of performance, and recommending to the CO any changes in requirements;
ii) interpreting the SOW and any other technical performance requirements;
iii) performing technical evaluation as required;
iv) performing technical inspections and acceptances required by the contract; and
v) assisting in the resolution of technical problems encountered during performance.

Performance of the work under the contract shall be subject to the technical direction of the COR identified in the contract, or a representative designated in writing. All questions regarding changes to the scope of work shall be directed to the CO. The term "technical direction" includes, without limitation, direction to the Contractor that directs or redirects the labor effort and shifts the work between work areas or locations to ensure that tasks outlined in the work statement are accomplished satisfactorily. Technical direction must be within the scope of the specifications SOW.

The COR **does not** have the authority to issue any technical direction that:

i) Constitutes a change of assignment of additional work outside the SOW;
ii) Constitutes a change as defined in the contract clause entitled "Changes";
iii) In any manner causes an increase or decrease in the total contract price, or the time required for contract performance;
iv) Changes any of the terms, conditions, or specification(s)/work statement of the contract.
v) Interferes with the Contractor's right to perform under the terms and conditions of the contract; or

vi) Directs, supervises or otherwise controls the actions of the Contractor's Employees.

Technical directions may be communicated orally or in writing. The COR shall confirm oral direction in writing within two (2) workdays, with a copy to the CO.

The Contractor shall proceed promptly with the performance resulting from the technical directions issued by the COR. If, in the opinion of the Contractor, any direction of the COR, or his/her designee, falls within the limitations in the above terms, the Contractor shall immediately notify the CO no later than the beginning of the next Government workday.

Failure of the Contractor and the CO to agree that technical direction is within the scope of the contract shall be subject to the terms of the clause entitled "Disputes."

The type of actions within the purview of the COR's authority is to assure that the Contractor performs the technical requirements of the contract, and to notify both the Contractor and the CO of any deficiencies observed.

G.2 Invoicing

Invoices shall be submitted in accordance with JAR 2852-212-4

An invoice must include-

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.,* 52.232-33, Payment by Electronic Funds Transfer-System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer-Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

The COR will certify the invoice for payment. Negative inspection results will be reported immediately to the Contracting Officer. **An email instructing where invoices shall be sent will be forthcoming upon award of the contract.**

All follow-up invoices shall be marked "Duplicate of Original." Contractor questions regarding payment information or check identification should be directed to the ordering agency's designated payment office unless otherwise specified in the task order.

The COR will approve satisfactory completion of all work and services billed.

It is the Contractor's responsibility to set up accountability and oversight to ensure all work was completed satisfactorily. Failure to accurately bill the agency will result in adjustments of amount billed in coordination between the Contractor, Contracting Officer, and COR.

G.3 Contractor Performance Evaluation

Performance assessments under this contract will be administered by the Contracting Officer's Representative (COR) and Contracting Officer (CO) in accordance with agency procedures. Evaluations will be entered into the Contractor Performance Assessment Reporting System (CPARS).

G.4 Contract Closeout

When applicable, it is the intent of the CO to perform contract closeout procedures on the contract. The Contractor agrees to perform any functions necessary to support the process in a timely manner. Contract closeout will occur, as soon as possible, after completion and acceptance of contract performance.

G.5 Terminations

The Government may modify or terminate the contract upon written notice from the CO. Upon termination, the Contractor shall deliver to the Government all documents, invoices and/or

reports, deliverables provided to the Contractor as of the date of the termination. Reference FAR Clause 52.212-4(l) Termination for the Government's Convenience and 52.212-4(m)Termination for Cause.

Section H – Special Contract Requirements

H.1 Key Personnel. Offerors may identify key personnel in their proposal to demonstrate understanding of the requirement and organizational capability.

If the offeror includes key personnel in its proposal, the following applies:

The Government will consider proposed key personnel as part of the technical evaluation under section M. The absence of identified key personnel shall not, in itself, render a proposal unacceptable.

a. Individuals identified as key personnel in the successful offeror's proposal shall be considered committed to the contract upon award.

b. Substitution of key personnel, once contract performance begins, shall require prior written approval of the Contracting Officer. Approval will be granted only when the replacement possesses qualifications equal to or greater than those of the individual originally proposed.

c. The Contractor shall notify the Contracting Officer at least 30 calendar days in advance of any proposed substitution and provide:
    - Resume of proposed replacement
    - Explanation of substitution
    - Impact of performance (if any)

d. The contractor shall not request substitution or replacement of the key personnel within the first ninety (90) days of contract performance. Key personnel shall be added and removed via modification to the contract by the Contracting Officer after the Government provides notification that the key personnel are approved to commence performance of services. All replacement key personnel shall meet the requirements of the contract. The Government shall have three (3) days to review replacement key personnel resumes. All requests for approval of changes hereunder must be in writing, via email, and provide a detailed explanation of circumstances necessitating the proposed change.

H.2 Transition Support

The Contractor shall provide transition support at the beginning and end of contract performance as specified herein and in accordance with the Statement of Work. Transition support is intended to ensure continuity of services and minimize disruption to Government operations.

Transition In Support

The Contractors shall provide a draft Transition-In Plan to the COR via electronic mail within 30 calendar days after the award issuance unless otherwise directed by EOIR. The transition-in plan shall describe how the Contractor will ensure no interruption to case services or statutory timeframes. The Contractor shall account for 10 business days of EOIR review and approval of the final Transition Plan. The transition-in period will begin upon receipt and approval of the Contractor's Transition Plan. See the Statement of Work for more information.

Transition Out Support

The Contractor shall complete the Transition Out process at least 90 calendar days prior to the end of the contract (or as directed by the CO or COR) without service disruption. In accordance with FAR 52.237-3, *Continuity of Services*, the Government reserves the right to require additional transition services for up to 90 days after this contract expires. Transition-out support shall be performed at no additional cost to the Government, unless otherwise specified in the contract.

The Contractor shall remain fully responsible for contract performance during the transition period. Transition activities shall not adversely impact ongoing service delivery. See the Statement of Work for more information.

H.3 Organizational Conflict of Interest (OCI)

The Contractor shall disclose any actual or potential OCI situations prior to award and throughout performance. The Contractor shall not participate in any activity that could impair its objectivity. If any OCI is identified, the Contractor shall recuse involved personnel, physically and informationally separate conflicting work, and ensure no access or use of information advantageous in the performance of this contract. Any unresolved OCI may result in disqualification or corrective action.

H.4 Safeguarding Information: The Contractor shall protect from unauthorized disclosure of any materials, deliverables, invoice and/or reports, and submittals, etc. or any information made available by the Government or that the Contractor has access to by virtue of the provisions of the contract, that are not intended for public disclosure. It is understood that disclosures of any information relating to the work or services outlined in the contract will not be provided to any persons not entitled to receive it. Failure to safeguard any information that may come to the Contractor or any person under the Contractor's control in connection with the work under the

contract may subject the Contractor, the Contractor's agents or employees to criminal liabilities as outlined elsewhere in the contract.

H.5 News Releases*:* The Contractor shall **NOT** release information (e.g., news releases) in connection with the contract unless prior written approval has been received from the CO.

H.6 Contractor Provision of Staff and Resources: The Contractor shall provide the skilled personnel, supervision, management, labor, legal services and any other items necessary to successfully execute the Statement of Work and all other contract requirements. The Contractor shall schedule work hours of all personnel in a manner that will provide maximum compliance with the Government's requirements.

H.7 Employee Standards: The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct and integrity and shall be responsible for taking such disciplinary action with respect to employees as may be necessary.

H.8 Service Contract Labor Standards (SCLS) Applicability: The Government has determined that this requirement is principally for professional legal services and that the provisions of the SCLS statute are not expected to apply to the labor categories anticipated for performance. Offerors shall review the requirements of the SCLS statute and identify in their proposals any labor categories they intend to utilize that may qualify as covered employees. If an offeror proposes the use of covered service employees, the Offeror shall:

Identify the applicable labor categories, provide an explanation of why such employees are required for contract performance, and identify any applicable wage determination believed to apply. Wage Determination: The Contractor(s) shall be expected to utilize the official wage determination received from the Department of Labor (DOL) for the employees who are covered by the Service Contract Act. See FAR 52.222-41 and FAR 52.222-49. The DOL has established a web site to obtain wage determinations by locality and is available online at: https://sam.gov/wage-determinations. The Government reserves the right to review the applicability of SCLS requirements prior to award and incorporate the appropriate clauses and wage determination if required. Upon award of the contract, the CO will request official wage determinations if applicable. The official wage determination will be incorporated into the contract by formal modification. Please submit with the proposal a complete listing of service employees that will be employed under the contract. See FAR 52.222-42, Statement of Equivalent Rates for Federal Employees. A listing of standard occupations in Adobe PDF reader format is available at:
http://www.dol.gov/whd/regs/compliance/wage/SCADirV5/SCADirectVers5.pdf.

H.9 Subcontracting: Offerors that are other than small business concerns shall submit a Subcontracting Plan with their proposal in accordance with FAR 52.219-9, if subcontracting possibilities exist. The plan will be evaluated for acceptability. For awareness, please see the Government’s small business goals.

Small Business Category	*Small Business Participation Goal*
Small	36.0%
Small Disadvantaged Business	5.0%
Women-Owned	5.0%
HUBZone	3.0%
ervice-Disabled Veteran-Owned Small Business	5.0%

H.10 Supervision of Personnel: The Contractor's personnel are employees of the Contractor and under the administrative control and supervision of the Contractor. The Contractor, through its personnel, shall perform the requirements of the contract. The Contractor shall select, supervise, and exercise control and direction over its employees under the contract. The Contractor shall not supervise, direct or control the activities of Government personnel (DOJ).

H.11 No Personal Services: As stated elsewhere, no personal services shall be performed under the contract. The Government will not directly supervise Contractor employees.

H.12 Privity of Contract: The Contractor is the Prime Contractor for the life of the contract and is responsible for all actions of its subcontractors, teaming arrangement, if any. The Contractor shall provide a single point of contact that will function as a primary interface for all contractual matters arising from the contract. The Contractor shall complete a Subcontracting Plan as part of the proposal submission if applicable.

PART II – CONTRACT CLAUSES

Section I – Provisions, Clauses, and Agency Regulations

I.1 FAR 52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)
The 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 the 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

Federal Acquisition Regulation (FAR) Solicitation Provisions

Provision No.	Title	Date
52.203-11	Certification of Disclosure Regarding Payments to Influence Certain Federal Transactions	(Sep 2024)
52.204-7	System for Award Management	(Nov 2025)
52.204-19	Incorporation by Reference of Representations and Certifications	(Dec 2014)
52.215-1	Instructions to Offerors-Competitive Acquisition	(Dec 2025)

52.217-5 Evaluation of Options (Aug 2025)

52.212-2 Evaluation—Commercial Products and Commercial Services (Nov 2025)

(a) Evaluation factors. The Government will award a contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors will be used to evaluate offers:

1. Technical Approach
2. Management Approach
3. Past Performance
4. Price

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

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

(End of provision)

FAR 52.215-6 Place of Performance (Dec 2025)

(a) The offeror or respondent, in the performance of any contract resulting from this request for proposals, □ intends, □ does not intend [check applicable block] to use one or more plants or facilities located at a different address from the address of the offeror or respondent as indicated in this proposal or response to request for information.

(b) If the offeror or respondent checks "intends" in paragraph (a) of this provision, it shall insert in the following spaces the required information:

Place of Performance (Street Address, City, State, County, ZIP Code)

_____

_____

Name and Address of Owner and Operator of the Plant or Facility if Other than Offeror or Respondent

_____

_____

(End of provision)

I.2 FAR Clauses Incorporated 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**.

FAR Clause No.	Title	Date
52.202-1	Definitions	(Jun 2020)
52.203-3	Gratuities	(Apr 1984)
52.203-5	Covenant Against Contingent Fees	(May 2014)
52.203-7	Anti-Kickback Procedures.	(Jun 2020)
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity.	(May 2014)
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	(May 2014)
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	(Jun 2020)
52.203-13	Contractor Code of Business Ethics and Conduct	(Nov 2021)
52.203-16	Preventing Personal Conflicts of Interest	(Jun 2020)
52.204-9	Personal Identity Verification of Contractor Personnel	(Jan 2011)
52.204-13	System for Award Management Maintenance	(Nov 2025)
52.204-14	Service Contract Reporting Requirements	(Nov 2025)
52.204-19	Incorporation by Reference of Representations and Certifications.	(Dec 2014)
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	(Nov 2021)
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	(Nov 2021)
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded.	(Nov 2025)
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters.	(Nov 2025)
52.212-4	Terms and Conditions—Commercial Products and Commercial Services.	(Apr 2026)
52.215-2	Audit and Records – Negotiation	(Dec 2025)
52.215-19	Notification of Ownership Changes	(Dec 2025)
52.216-4	Economic Price Adjustment – Labor and Material	(Jan 2017)
52.219-8	Utilization of Small Business Concerns	(Dec 2025)
52.219-9	Small Business Subcontracting Plan	(Dec 2025)
52.219-16	Liquidated Damages-Subcontracting Plan	(Dec 2025)
52.222-1	Notice to the Government of Labor Disputes	(Dec 2025)
52.222-3	Convict Labor	(Dec 2025)

52.222-4	Contract Work Hours and Safety Standards Act – Overtime Compensation	(Dec 2025)
52.222-49	Service Contract Labor Standards-Place of Performance Unknown	(Dec 2025)
52.222-54	Employment Eligibility Verification	(Dec 2025)
52.222-19	Child Labor-Cooperation with Authorities and Remedies	(Apr 2026)
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	(Dec 2025)
52.222-41	Service Contract Labor Standards	(Dec 2025)
52.222-43	Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts).	(Dec 2025)
52.224-1	Privacy Act Notification	(Apr 1984)
52.224.2	Privacy Act	(Apr 1984)
52.226-7	Drug-Free Workplace	(May 2024)
52.227-1	Authorization and Consent	(Jun 2020)
52.227-14	Rights In Data- General	(May 2014)
52.228-5	Insurance-Work on a Government Installation	(Jan 1997)
52.229-3	Federal State, and Local Taxes	(Aug 2025)
52.232-1	Payments	(Apr 1984)
52.232-8	Discounts for Prompt Payment	(Feb 2002)
52.232-9	Limitation on Withholding of Payment	(Apr 1984)
52.232-11	Extras	(Apr 1984)
52.232-18	Availability of Funds	(Apr 1984)
52.232-23	Assignment of Claims	(May 2014)
52.232-33	Payment by Electronic Funds Transfer-System for Award Management	(Oct 2018)
52.233-1	Disputes	(Dec 2025)
52.232-39	Unenforceability of Unauthorized Obligations	(Jun 2013)
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	(Apr 1984)
52.237-3	Continuity of Services	(Jan 1991)
52.242-5	Payments to Small Business Subcontractors	(Jan 2017)
52.242-15	Stop-Work Order	(Sep 2019)
52.242-17	Government Delay of Work	(Apr 1984)
52.243-1	Changes-Fixed Price	(Jul 2025)
52.244-2	Subcontracts	(Jun 2020)
52.244-6	Subcontracts for Commercial Products and Commercial Services	(Apr 2026)
52.246-25	Limitation of Liability-Services	(Feb 1997)
52.247-5	Familiarization with Conditions	(Apr 1984)
52.249-4	Termination for Convenience of the Government (Services) (Short Form)	(Apr 1984)
52.253-1	Computer Generated Forms	(Nov 2025)

C2. FAR Clauses Incorporated in Full Text

FAR 52.203-17 Contractor Employee Whistleblower Rights (Nov 2023)

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

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

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

(End of clause)

FAR 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (Nov 2025)

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

Inverted domestic corporation means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

Subsidiary means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

(b) If the contractor reorganizes as an inverted domestic corporation or becomes a subsidiary of an inverted domestic corporation at any time during the period of performance of this contract, applicable law may prohibit the Government from paying for Contractor activities performed after the date when it becomes an inverted domestic corporation or subsidiary. The Government may seek any available remedies in the event the Contractor fails to perform in accordance with the terms and conditions of the contract as a result of Government action under this clause.

(c) Exceptions to this prohibition are located at 9.108-3.

(d) In the event the Contractor becomes either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation during contract performance, the Contractor shall give written notice to the Contracting Officer within five business days from the date of the inversion event.

(End of clause)

FAR 52.233-3 Protest after Award (Nov 2025)

(a) Upon receipt of a stop-work order, the Contractor must immediately comply with its

terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the order during the period of work stoppage. After receiving the final decision in the protest, the Contracting Officer must either—

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled either before or after a final decision in the protest, the Contractor must resume work. The Contracting Officer must make an equitable adjustment in the delivery schedule or contract price, or both, and the contract must be modified, in writing, accordingly, if—

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to an adjustment within 30 days after the end of the period of work stoppage; provided, that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer must allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer must allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

(e) The Government's rights to terminate this contract at any time are not affected by action taken under this clause.

(f) If, as the result of the Contractor's intentional or negligent misstatement, misrepresentation, or miscertification, a protest related to this contract is sustained, and the Government pays costs, the Government may require the Contractor to reimburse the Government the amount of such costs. In addition to any other remedy available, and pursuant to the requirements of subpart 32.6, the Government may collect this debt by offsetting the amount against any payment due the Contractor under any contract between the Contractor and the Government.

(End of clause)

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

(a) *Definitions*. As used in this clause—
Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.
Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (*e.g.*, vendor agreements), program participation, or allocation or deployment of an entity's resources.
(b) In connection with the performance of work under this contract, the Contractor agrees as follows:
(1) The Contractor will not engage in any racially discriminatory DEI activities;
(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;
(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;
(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and
(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.
(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).
(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.
(End of clause)

FAR 52.233-4 Applicable Law for Breach of Contract Claim (Nov 2025)

United States law will apply to resolve any claim of breach of this contract.

(End of clause)

FAR 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.

(End of clause)

FAR 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 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days 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 five (5) years.

(End of clause)

C.3 Justice Acquisition Regulation (JAR) Clauses

DOJ-01 Whistleblower Information Distribution (OCT 2021)

Within 30 days of contract award, the contractor and its subcontractors must distribute the "Whistleblower Information for Employees of DOJ Contractors, Subcontractors, Grantees, or Sub-Grantees or Personal Services Contractors" ("Whistleblower Information") document to their employees performing work in support of the products and services delivered under this contract (https://oig.justice.gov/sites/default/files/2020-04/NDAA-brochure.pdf). By agreeing to the terms and conditions of this contract, the prime contractor acknowledges receipt of this requirement, in accordance with 41 U.S.C. § 4712 and FAR 3.906 & 52.203-17 and commits to distribution. Within 45 days of award, the contractor must provide confirmation to the contracting officer verifying that it has distributed the whistleblower information as required.

(End of Clause)

DOJ-02 Contractor Privacy Requirements (JAN 2022)

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984) and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DOJ system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.justice.gov/opcl/doj-systems-records. 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 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. 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 0900.00.015, 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. 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.

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.

vi. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.

vii. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be

required.

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

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

(6) Victim Remediation

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

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

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

b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records containing PII and those covered by the Privacy Act of 1974. These policies include the preservation of all

records created or received regardless of format, mode of transmission, or state of completion.

(2) Records Creation, Ownership, and Disposition

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

b) Except as stated in the Statement of Work 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, 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 project10 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.

(End of Clause)

DOJ-03 Personnel Security Requirements for Contractor Employees (NOV 2021) (Alt.

I) Classified Information – Cleared Contractors

Work performed under this contract will involve any one or more of the following: access to DOJ Information, which may include Controlled Unclassified Information (CUI), i.e., unclassified, sensitive DOJ information, and/or access to DOJ Information Technology (IT) systems, and/or unescorted access to DOJ space or facilities. Contractor employees will occupy Public Trust Positions, unless clause alternates are applied. ___ (*Check if applicable) Access to/safeguarding of classified information will be required. Alternate I sections also apply*

1. General Requirements

(a) (1) All references to "contract(or) personnel" and "contract(or) employee" in this clause means all individuals, without limitation, to include individuals employed by the contractor, team member, subcontractor, consultant, and/or independent contractor, who will have access to information of the Department of Justice (DOJ) or information that is within the custody and control of the DOJ, access to DOJ IT systems, and/or unescorted access to DOJ facilities/space in connection with the performance of this contract. "Employment" as used herein does not create nor imply an employer/employee relationship between the DOJ and contractor employees. (Alt. I) [The following is added to the clause]: (2) Additionally, work performed under this contract will involve access to classified information [National Security Information (NSI)].

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

(Alt. I) [The following is added to the Clause]: (2) All contractor employees requiring access to classified information will be processed by Defense Counterintelligence and Security Agency (DCSA) in accordance with the National Industrial Security Program (NISP). The contractor will not be permitted to commence performance under this contract until a sufficient number of its personnel, as determined by the SPM in consultation with the Contracting Officer's Representative (COR) if one is appointed, have received the requisite NSI Clearance.

(c) Except where specifically noted otherwise, the federal government will be responsible for the cost and conduct of the investigation.

(d) The contractor shall ensure that no contractor employee commences performance prior

to receipt of a written authorization from the contracting officer, COR, or the SPM that performance by the respective contractor employee is authorized.

(e) The data and other information to which the contractor may have access as a result of this contract is the property of, and/or within the custody and control of, the Department, and its disclosure to third parties is governed by various statutes and regulations, the violation of which may subject the discloser to criminal penalties.

2. Citizenship and Residency Requirements

(a) *Residency Requirement.* (1) Contractor employees in Public Trust positions, both U.S. citizens and non-U.S. citizens, must meet the Department's residency requirement if they will require access to DOJ information, IT systems, or unescorted access to facilities. For three years (not necessarily consecutive years) out of the last five years immediately prior to employment under the Department contract the contractor employee must have: (i) resided in the U.S.; (ii) worked for the U.S. in a foreign country as either an employee or contractor in a federal civilian or military capacity; or, (iii) been a dependent of a federal civilian or military employee or contractor working for the U.S. in a foreign country. At the Department's sole discretion, the residency requirement may be waived by the Department Security Officer (DSO) for contractor employees on a case-by-case basis where justified by extenuating circumstances. The residency requirement does not apply to contractor employees residing in foreign countries that are hired to work in American embassies/consulates/missions located outside of the United States and who require access to DOJ information, IT systems, or unescorted access provided that an adequate background investigation can be conducted, with favorable adjudication, as determined by the DSO.

(Alt. I) [The following is added to the clause]: (2) The residency requirement does not apply to contractor employees working on the classified portion of this contract whose national security clearance has been processed by DCSA in accordance with the NISP.

(b) *Citizenship.* (1) Aside from the specific exceptions set forth in Section 1.2(b)(2), for Public Trust positions, the DOJ requires that contractor employees be U.S. citizens and nationals, or lawful permanent residents seeking U.S. citizenship. Any prospective non-U.S. citizen contractor employee who requires access to DOJ information systems, DOJ information, and/or unescorted facilities access must also have been granted a waiver as described below in paragraphs 1.2(d) and/or (e). The contractor is responsible for verifying that the non-U.S. citizens working under this contract are lawful permanent residents seeking U.S. citizenship.

(2) *Exception for Certain Non-U.S. Citizen Contractor Employees:* (i) Non-U.S. citizen expert witnesses, litigative consultants, and interpreters in rare foreign languages are not

required to be lawful permanent residents seeking U.S. citizenship. However, they must be granted a waiver for access to unclassified DOJ information, whether CUI or not, DOJ IT systems, and/or unescorted facility access, as described below in paragraph 1.2(d) and (e), regardless of the duration of their duties. (ii) Non-U.S. Citizen contractor employees residing in foreign countries who are hired to work for the Department of Justice in American embassies/consulates/missions outside of the United States are not required to be lawful permanent residents seeking U.S. citizenship.

(Alt. I) [The following is added to the Clause]: (3) Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.

(c) *Dual Citizenship.* (1) U.S. citizens who hold dual citizenship with a foreign country are considered U.S. citizens within the meaning of this clause, and may be considered for, but are not entitled to, contract employment as U.S. citizens consistent with this clause. The means by which the contractor employee obtained or exercises his or her dual citizenship status will be a consideration in the Public Trust Investigation (PTI) adjudication, and/or waiver approval processes discussed in this clause.

(Alt. I) [The following is added to the clause]: (2) Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.

(d) *Access to DOJ Information Technology Systems*. Non-U.S citizens are not authorized to access DOJ information technology (IT) systems or assist in the development, operation, management, or maintenance of DOJ IT systems, including providing IT system support, unless a waiver has been granted by the Head of the DOJ component or designee, with the prior concurrence of both the DSO and the DOJ Chief Information Officer, allowing computer access by the non-U.S. citizen. Such a waiver will be granted only in exceptional and unique circumstances on a case-by-case basis. It should be noted that the Justice Consolidated Office Network (JCON) is a sensitive DOJ IT system and any contractor employee who will need access to JCON must be a U.S. citizen or have received a waiver. In order for a waiver to be considered for approval: (1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; (2) The type of personnel security vetting that has been conducted on the individual, and vetting results, that would mitigate risk; and (3) The waiver must be in the best interest of the federal government.

(e) *Access to Unclassified DOJ Information and Unescorted Access to DOJ Facilities or Space.* (1) Except as provided under 1.2(b)(2), non-U.S. citizens are not authorized to access DOJ information and/or unescorted access to DOJ facilities or space, unless a waiver has been granted by the DSO, allowing access by the non-U.S. citizen. Such a waiver will be granted on a case-by-case basis where justified at the discretion of the DSO.

3. Background Investigation Requirements

(a) (1) Unless otherwise stated below, all contractor personnel are subject to a Public Trust Investigation (PTI). The SPM will determine the type of investigation for each contractor employee based on the risk category (i.e., the nature of the position and degree of harm that could be caused by the individual in that position) and whether the position is long-term or short-term. The PTI risk categories are listed below.

(i) High Risk Positions. The minimum background investigation required is a Tier 4 (T4) investigation, and the five-year reinvestigation required is a Tier 4R (T4R) investigation. The 2017 version of the Standard Form (SF) 85P, Questionnaire for Public Trust Positions, is required.

(ii) Moderate Risk Positions. The minimum background investigation required is a Tier 2 (T2) investigation. The five-year reinvestigation required is a Tier 2R (T2R) investigation. The 2017 version of the SF-85P is required.

(iii) Low Risk/Non-Sensitive Positions. The minimum background investigation required for Low Risk/Non-Sensitive positions is a Tier 1 (T1) investigation and the required five-year reinvestigation is also a Tier 1 (T1) investigation. The SF 85, Questionnaire for Non-Sensitive Positions, is required.

(Alt. I) [The following is added to the clause]: (2). Contractor employees requiring access to classified information will be processed by DCSA in accordance with the NISP.

(b) *Exception for Expert Witnesses*. Expert Witnesses, litigative consultants, and interpreters in rare foreign languages may not be subject to full background investigation requirements if alternative security requirements are approved by the DSO.

(c) *Short-Term U.S. Citizen Contractor Employees*. Other than the exception in Section 1.3(b), short-term contractor employees (6 months or less) who are U.S. citizens are not subject to a full background investigation, however, must receive an approved pre employment background investigation waiver. The required forms to complete and submit are listed in Section 1.4(b) and (c)(2).

(d) *Long-Term U.S. Citizen Contractor Employees.* Other than the exception in Section 1.3(b), all long-term U.S. citizen employees (longer than 6 months) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(e) *Non-U.S. Citizen Contractor Employees.* Other than the exception in 1.3(b), all non U.S. citizen contractor employees regardless of performance duration (short or long term) are subject to a full background investigation in the risk category appropriate to the position they will hold.

(f) *Reciprocity*. (1) A Public Trust Investigation will be accepted under reciprocity if it meets the following guidelines: (i) the investigation is current (investigations are considered current if completed within the last five years) and favorably adjudicated, or the reinvestigation has been deferred; (ii) the investigation meets or exceeds the level of investigation required for the DOJ contractual instrument; (iii) there has been no continuous (not cumulative) break in federal contract/service employment of two years or more; (iv) there is no derogatory information since the favorable fitness determination or adjudication that calls into question the individual's fitness based on character or conduct; and (v) the investigative record does not show conduct that is incompatible with the core duties of the new contract position. A "core duty" is a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. Core duties will vary from position to position.

(Alt. I) [The following is added to the clause]: (g) National security investigations will be accepted from other federal agencies under reciprocity guidelines provided all of the following are true: (i) The new position does not require a higher eligibility than what the subject currently possesses; (ii) the existing eligibility is not granted on an interim or temporary basis, or limited or one-time basis; (iii) the covered individual's eligibility is not currently denied, revoked, or suspended; (iv) the favorable adjudication was based on the 13 Adjudicative Guidelines (SEAD 4) and E.O. 12968. Agencies may accept eligibility recorded with an exception based on their own risk assessment; (v) the most recent background investigation is not more than seven years old; (vi) there is no new derogatory information of national security adjudicative relevance that has been reported/developed since last investigation; (vii) the Bond Amendment disqualifier (SEAD 4) does not apply and individual requires SCI, SAP, or restricted access; and (viii) the subject does not have a break in federal service of 24 months or longer.

4. Background Investigation Process

(a) e-QIP (or its successor). Public Trust background investigations/reinvestigations of contractor employees will be performed by the DCSA. The investigative process requires contractor employees to complete the Electronic Questionnaires for Investigations Processing (e-QIP) and provide additional information as specified in paragraph 1.4(b) below. Immediately after contract award, the contractor shall designate an employee as its "e-QIP Initiator" and provide the name of this person to the SPM. The e-QIP Initiator must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being given access to e-QIP. After the e-QIP Initiator's security approval is granted, the Contractor will be configured in e-QIP as a sub-agency to DOJ. The contractor will then be responsible for initiating investigations for all contract personnel,

whose previous investigation does not meet reciprocity, in e-QIP for completion of the security questionnaire form and forwarding the electronic form with the remainder of the security package to the SPM. Subject to the prior written approval of the SPM, the contractor may designate an e-QIP Initiator for each subcontractor. Subcontractor e-QIP Initiators must have, at a minimum, a favorably adjudicated Tier 1 investigation and the appropriate DOJ security approval before being provided access to e-QIP.

(b) *Additional Documentation*. (1) In addition to completing the e-QIP questionnaire (see 1.4(a), above), the contractor shall ensure that each contractor employee occupying Public Trust Positions, including short-term employees, completes and submits the following information through the contractor's Corporate Security Officer:

(i) Digital Fingerprinting/FD-258 Applicant Fingerprint Card. Two sets are required per applicant. The contractor may schedule appointments with the SPM to be digitally fingerprinted; otherwise, fingerprinting by the FBI or other law enforcement entity, as approved by the SPM, is required to ensure the identity of the person being fingerprinted and for printing quality. All pertinent information must be completed by the individual taking the fingerprints (FBI or other). Use of the physical FD-258 Applicant Fingerprint Card should only be used in extenuating circumstances.

(ii) DOJ-555 Fair Credit Reporting Act Disclosure. Authorizes DOJ to obtain one or more consumer/credit reports on the individual. This form will be required if the Component SPM determines a credit check is necessary for its Low Risk Level 1 contractor positions.

(iii) OF-306, Declaration for Federal Employment.

(iv) Foreign National Relatives or Associates Statement. This is only required if foreign national relatives or associates were not disclosed on the security questionnaire form.

(v) Self-Reporting Requirements for All Contractor Personnel. This is an acknowledgement and acceptance statement that every contractor must sign.

(vi) Additional information as may be required based on the review of the security questionnaire form.

The contractor shall review all forms/documents to ensure each is complete, accurate and meets all DOJ requirements, including applicable residency and citizenship requirements. The contractor shall resolve any issues or discrepancies with the contractor employee, including resubmission of corrected forms or documentation. Completed forms/documents shall be submitted to the SPM (or designee, which may include the COR) within five (5) calendar days after being finalized.

(c) Adjudication and Pre-Employment Background Investigation Waivers

(1) Except as set forth in this section, background investigations must be conducted and favorably adjudicated for each contractor employee prior to commencing their work on this contract. Where programmatic needs do not permit the federal government to wait for completion of the entire background investigation, a pre-employment background investigation waiver for public trust contractors can be granted by the SPM, in consultation with the cognizant COR. Pre-employment waivers cannot be used to circumvent delays in clearing classified contractors through the DCSA, if access to classified information is required.

(2) As directed by the SPM, the contractor shall initiate pre-employment waivers for Public Trust Positions when necessary. This may entail performing credit history checks and submission of these checks as part of the security package, including satisfactory resolution of any issues prior to submission to the federal government. A waiver will be disapproved if it develops derogatory information that cannot be resolved in the contractor employee's favor. When a waiver has been disapproved, the CO, in consultation with the SPM and COR, will determine (i) whether the contractor employee will no longer be considered for work on a DOJ contract or (ii) whether to wait for the completion and favorable adjudication of the background investigation before the contractor employee commences work on a Department contract. The pre-employment background investigation waiver requirements include:

1. Verification of citizenship (copy of a birth certificate, naturalization certificate, or U.S. passport);

2. Verification of compliance with the DOJ Residency Requirement of this Clause;

3. Favorable review of the security questionnaire form;

4. Favorable FBI fingerprint results;

5. Favorable credit report;

6. Favorable review of the OF-306 form, Declaration for Federal Employment;

7. Verification of the initiation of the appropriate background investigation (for long-term personnel); and

8. Receipt of the signed DOJ Self-Reporting Requirements for All Contractor Personnel (see Section 6, below).

(3) The investigating agency (DCSA) will provide the SPM with the results of each proposed contractor employee's Public Trust investigation. Upon receipt of the investigation and any other pertinent documents from the investigating agency, the SPM will determine whether each proposed contractor employee should be granted employment

security approval.

(4) The COR will notify the contractor of the results of Public Trust background investigations as they are completed and adjudicated, including any individual who is found ineligible for employment security approval. For any individual found ineligible for employment on a Department contract, the contractor shall propose a replacement and initiate the background investigation process consistent with this clause.

(Alt. I) [The following is added to the clause]:

(5) (1) For classified contracts, the contractor shall possess or be capable of obtaining a Department of Defense Central Adjudication Facility (DODCAF) Defense Industrial Security Clearance Facility Cage Code and the security clearance required to fully perform this contract. As directed by the COR or SPM, the contractor shall submit the information necessary to allow the Government to prepare and obtain for the Contractor a "Department of Defense Contract Security Classification Specification" (DD Form 254) for this contract. Where such clearance is required, the contractor agrees to provide information and access to contractor facilities as may be required by federal government investigators.

(2) Immediately after contract award (or post-award receipt of the required Facility Clearance), the contractor's Facility Security Officer (FSO) shall furnish to the COR a list of all personnel proposed to work under this contract who have been processed in accordance with the NISP by the DCSA. The contractor shall update this information as individuals are added or separated from the contract and the FSO shall provide the updated list to the COR.

(3) For each contractor employee who requires access to classified information under this contract, the contractor shall forward a Visit Authorization Request (VAR) indicating the current background investigation information and clearance level to the COR.

5. <u>Identity Proofing and Badging</u>

(a) Access to DOJ Information, federally-controlled IT systems, and/or unescorted access to federally-controlled facilities or space (regardless of whether the contractor employee will be issued a DOJ PIV card or building access badge) shall be made available after each respective contractor employee has (1) met the identity proofing requirements outlined below, and (2) completed all other security requirements stated elsewhere in this contract.

(b) (1) Public Trust contractor employees must appear in person at least once before a DOJ official or an official of a trusted contract company (i.e., has a facility security clearance) who is responsible for checking two forms of identification in original form prior to commencement of work by the contractor employee and PIV card or building access badge issuance (as applicable). Approval will be documented by the DOJ official or an official of

a trusted contract company. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID).

(c) (Alt. I) [The following is added to the clause]: (2) All contractor employees requiring access to classified information must appear in person at least once before an official of the contractor possessing the facility clearance, who is responsible for checking the identification documents. (Acceptable documents are listed in Form I 9, Employment Eligibility Verification, and at least one document must be a valid state or federal government issued picture ID). This identity proofing must be completed prior to commencement of work by the contractor employee under this contract and badge issuance (as applicable) and must be documented by the contractor official.

(d) All contractor employees requiring unescorted access to a DOJ controlled facility or space shall comply with the PIV card or building access badge requirements outlined below:

(i) When any contractor employee enters a DOJ building for the first time, he/she shall allow one hour for security processing and the creation and issuance of a building access badge. PIV cards require additional processing time and will not likely be issued on the same day.

(ii) Building access badges shall be subject to periodic review by the contractor employee's supervisor and checked against his/her personal identification. The contractor employees shall present themselves for the issuance of renewed badges when required by the government as scheduled by the COR or his/her designee. The contractor shall notify the COR when contractor employee badges are lost, and must immediately apply for reissuance of a replacement badge. The contractor shall pay for reissued building access badges at no cost to the government. It is the contractor employee's responsibility to return badges to the COR or his/her designee when a contractor employee is dismissed, terminated or assigned to duties not within the scope of this contract.

6. Employee Reporting Requirements

(a) All contractor employees must sign the DOJ Self-Reporting Requirements for All Contractor Personnel statement acknowledging and accepting the DOJ requirement that they immediately self-report certain information using the Department’s iReport system. The COR or SPM will provide the Self-Reporting statement as well as a list of reportable information, which varies by position sensitivity designation, to the contractor employee before commencing work under the contract. If the contractor employee does not have access to the DOJ iReport System, the COR or SPM will provide a fillable form for the

contractor employee to complete and submit.

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

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

7. Replacement Personnel

(a) The contractor shall make every effort to avoid costs to the government for security investigations for replacement of contractor employees, and in so doing shall ensure that otherwise satisfactorily performing and physically able contractor employees remain in contract performance for the duration of the contract. The contractor shall take all necessary steps to ensure that contractor personnel who are selected for assignment to this contract are professionally qualified and personally reliable, of reputable background and sound character, and able to meet all other requirements stipulated in the contract.

(b) The fact that the government performs security investigations shall not in any manner relieve the contractor of its responsibility to ensure that all contract personnel are reliable and of reputable background and sound character. Should a security investigation conducted by the government and/or a contractor's self-report or failure to self-report render ineligible a contractor employee, the contracting officer will determine whether the contractor has violated this clause. The contracting officer may direct the contractor, at its own expense, to remove and replace any contractor personnel who fails to comply with or violates applicable requirements of this contract. Such action may be taken at the government's direction without prejudice to its rights under any other provision of this contract, including termination for default, and the contractor may be held liable, at a minimum, for all reasonable and necessary costs incurred by the government to (i) provide coverage (performance) through assignment of individuals employed by the government or third parties in those cases where absence of contractor personnel would cause either a security threat or DOJ program disruption and (ii) conduct security investigations in excess of those which would otherwise be required.

(c) Nothing in this clause shall require the contractor to bear costs involved in the conduct of security investigations for replacement of a contractor employee who separates from the contractor of his/her own accord, is incapacitated, or is deceased. (d) The contractor shall comply with the terms and conditions set forth under this clause and assumes all liability for failure to comply. The rights and remedies conferred upon the government by this clause are in addition to all and other rights and remedies pursuant to the contract and as established by law.

(End of Clause)

DOJ-05 Security of Department Information and Systems (OCT 2023)

I. Applicability to Contractors and Subcontractors

Section 2839.102 of the Justice Acquisition Regulation (JAR), (48 C.F.R. § 2839.102), applies to this contract. Accordingly, all contractors are obligated to comply with all applicable DOJ security policies, directives, or guidance documents, including the security requirements in the provisions in this contract clause. This contract clause applies to all contractors and subcontractors, including cloud service providers ("CSPs"), and personnel of the contractors and subcontractors (hereinafter collectively, "Contractor") that may access, collect, store, process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information. The security requirements set forth herein are in addition to those required by the Federal Acquisition Regulation ("FAR"), and any other applicable laws, mandates, contract clauses, DOJ policies, directives or guidance documents and Executive Orders pertaining to the development and operation of Information Systems and/or the protection of Government Information. This clause does not alter or diminish any existing rights, obligations, or liability under any other civil and/or criminal law, rule, regulation, or mandate.

II. General Definitions

The following general definitions apply to this clause. Specific definitions also apply as set forth in other paragraphs.

A. Authorization to Operate ("ATO"), as defined in National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-37 Revision 2, is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.

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

C. Covered Contract is any contract, order or other agreement under which the contractor, or a subcontractor at any tier, including a cloud service provider, may access, collect, store,

process, maintain, use, share, retrieve, disseminate, transmit, or dispose of DOJ Information (as defined below) in the course of providing a product or service to the Department, with the exception of acquisitions under the micro-purchase threshold.

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

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

F. DOJ Information, as defined in DOJ Order 0904, means any Information that is owned, produced, controlled, protected by, or otherwise within the custody or responsibility of the DOJ, including, without limitation, information related to DOJ programs or personnel. It includes, without limitation, Information (1) provided by or generated for the DOJ, (2) managed or acquired by the Contractor for the DOJ in connection with the performance of the contract, and/or (3) acquired to perform the contract.

G. Information, as defined in DOJ Order 0904, is any communication or representation of knowledge such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audiovisual. This includes any communication or representation of knowledge in an electronic format that allows it to be stored, retrieved, or transmitted.

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

I. Personally Identifiable Information ("PII"), as defined in the FAR 24.101, means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. It includes but is not limited to common data elements such as names, addresses, dates of birth, and places of employment, to identity documents, Social Security numbers or other government-issued identifiers, precise location information, medical history, and biometric records. This definition covers all PII that is created by or becomes available to the contractor, including its employees, subcontractors, or affiliates, as a result of performing under this contract. PII, as supplementally defined in DOJ Order 0904, also includes information about an individual maintained by an agency, including, but not limited to,

information related to education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity.

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

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

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

b. Confirmed Security Breach (hereinafter, "Confirmed Breach") means any confirmed security breach (as defined above).

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

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

b. Confirmed Security Incident means any confirmed security incident (as defined above).

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

III. Confidentiality and Non-Disclosure of DOJ Information

A. Preliminary and final contract deliverables and all associated working papers and

material generated by the Contractor developed using DOJ Information, product, source code, and/or methods of operations, are the property of the U.S. Government and must be submitted to the Contracting Officer ("CO") or the CO's Representative ("COR") at the conclusion of the contract. The U.S. Government has unlimited data rights to all such deliverables and associated working papers and materials in accordance with FAR 52.227-14 (Rights in Data-General). The Contractor will define a method of monitoring the development activity to include any activity associated with DOJ Information, product, source code, and methods of operations. The data rights and development details shall be defined within the Contract.

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

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

C. Any DOJ Information made available to the Contractor under this contract shall be used only for the purpose of performance of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this contract. In performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of all DOJ Information processed, stored, or transmitted by the Contractor. The Contractor shall comply with information security responsibilities and duties throughout the contract and after expiration/termination as appropriate per contract close-out activities. When requested by the CO (typically no more than annually), the Contractor shall provide a report to the CO identifying, to the best of the Contractor's knowledge and belief, the type, amount, and level of sensitivity of the DOJ Information processed, stored, or transmitted under the Contract, including an estimate of the number of individuals for whom PII has been processed, stored or transmitted under the Contract and whether such information includes social security numbers (in whole or in part).

IV. Compliance with Information Technology Security Policies, Procedures and Requirements

A. For all Covered Information Systems, in addition to any other applicable requirements, as set forth in Part I, the Contractor shall comply with the security requirements of the

Federal Information Security Modernization Act of 2014 ("FISMA"), Privacy Act of 1974, E-Government Act of 2002, National Institute of Standards and Technology ("NIST") Special Publications ("SP"), including NIST SP 800-37, 800-53, and 800-60 Volumes I and II, Federal Information Processing Standards ("FIPS") Publications 140-2, 199, and 200, Federal Risk and Authorization Management Program ("FedRAMP"), DOJ IT Security Standards as amended, and OMB Memoranda relating to the security of information and/or Federal Information Systems.

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

1. Limiting access to DOJ Information and Covered Information Systems to authorized users and to transactions and functions that authorized users are permitted to exercise.

U.S. Department of Justice Departmental Provisions and Clauses

2. Providing security awareness training at least annually to all Contractor employees and contractors involved with the Covered Contract. Such training shall include, but not be limited to, recognizing and reporting potential indicators of insider threats to users and managers of DOJ Information and Covered Information Systems.

3. Creating, protecting, and retaining, in accordance with applicable requirements but in any event at least until the expiration of the contract, Covered Information System audit records, reports, and supporting documentation to enable reviewing, monitoring, analysis, investigation, reconstruction, and reporting of unlawful, unauthorized, or inappropriate activity related to such Covered Information Systems and/or DOJ Information.

4. Maintaining authorizations to operate any Covered Information System.

5. Performing continuous monitoring on all Covered Information Systems, to include but not be limited to, collecting, reviewing, and analyzing appropriate logs and timely investigating security alerts and potential security incidents.

6. Establishing and maintaining baseline configurations and current inventories of Covered Information Systems, including hardware, software, firmware, and documentation, throughout the Information System Development Lifecycle, and establishing and enforcing security configuration settings for IT products employed in Covered Information Systems.

7. Ensuring appropriate contingency planning has been performed, including DOJ

Information and Covered Information System backups.

8. Identifying Covered Information System users, processes acting on behalf of users, or devices, and authenticating and verifying the identities of such users, processes, or devices, using multifactor authentication or HSPD-12 compliant authentication methods as defined by NIST 800-63-3, Digital Identity Guidelines or current revision.

9. Establishing and maintaining an operational incident handling capability for Covered Information Systems that includes adequate and timely development, logging, detection, analysis, containment, recovery, and user response activities, and tracking, documenting, and timely reporting incidents to appropriate officials and authorities within the Contractor's organization and the DOJ.

10. Performing periodic and timely maintenance on Covered Information Systems, and providing effective controls on tools, techniques, mechanisms, and personnel used to conduct such maintenance.

11. Protecting Covered Information System media containing DOJ Information, including paper, digital and electronic media, and DOJ assets under Contractor control; protecting them from environmental impacts, access, and equipment positioning requirements defined; limiting access to DOJ Information to authorized users; and sanitizing or destroying Covered Information System media containing DOJ Information before disposal, release or reuse of such media.

12. Limiting physical access to Covered Information Systems, equipment, and physical facilities housing such Covered Information Systems to authorized personnel according to DOJ 03.

13. Screening individuals prior to authorizing access to Covered Information Systems to ensure compliance with DOJ Security standards including personnel background checks.

14. Continuously assessing the risk to DOJ Information in Covered Information Systems, including scanning and remediating vulnerabilities, or implementing appropriate mitigation in accordance with DOJ policy, and ensuring the timely removal of assets no longer supported by the Contractor.

15. Continuously monitoring the application of security controls of Covered Information Systems, assessing the efficacy of such controls, and developing and implementing plans of action designed to correct deficiencies and eliminate or reduce vulnerabilities in such Covered Information Systems.

16. Monitoring, controlling, and protecting information transmitted or received by Covered Information Systems at the external boundaries and key internal boundaries of such Covered Information Systems, and employing architectural designs, software development

techniques, and systems engineering principles that promote effective security.

17. Identifying, reporting, and correcting Covered Information System security flaws in a timely manner, providing protection from malicious code at appropriate locations, monitoring security alerts and advisories and taking appropriate and timely action in response.

18. Ensuring return of Government Furnished Equipment ("GFE") and/or PIV card assets within 10 business days of notification for end of use (contract end, staff change, etc.).

19. Complying with rights in data (FAR 52.227-14) as to the development, management, and protection of DOJ Information.

20. Reporting on risks or known issues impacting DOJ Services (staffing, hardware, process, changes, etc.) through the Contractor's CO or COR, DOJ Service Owner ("SO"), and Government Technical Manager ("GTM") including risk mitigation activities.

21. Reporting through the Contractor's CO or COR on any projected or planned changes in corporate ownership, covered information system design, and/or any technical changes that could impact the confidentiality, integrity or availability of DOJ Information, data, or systems. Changes to system design must be updated through the authorization process per NIST SP 800-37 Revision 2, Step 6 ('Continuous Monitoring") or current NIST revision.

22. When, as part of operating within the DOJ environment, the Contractor's covered information system is subject to review, audit, or assessment by third parties, facilitating DOJ access to information system resources, facilities, personnel, and documentation in a timely manner as required by the auditors. Should a third-party organization conduct a review of any Covered Information System, the Contractor must provide a copy of the report to DOJ, through the CO and COR.

23. Completing an attestation that meets OMB Memorandum M-22-18 for software procurements following the template attestation form developed by NIST. The attestation form must be returned to the CO and COR for sharing with the component Chief Information Officer (CIO).

24. Reporting on outages impacting DOJ Services through the Contractor's CO, COR, and DOJ Service Owner (SO) to include event and mitigation details.

C. The Contractor shall not process, store, or transmit DOJ Information using a Covered Information System without first obtaining an ATO for each Covered Information System. The ATO shall be signed by the Authorizing Official for the DOJ component responsible for maintaining the security, confidentiality, integrity, and availability of the DOJ Information under this contract. (For Cloud Computing Systems, see Section V, below.)

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

E. When requested by the DOJ CO or COR as described below, the Contractor shall provide DOJ, including the Office of Inspector General ("OIG") and Federal law enforcement components, (1) access to any and all information and records, including electronic information, regarding a Covered Information System, and (2) physical access to the Contractor's facilities, installations, systems, operations, documents, records, and databases. Such access may include independent validation testing of controls, system penetration testing, and FISMA data reviews by DOJ or agents acting on behalf of DOJ, and such access shall be provided within 72 hours of the request. Additionally, the Contractor shall cooperate with DOJ's efforts to ensure, maintain, and safeguard the security, confidentiality, integrity, and availability of DOJ Information.

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

1. Media must be encrypted using a NIST FIPS 140-2 approved product.

2. The Contractor must develop and implement a process to ensure that security and other applications software is kept up to date.

3. Where applicable, media must utilize antivirus software and a host-based firewall mechanism.

4. The Contractor must log all computer-readable data extracts from databases holding DOJ Information and verify that each extract including such data has been erased within 90 days of extraction or that its use is still required. All DOJ Information should be treated by the Contractor as sensitive information unless specifically designated as non-sensitive by the DOJ.

5. A Rules of Behavior (ROB) form must be signed and acknowledged annually by users. These rules must address, at a minimum, authorized, and official use, prohibition against unauthorized users and use, and the protection of DOJ Information. The form also must notify the users that they have no reasonable expectation of privacy regarding any communications transmitted through or data stored on Contractor-owned laptops or other

portable digital or electronic media.

6. Cybersecurity Awareness Training (CSAT) shall be provided annually by Contractor for all users of Covered Information System. This training must be submitted to, and approved by, the CO or COR in advance of being provided to users. Users must complete and acknowledge having received CSAT each year. At a minimum, CSAT provided by contractors must include:

a. Insider Threat Detection and Reporting – Importance of detecting, methodologies, indicators, and reporting

b. Privacy Awareness – Privacy Act and PII

c. General Cybersecurity – Information security, trends in advance persistent threats, social engineering/phishing, appropriate use, mobile devices, remote access, basic security best practices

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

H. When no longer needed, all media must be processed (sanitized, degaussed, or destroyed) in accordance with NIST SP 900-88, Guidelines for Media Sanitization.

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

J. The Contractor must remove all DOJ Information from Contractor media and return all such information to the DOJ within 10 days of the expiration or termination of the contract, unless otherwise extended by the CO, or waived (in part or whole) by the CO, and all such information shall be returned in a format and form acceptable to DOJ. The Contractor shall provide a written certification certifying the removal and return of all such information to the CO within 10 business days of the removal and return of all DOJ Information.

K. DOJ, at its discretion, may suspend the Contractor's access to any DOJ Information, or terminate the contract, when DOJ suspects that the Contractor has failed to comply with any security requirement, or in the event of an Information System Security Incident or Security Breach (see definitions above), where the Department determines that either event gives cause for such action. The suspension of access to DOJ Information may last until such time as DOJ, in its sole discretion, determines that the situation giving rise to such action has been corrected or no longer exists. Any termination action taken because of the Contractor's suspected failure to comply with any security requirement will be conducted in accordance with the applicable termination clause governing the awarded contract. The Contractor understands that any suspension or termination in accordance with this provision shall be at

no cost to DOJ, and that upon request by the CO, the Contractor must immediately return all DOJ Information to DOJ, as well as any media upon which DOJ Information resides, at the Contractor's expense. The Contractor must comply with FAR 52.227-14 (Rights in Data), FAR 52.245-1 (Government Property), DOJ 2400.3A Chapter 1 (component property procedures), and FAR 4.804-5(a)(6) (Procedures for closing out contract files).

V. Cloud Computing

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

1. All of the following has occurred: (a) the Cloud system and CSP have been evaluated by a Third Party Assessing Organization ("3PAO") certified under FedRAMP; (b) the Cloud system received FedRAMP authorization; (c) the Contractor has provided the most current System Security Plan ("SSP") and Security Assessment Report ("SAR") to the DOJ CO for consideration, and provides any subsequent SSPs and SARs within 30 days of issuance; and, (d) the Authorizing Official for the DOJ component responsible for maintaining the security confidentiality, integrity, and availability of the DOJ Information under the Covered Contract has issued an ATO; or,

2. In cases where the CSP or its offering is not FedRAMP authorized, the COR approves utilization of the Cloud System after the CSP has worked with the authorizing official, the DOJ OCIO, and the FedRAMP Program Management Office to determine that the CSP is likely to seek and receive Agency/FedRAMP authorization within 1 year, or DOJ has authorized use as a Private Cloud or Contractor Owned, Contractor Operated system.

B. The Contractor must ensure that the CSP allows DOJ to access and retrieve any DOJ Information processed, stored, or transmitted in a Cloud system under this Contract within a reasonable time of any such request, but in no event less than 48 hours from the request. To ensure that the DOJ can fully and appropriately search and retrieve DOJ Information from the Cloud system, access shall include any schemas, meta-data, and other associated data artifacts.

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

D. The Contractor must ensure that the CSP provides evidence of annual recertification of

privileged user access management.

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

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

1. The Contractor shall develop and deliver a SCRM Plan. The SCRM Plan shall meet the format described in NIST SP 800-161, Appendix E. The SCRM plan shall address the following security controls from NIST SP 800-53 Rev 5: SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-10, and SR-11. Equivalent ISO 27000 series controls may be used if they are mapped to the NIST control(s).

2. The Contractor shall implement the required security controls as documented in the SCRM Plan. The requirements of the SCRM plan shall flow down to all subcontractors. Evidence of the certification and compliance is required.

3. The Contractor shall provide evidence of compliance with the documented SCRM Plan. (CO select which applies)

_____ Self-assessment by a contractor security team

_____ External assessment by an independent auditor

VI. Information System Security Incident or Security

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

B. Potential Security Incident.

1. If the Contractor suspects that DOJ information has been potentially disclosed or impacted, the Contractor shall promptly investigate to determine if a Security Incident has occurred. If the Contractor has not determined within 24 hours (i.e., 24 hours from detection of potential security incident and/or security breach) whether the Potential Security Incident was in fact a Security Incident, then it must immediately report the Potential Security Incident to the DOJ CO and the COR. If the time by which to report the Potential Security Incident occurs outside of regular business hours and/or neither the DOJ CO nor the COR can be reached, the Contractor must call or e-mail the JSOC Team at 1-202-357-7000 or JSOC@USDOJ.GOV and contact the DOJ CO and COR as soon as practicable. If the contract involves PII, the Contractor must comply with the notification requirements of DOJ-02 and Executive Order M-17-12 (Memorandum on Preparing for and Responding to a Breach of Personally Identifiable Information), Contractor Privacy Requirements, Section B.5, for an actual or suspected Security Incident.

2. The Contractor must limit sharing of Security Incident details to only those individuals involved in responding to the potential Security Incident. Any provisions of the Covered Contract regarding the citizenship or location of individuals working on the Covered Contract apply equally to individuals involved in responding to any potential Security Incidents. The Contractor may request assistance from the JSOC for advice, incident response, or FBI coordination. The Contractor must provide weekly updates to CO, COR and JSOC during the course of a Security Incident investigation.

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

1. Both the Covered Information Systems and DOJ Information involved or at risk, including the type, amount, and level of sensitivity of the DOJ Information and, if the DOJ Information contains PII, the estimated number of unique instances of PII.

2. All steps and processes being undertaken by the Contractor to minimize, remedy, and/or investigate the Security Incident.

3. Any and all other information as required by the CISA Federal Incident Notification Guidelines, including the functional impact, information impact, impact to recoverability, threat vector, mitigation details, and all available incident details; and

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

D. Except as otherwise required by Federal, State and local laws, executive orders, rules and regulations, all determinations regarding whether and when to notify other individuals

and/or federal agencies potentially affected by a Security Incident will be made by DOJ senior officials, the DOJ Core Management Team, or the COR at DOJ's discretion.

E. The Contractor must provide to DOJ full access to any facility and/or Covered Information System affected or potentially affected by any potential or confirmed Security Incident, including access by the DOJ OIG and federal law enforcement organizations, and undertake any and all response actions DOJ determines are required to ensure the protection of DOJ Information, including providing all requested images, log files, and event information to facilitate rapid resolution of any Security Incident.

F. DOJ, at its sole discretion, may obtain, and the Contractor will permit, the assistance of other federal agencies and/or third-party contractors or firms to aid in response activities related to any potential or confirmed Security Incident. Additionally, DOJ, at its sole discretion, may require the Contractor to retain, at the Contractor's expense, a 3PAO acceptable to DOJ, with expertise in incident response, compromise assessment, and federal security control requirements, to conduct a thorough vulnerability and security assessment of all affected Covered Information Systems.

G. Response activities related to any Security Incident undertaken by DOJ, including activities undertaken by the Contractor, other federal agencies, and any third-party contractors or firms at the request or direction of DOJ, may include inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Security Incident and/or liability for any additional response activities. The Contractor shall be responsible for all costs and related resource allocations required for all such response activities related to any Security Incident, including the cost of any penetration testing.

VII. Pass-Through of Security Requirements to Subcontractors and CSPs

A. The requirements set forth in the preceding paragraphs of this clause apply to all subcontractors and CSPs who perform work in connection with the contract, including any CSP providing services for any other CSP under the contract, and the Contractor shall flow down this clause to all subcontractors and CSPs performing under this contract. Any breach by any subcontractor or CSP of any of the provisions set forth in this clause will be attributed to the Contractor.

(End of Clause)

DOJ-07 Prohibition On Access By Non-U.S. Citizens To DOJ It Systems (MAR 2002)

The Department of Justice does not permit the use of Non-U.S. citizens in the performance of this contract or commitment for any position that involves access to or development of any DOJ Information Technology (IT) system. By signing the contract or commitment

document, the contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract or commitment can be met by using Non-U.S. citizens, those requirements shall be clearly described.

(End of Clause)

DOJ-08 Continuing Contract Performance During a Pandemic Influenza or Other National Emergency (OCT 2007)

During a Pandemic or other emergency we understand that our contractor workforce will experience the same high levels of absenteeism as our federal employees. Although the Excusable Delays and Termination for Default clauses used in government contracts list epidemics and quarantine restrictions among the reasons to excuse delays in contract performance, we expect our contractors to make a reasonable effort to keep performance at an acceptable level during emergency periods.

The Office of Personnel Management (OPM) has provided guidance to federal managers and employees on the kinds of actions to be taken to ensure the continuity of operations during emergency periods. This guidance is also applicable to our contract workforce. Contractors are expected to have reasonable policies in place for continuing work performance, particularly those performing mission critical services, during a pandemic influenza or other emergency situation. The types of actions a federal contractor should reasonably take to help ensure performance are:

• Encourage employees to get inoculations or follow other preventive measures as advised by the public health service.

• Contractors should cross-train workers as backup for all positions performing critical services. This is particularly important for work such as guard services where telework is not an option.

• Implement telework to the greatest extent possible in the workgroup so systems are in place to support successful remote work in an emergency.

• Communicate expectations to all employees regarding their roles and responsibilities in relation to remote work in the event of a pandemic health crisis or other emergency.

• Establish communication processes to notify employees of activation of this plan.

• Integrate pandemic health crisis response expectations into telework agreements.

• With the employee, assess requirements for working at home (supplies and equipment needed for an extended telework period). Security concerns should be considered in making equipment choices; agencies or contractors may wish to avoid use of employees' personal computers and provide them with PCs or laptops as appropriate.

• Determine how all employees who may telework will communicate with one another and with management to accomplish work.

• Practice telework regularly to ensure effectiveness.

• Make it clear that in emergency situations, employees must perform all duties assigned by management, even if they are outside usual or customary duties.

• Identify how time and attendance will be maintained.

It is the contractor's responsibility to advise the government contracting officer if they anticipate not being able to perform and to work with the Department to fill gaps as necessary. This means direct communication with the contracting officer or in his/her absence, another responsible person in the contracting office via telephone or email messages acknowledging the contractors notification. The incumbent contractor is responsible for assisting the Department in estimating the adverse impacts of nonperformance and to work diligently with the Department to develop a strategy for maintaining the continuity of operations.

The Department does reserve the right in such emergency situations to use federal employees. employees of other agencies, contract support from other existing contractors, or to enter into new contracts for critical support services. Any new contracting efforts would be acquired following the guidance in the Office of federal Procurement Policy issuance "Emergency Acquisitions", May, 2007 and Subpart 18.2. Emergency Acquisition Flexibilities, of the federal Acquisition Regulations.

(End Of Clause)

JAR 2852.212-4 Contract Terms and Conditions, Commercial Items (FAR Deviation).

When a commercial item is contemplated (using FAR part 12 procedures or otherwise) and the contract will include FAR 52.212-4, the following replaces subparagraph (g)(2); paragraph (h); subparagraph (i)(2); paragraph (s); and paragraph (u), Unauthorized Obligations, of the basic FAR clause, and adds paragraph (w), as follows:

(g)(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment act regulations at 5 CFR part 1315, as modified by subparagraph (i)(2), *Prompt payment,* of this clause.

(h) *Patent indemnity.* Contractor shall indemnify and hold harmless the Government and its respective affiliates, officers, directors, employees, agents, successors and assigns (collectively, “Indemnities”) from and against any and all liability and losses incurred by the Indemnities that are (i) included in any settlement and/or (ii) awarded by a court of competent jurisdiction arising from or in connection with any third party claim of

infringement made against Indemnities asserting that any product or service supplied under this contract constitutes infringement of any patent, copyright, trademark, service mark, trade name or other proprietary or intellectual right. This indemnity shall not apply unless Contractor shall have been informed within a reasonable time by the Government of the claim or action alleging such infringement and shall have been given such opportunity as is afforded by applicable laws, rules, or regulations to participate in its defense. This indemnity also shall not apply to any claim unreasonably settled by the Government which obligates Contractor to make any admission or pay any amount without written consent signed by an authorized officer of Contractor, unless required by final decree of a court of competent jurisdiction.

(i)(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations (5 CFR part 1315), with the following modification regarding the due date: For the sole purpose of computing an interest penalty due the Contractor, the Government agrees to inspect and determine the acceptability of any supply delivered or service performed specified in the invoice within thirty (30) days of receipt of a proper invoice from the Contractor, after which time, if no affirmative action has been taken by the Government to accept such supply or service, the supply or service will be deemed accepted and payment due thirty (30) days from the date of deemed acceptance. If the Government makes the determination that the item delivered or service performed is deficient or otherwise unacceptable, or the invoice is otherwise determined not to be a proper invoice, the terms and conditions of this paragraph regarding prompt payment will apply to the date the Contractor corrects the deficiency in the item delivered or service performed or submits a proper invoice. If actual acceptance occurs within the constructive acceptance period, the Government will base the determination of an interest penalty on the actual date of acceptance. The constructive acceptance requirement does not, however, compel Government officials to accept supplies or services, perform contract administration functions, or make payment prior to fulfilling their responsibilities.

(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts provisions of the basic FAR clause at 52.212-4, and the Unauthorized Obligations and Contractor's Commercial Supplier Agreements—Unenforceable Clauses provisions of JAR 2852.212-4.

(3) FAR 52.212-5.

(4) Other paragraphs of the basic FAR clause at 52.212-4, with the exception of paragraph (o), Warranty, and those paragraphs identified in this deviation of 52.212-4.

(5) Addenda to this solicitation, contract, or order, including contractor's Commercial supplier agreements incorporated into the contract.

(6) Solicitation provisions if this is a solicitation.

(7) Paragraph (o), Warranty, of the basic FAR clause at 52.212-4.

(8) The Standard Form 1449.

(9) Other documents, exhibits, and attachments.

(10) The specification.

(u) *Unauthorized obligations.*

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract or order is subject to any Commercial supplier agreement that includes any language, provision, or clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (see 31 U.S.C. 1341), the following shall govern:

(i) Any such language, provision, or clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an “I agree” click box or other similar mechanism (*e.g.,* “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement and have no effect.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(w) *Commercial supplier agreements—unenforceable clauses.* When any supply or service acquired under this contract or order is subject to a contractor's commercial supplier agreement, the following shall be deemed incorporated into such agreement and modifies and replaces any similar language, provision, or clause in such agreement. As used herein, “this agreement” means any contractor commercial supplier agreement:

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) *Applicability.* This agreement is a part of a contract between commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR part 12).

(ii) *End user.* This agreement shall bind the Government as end user but shall not operate to bind the Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) *Law and disputes.* This agreement is governed by Federal law.

(A) Any language, provision, or clause purporting to subject the U.S. Government to the laws of any U.S. state, territory, district, or municipality, or the laws of a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted and shall have no effect.

(B) Any language, provision, or clause requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted and shall have no effect.

(C) Any language, provision, or clause prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted and shall have no effect.

(iv) *Continued performance.* Notwithstanding any other provision in this agreement, if the Contractor believes the Government to be in breach of this contract, order, or agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in subparagraph (d), Disputes, of FAR 52.212-4.

(v) *Arbitration; equitable or injunctive relief.* In the event of a claim or dispute arising under or relating to the contract, order, or this agreement, (A) binding arbitration shall not be used unless otherwise specifically authorized by agency guidance, and (B) equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the Government only when explicitly provided by statute.

(vi) *Updating terms.*

(A) After award, the contractor may unilaterally revise terms if they are not material. Material terms are defined as:

(1) Terms that change Government rights or obligations;

(2) Terms that increase Government prices;

(3) Terms that decrease the overall level of service; or

(4) Terms that limit any other Government right addressed elsewhere in this contract.

(B) For revisions that materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.

(C) Any agreement terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provisions of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.

(vii) *Order of precedence.* Any Order of Precedence clause in any commercial supplier agreement is not enforceable against the Government. The applicable Order of Precedence for this contract, order, or agreement is FAR 52.212-4(s), as revised by JAR 2812.302 and 2852.212-4(s).

(viii) *No automatic renewals.* If any license or service tied to period payment is provided under this agreement (*e.g.,* annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by a properly warranted contracting officer, and any provision or term of any license or service purporting to provide for automatic renewal is unenforceable against the Government.

(ix) *Indemnification by the Government or end-user.* Any language, provision, or clause of this commercial supplier agreement requiring the Government or End-user to indemnify the commercial supplier or licensor is not enforceable against the Government.

(x) *Indemnification by the commercial supplier or licensor.* Any clause of this agreement requiring or permitting the commercial supplier or licensor to defend the Government as a condition of indemnifying the Government for any claim of infringement is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(xi) *Audits.* Any language, provision, or clause of this commercial supplier agreement permitting Contractor to audit the end user's compliance with this agreement is not enforceable against the Government. To the extent any language, provision or clause of this agreement permits Contractor to audit the Government's compliance under this contract, order, or agreement, such language, provision, or clause of this agreement is hereby stricken and replaced as follows:

"(A) If Contractor reasonably believes that the Government has violated the terms of this agreement with regard to the restrictions on authorized use and/or the number of authorized users, upon written request from Contractor, including an explanation of the basis for the request, DOJ will provide a redacted version of the Government's most recent Security Assessment and Authorization package (SAA) to Contractor on a confidential basis, so that

Contractor may reasonably verify the Government's compliance with its obligations under this agreement. Contractor understands and agrees that the Government will remove or redact any information from the SAA that it reasonably believes may compromise (a) the security of the Government's information technology environment; (b) the confidentiality of any third-party proprietary or confidential information; (c) any confidential, sensitive law enforcement information; and (d) any other information that the Government believes may compromise a past, current, or prospective investigation, prosecution, or litigation. Notwithstanding the preceding, and subject to the Government's policies and procedures for such review, including but not limited to complying with all Government security requirements prior to being granted access to the Government's facilities, including the execution of appropriate confidentiality and/or non-disclosure agreements, the Government will arrange, upon Contractor's written request, for Contractor to view an un-redacted version of the SAA on Government premises. Contractor understands that Contractor will be provided a copy of the un-redacted SAA on Government premises only and that no un-redacted copy of the SAA, or any medium containing information relating to it, will be permitted to be removed from Government premises.

(B) The Contractor also understands and agrees that the Contractor shall make a request under this paragraph no more than on an annual basis and only during the period of the contract, and that any activities performed by Contractor under this clause will be performed at Contractor's expense, without reimbursement by the Government.

(C) Discrepancies found with regard to the restrictions on authorized use and/or the number of authorized users may result in a charge by Contractor to the Government. Any resulting invoice must comply with the proper invoicing and payment requirements specified in the contract. This charge, if disputed by the Government, will be resolved through the Disputes clause at 52.212-4(d); no payment obligation shall arise on the part of the Government until the conclusion of the dispute process."

(xii) *Taxes or surcharges.* Any taxes or surcharges which the Contractor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xiii) *Non-assignment.* This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under FAR 52.212-4 (b), Assignment.

(xiv) *Confidential information.*

(A) During the term of this contract or order, either party may identify information as "confidential information," and there shall be no disclosure, dissemination, or publication of any such information except to the extent required for the performance of this contract or order and otherwise provided in this clause or by statute or regulation. Specifically, the parties agree that the party receiving confidential information may only disclose such information to its employees and contractors on a "need-to-know" basis to carry out the obligations of this contract or order, and that subcontractors performing under this Agreement are subject to the same stipulations provided in this provision. The parties also agree that this provision shall survive the termination of this contract or order, and any confidential information obtained or received which comes within these restrictions shall remain confidential, provided that the obligation to treat information as confidential shall not apply to information which is or becomes publicly available through no improper action of the receiving party; is or comes to be in the receiving party's possession independent of its relationship with the disclosing party; is developed by or becomes known to the receiving party without use of any confidential information of the disclosing party; or is obtained rightfully from a third party not bound by an obligation of confidentiality. Additionally, nothing in this contract or order shall restrict disclosure by the receiving party pursuant to any applicable law, including but not limited to the Freedom of Information Act, 5 U.S.C. 552, *et seq.,* or an order of any court of competent jurisdiction, provided that in either such case the receiving party gives prompt notice to the disclosing party to allow the disclosing party to interpose an objection to such disclosure, take action to assure confidential handling of the confidential information, or take such other action as it deems appropriate to protect its confidential information.

(B) The Government considers and hereby identifies as confidential any and all information related to any inquiries and/or searches performed by the Government or by contractor at the Government's direction under this contract or order, including the subject of any such inquiry or search and any and all search terms, regardless of whether provided in writing or orally to Contractor, and Contractor agrees that it may only disclose such information to its employees and contractors on a "need-to-know" basis to carry out the obligations of this contract or order and that it will not share, reveal, divulge, disclose, disseminate, or publicize any such information to any third party except as provided in this provision without the prior written approval of the Contracting Officer. Contractor also understands and agrees that any subcontractors performing under this contract or order are subject to the same stipulations and that Contractor may be held responsible for any violations of confidentiality by a subcontractor.

(C) These provisions are consistent with and do not supersede, conflict with, or otherwise

alter an employee's obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by Executive orders and statutory provisions relating to whistleblower protection are incorporated into this contract and are controlling.

(D) The Government may share the terms, conditions and prices set forth in this Order with, and provide a copy of the Order to, other Executive branch agencies of the U.S. Government, provided that the Government shall ensure that other Executive branch agencies to which it provides such information will be required to treat all such information consistent with terms and conditions set forth in this Order.

(E) Notwithstanding anything in this agreement, the Government may retain any confidential information as required by law, regulation, or its internal document retention procedures for legal, regulatory, or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this Order.

(xv) *Authorized users.* Authorized users may include full and part-time employees of the Government, including those working at or from remote locations, and contractors and contractor employees working within the scope of their contract with the Government, including those at or from remote locations.

(xvi) *Authorized use.* Authorized users are authorized to use the product or service acquired under this contract in performing business on behalf of the Government. Any information obtained or acquired by the Government under this contract may be used by the Government in the performance of Government business.

(2) If any language, provision, or clause of this agreement conflicts or is inconsistent with the preceding paragraph (w)(1), the language, provisions, or clause of paragraph (w)(1) shall prevails to the extent of such inconsistency.

(End of Clause)

JAR 2852.222-70 Domestic Violence, Sexual Assault, and Stalking.

Domestic Violence, Sexual Assault, and Stalking (DEC 2014)

(a) It is DOJ 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, Federal Workforce Responses to Domestic Violence, Sexual Assault, and*

Stalking," available in full for public viewing at: *http://www.justice.gov/sites/default/files/ovw/legacy/2013/12/19/federal-workplacee-responses-to-domesticeviolence-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 Vendor employees and employees of subcontractors who will be assigned to work on DOJ premises.

(b) Upon contract award, DOJ will provide the Contractor with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking for the component or components where the Contractor will be performing. The Contractor agrees to inform its employees and employees of subcontractors, who will be assigned to work on DOJ premises, with the name and contact information of the point of contact for victims of domestic violence, sexual assault, and stalking.

(End of Clause)

JAR 2852.233-70 Protests Filed Directly with the Department of Justice.

Protests Filed Directly With the Department of Justice (NOV 2020)

(a) The following definitions apply in this provision:

(1) "Agency Protest Official" (APO) means the Deciding Official for a procurement protest filed with a contracting activity of DOJ when the contracting officer will not be the Deciding Official because of the protestor's election under JAR 2833.103(b)

(2) "Deciding Official" means the official who will review and decide a procurement protest filed with the agency. The Deciding Official will be the contracting officer unless the protestor requests pursuant to JAR 2833.103(b) that the protest be decided by an individual above the level of the contracting officer, in which case the HCA will designate an APO to serve as the Deciding Official.

(3) "Interested Party" means an actual or prospective offeror whose direct economic interest would be affected by the award of a contract or by the failure to award a contract.

(b) Only interested parties may file a protest.

(c) An interested party filing a protest with the DOJ has the choice of requesting either that the Contracting Officer or the APO decide the protest.

(d) A protest filed directly with the DOJ shall:

(1) Indicate that it is a protest to DOJ.

(2) Be filed with the Contracting Officer.

(3) State whether the protestor chooses to have the Contracting Officer or the Agency

Protest Official decide the protest. If the protestor is silent on this matter, the Contracting Officer will decide the protest.

(4) Indicate whether the protestor prefers to make an oral or written presentation of arguments in support of the protest to the deciding official.

(5) Include the information required by FAR 33.103(d)(2):

(i) Name, address, facsimile number and telephone number of the protestor.

(ii) Solicitation or contract number.

(iii) Detailed statement of the legal and factual grounds for the protest, to include a description of resulting prejudice to the protestor.

(iv) Copies of relevant documents.

(v) Request for a ruling by the agency.

(vi) Statement as to the form of relief requested.

(vii) All information establishing that the protestor is an interested party for the purpose of filing a protest.

(viii) All information establishing the timeliness of the protest.

(e) The decision by the APO is an alternative to a decision by the Contracting Officer. The APO will not consider appeals from the Contracting Officer's decision on an agency protest and a decision by the APO is final and not appealable.

(f) The Deciding Official may conduct a scheduling conference. The scheduling conference, if conducted, will establish deadlines for oral or written arguments in support of the agency protest and for agency officials to present information in response to the protest issues. The deciding official may hear oral arguments in support of the agency protest at the same time as the scheduling conference, depending on availability of the necessary parties.

(g) Oral conferences may take place either by telephone or in person.

(h) The protestor has only one opportunity to support or explain the substance of its protest. DOJ procedures do not provide for any discovery. The deciding official may request additional information from the agency or the protestor. The deciding official will resolve the protest through informal presentations or meetings to the maximum extent practicable.

(i) A protestor may represent itself or be represented by legal counsel. The DOJ will not reimburse the protester for any legal fees related to the agency protest.

(j) The DOJ will stay award or suspend contract performance in accordance with FAR 33.103(f), unless the contract award is justified, in writing, for urgent and compelling reasons or is determined, in writing, to be in the best interest of the Government. The

justification or determination shall be approved at a level above the Contracting Officer. The stay or suspension, unless over-ridden, remains in effect until the protest is decided, dismissed, or withdrawn.

(k) The deciding official will make a best effort to issue a decision on the protest within thirty-five (35) days after the filing date. The decision shall be written, and provided to the protestor using a method that provides for evidence of receipt.

(l) The DOJ may dismiss or stay proceedings on an agency protest if a protest on the same or similar basis is filed with a forum outside DOJ.

(End of Clause)

PART III – Attachments

Section J – The following are attachments as part of this solicitation:

Attachment 1 – Statement of Work

Attachment 2 – Pricing Schedule

Attachment 3 – Questions Format

Attachment 4 – Supporting Documentation Place of Performance

Attachment 5 – Performance Requirement Standards (PRS)

PART IV – Representations and Instructions

Section K – Representations, Certifications, and other Statements of Offerors

K.3. FAR Subpart 9.5 Organizational Conflict of Interest Disclosure

K.4. FAR 52.203-2 Certification of Independent Price Determination (APR 1985)

K.5. FAR 52.209-5 and FAR 52.209-7 Responsibility Matters

Section L – Instructions, Conditions, and Notices to the Offerors

General Information

FAR 52.216-1 Type of Contract (Dec 2025)

The Government contemplates award of a standalone Firm Fixed Price contract resulting from the solicitation to an Offeror whose proposal is determined to provide the Best Value to the Government.

***Note that the solicitation does not commit the Government to pay any cost for the preparation and submission of a proposal. Until a formal notice of award is issued, no communication by the Government, either written or oral, shall be interpreted as a promise

that an award will be made. It is also advised that the Contracting Officer (CO) is the only individual who can legally commit and obligate the Government to the expenditure of public funds in connection with the proposed acquisition.

FAR 52.233-2, Service of Protest (Nov 2025)

(a) Protests, (as defined in FAR 33.102), that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), must be served on the Contracting Officer identified in the solicitation by obtaining written and dated acknowledgment of receipt from them.

Tracy-Ann Thomas-Arthur
USDOJ/JMD
145 N St. NE
Washington, DC 20002
Tracy-Ann.B.Thomas-Arthur@usdoj.gov

(b) The copy of any protest must be received in the office designated above within one day of filing a protest with the GAO.

Proposal Instructions

These instructions are a guide for preparing a proposal. The instructions describe the type and extent of information required and emphasize the significant areas to be addressed in the proposal. The Offeror shall review the Statement of Work (SOW) contained in the solicitation, for further insight into the areas to be addressed within the proposal. The Offeror's proposal shall include detailed information to enable the Government evaluators to conduct a meaningful review and make a determination, relative to the Offeror's understanding of the requirements in each of the evaluated areas. In addition, other than small business Offerors shall submit a subcontracting plan with their proposal in accordance with FAR 52.219-9.

Questions Due: Offerors must submit all questions concerning the solicitation to the CO via Attachment 3, Questions Format. Questions must be received no later than June 25, 2026, 10:00AM Eastern Standard Time (EST). All questions shall be submitted electronically to:

Tracy-Ann.B.Thomas-Arthur@usdoj.gov . The following must be listed in the subject line of the email "Questions – LASRF 15JPSS26Q00000058". No phone calls will be accepted.

Offerors are strongly encouraged to submit questions early in the process. Any responses made will be in the form of an amendment to the solicitation and will be furnished to all prospective Offerors via posting to: **www.sam.gov**. Explanations or instructions given in a form other than an amendment to the solicitation shall not be binding. Prospective Offerors are responsible for downloading the solicitation and any amendments from: **www.sam.gov** .

Proposals Due: All Offerors shall submit a proposal via email to:

Tracy-Ann.B.Thomas-Arthur@usdoj.gov, which will be considered if received by 10:00 AM,

Eastern Standard Time (EST) on July 13, 2026. The subject line shall read: "Proposal-15JPSS26Q00000058 – LASRF Legal Services." Within the e-mail body, the Offeror shall include a statement verifying that they are SAM Registered under NAICS CODE: 541110, Offices of Lawyers. No phone calls will be accepted.

Offers, modifications, revisions, or withdrawals of Offers received after the date established in the Request for Proposal (RFP) for receipt of proposals will be handled in accordance with FAR Clause 52.215-1. Offerors are advised to notify the Contracting Officer immediately if there is any change to the proposal after submission (e.g. a proposed employee departs from the company or is no longer available).

All Proposals shall consist of three (3) volumes:

1. **Volume I – Technical Capability (Technical Approach and Management Approach)**
2. **Volume II – Price**
3. **Volume III – Past Performance**

Offerors shall provide a technical description/narrative of the services being offered in sufficient detail to evaluate compliance with the requirements in the solicitation and Statement of Work and standards. Incomplete proposals shall be considered non-responsive and will not be evaluated.

Offerors that fail to submit all required documentation, or do not complete the required representations and certifications, or reject the terms and conditions of the solicitation, may be considered non-responsive and therefore, excluded from consideration.

The Offeror's proposal shall be clear, concise, and shall include detailed narrative information for evaluation and substantiation of the validity of stated claims. The Government may consider the Offeror's assertions or merely restating the Governments requirements without further explanation, clarification, or context, to be weaknesses or deficiencies. The Offeror shall not simply rephrase or restate the Government's requirements but shall rather provide a rationale or explanation to convince the Government that the Offeror's approach will meet the Government requirements. Likewise, the Government will not consider assertions or representations without substantiation and context to be convincing or explanatory.

DOJ reserves the right:

Not to hold negotiations
Not to award a contract, and/or
To cancel the solicitation.

Offerors are hereby notified that all information provided, including all resumes, must be accurate, truthful, and complete to the best of the Contractor's knowledge and belief. The Agency will rely upon all representations made by the Contractor both in the evaluation process and for the performance of the work by the Offeror selected for award. The Offeror's proposal shall, therefore, contain the Offeror's best terms from a price and technical standpoint. Offerors are cautioned to examine the solicitation in its entirety, inclusive of clauses and provisions

incorporated by reference, and to ensure that proposals contain all necessary information, provide all required documentation, and are complete in all respects. The Government is not obligated to make another request for the required information, nor does the Government assume the duty to search for data to cure problems it finds in proposals. During the evaluation process, the Government may request clarifications as necessary. Such clarifications do not constitute negotiations and do not permit offerors to revise their proposals or remedy deficiencies, material omissions, or substantive technical or cost issues, in accordance with FAR 15.202(a)(2).

Offerors shall assume that the Government has no prior knowledge of the company's capability and experience.

A proposal is presumed to represent the Offeror's best efforts in response to this solicitation. Any inconsistencies within the proposal should be clearly explained by the Offeror. This explanation will assist the Government in understanding the Offeror's pricing approach. The Government will evaluate prices in accordance with FAR 15.404-1(b), consistent with the solicitation's stated evaluation methodology.

*** Note proposals submitted in response to this solicitation shall be valid until 120-days after the deadline for receipt of proposals.

Submission of Offers

The proposal must be written clearly, legibly, and in English. It must be specific, complete, and follow all instructions and formatting requirements. Offerors should not create new samples or descriptive literature solely for inclusion in the proposal. An official authorized to bind the firm shall sign the Standard Form (SF) 1449, all amendment SF30 documents, and all certifications requiring original signature.

Proposals shall be provided in three volumes: Volume I, Volume II and Volume III. All information pertaining to a particular volume shall be confined to that volume. For example, no Price information shall be included in any volume other than the Price volume. The Government is not required to and will not search other volumes for a missing file.

Each volume shall be separate and complete so that evaluation of the one may be accomplished independently from the evaluation of the other. The technical proposal shall not identify proposed prices; however, it shall contain resource information (such as staffing levels) as called for by the instructions set forth below.

Each Offeror shall comply with the detailed instructions for the format and content of the offer in order to be considered for award. When evaluating an offer, the Government will consider how well the Offeror has complied with these instructions. The Government will consider any failure on the part of an Offeror to comply with the instructions to be an indication of the type of conduct it can expect during contract performance. The Government reserves the right to consider an Offeror non-responsive and not give further consideration for non-compliance with preparation of proposals instructions.

The Contractor shall be **registered** and **active** in the System for Award Management (SAM) in

accordance with FAR 52.204-7 and 52.204-13. The Offeror shall provide a Unique Entity ID (UEI) and Tax Identification Number (TIN) with submission of a proposal response. Register by going to https://sam.gov/content/home .

Electronic versions of the technical, past performance, and price proposal must be submitted together. Electronic files must be compatible with either Adobe Acrobat, Microsoft Word, or Excel. Hard copy, oral, and facsimile proposals will not be accepted.

Every proposal shall contain an electronic version of the proposal formatted using the same volume structure listed via instructions. Each volume shall contain a table of contents, list of tables or figures (if required) and list of appendixes. Contents shall follow the order of the evaluation criteria and pages shall be numbered.

Confidentiality: No proprietary, classified, confidential, or sensitive information should be included in the response. The Government reserves the right to use any non-proprietary technical information in any resultant solicitation(s). The penalty for making false statements in offers is prescribed in 18 U.S.C. § 1001.

Offer Format

Volume II shall contain the auxiliary supporting price data Microsoft (MS) Excel spreadsheets. The Government considers all proposals as “For Official Use Only" and to contain "Source Selection Information in accordance with FAR 2.101 and FAR 3.104.”

The offer shall meet the following format requirements for each Volume:

Offerors shall number all pages. Offeror’s proposals shall be 8.5 x 11 inches. Text shall be single-spaced. Except for the reproduced sections of the solicitation document, the font shall be Times New Roman, the font size shall be no less than 12 points. For tables, charts, graphs and figures, any readable font is acceptable, but the font size shall be no smaller than 10 points.

The Offeror may use legible tables, charts, graphs, and figures wherever practical to depict systems, implementation schedules, and plans. These displays shall be legible and easy to follow and shall not exceed 11 x 17 inches.

Offerors shall use cross-references within the offer and provide a clear, consistent reference system by section, paragraph, page, etc. The cross-reference index is excluded from the page limitation of the offer.

The offer shall be limited to the following submissions and pages:

Volume I: Technical Capability

Evaluation Factor 1 – Technical Approach – 60 pages (includes all sub-factors)

Evaluation Factor 2 – Management Approach – 20 pages

Volume II: Price Proposal

Evaluation Factor 4 – Price - No Page Limit

Volume III: Past Performance

Evaluation Factor 3 – Past Performance

Volume III shall contain Past Performance information regarding similar contracts and RFP Supporting Documents.

No page limit except for resumes, which are limited to 3 pages per resume. Key personnel Letters of Commitment are limited to 1 page. The page limits do not apply to the cover letter; solicitation; Amendments; table of contents; cross reference index; definitions; and required representations and certifications. The Government shall treat page limitations as maximums. If exceeded, the Contracting Officer will eliminate the excess pages prior to the evaluation. The Government will not read or evaluate excess pages, and the offer may be considered non-responsive.

Proposal Content

Volume I – Technical Approach

The Offeror's Technical Volume shall demonstrate an understanding of an ability to comply with all the requirements contained in the solicitation. General statements such as the Offeror "can or will comply with the requirements," "standard procedures will be used," "well-known techniques will be used," or proposals that simply rephrase, paraphrase or restate the Government's requirements, or the solicitation's SOW in whole or in part, will not constitute compliance. Offerors are required to provide supporting rationale/narratives to address how the Offeror intends to meet the requirements of the SOW. Failure to conform to any of the requirements of the solicitation may render the proposal "non-responsive" and may constitute the basis of rejection of the proposal or may render the proposal to be unsatisfactory and may not be considered for award. Proposals that merely offer to conduct the project or program in accordance with the requirements of the Government's SOW, shall be considered non-responsive for award. To be responsive for consideration for award, the Offeror shall submit a comprehensive explanation of the proposed technical approach and the tasks to be performed in achieving the procurement objectives. The Offeror shall describe its overall approach to the types of services that the Offeror expects to deliver and perform as a result of the award and its ability to perform the work in compliance with applicable standards, guidance, and EOIR's program objectives.

The following information shall be provided and will be evaluated to assess proposal risk in accordance with Section M, Evaluation. Proposals shall be clear, concise, and include detailed information for effective evaluation. Offerors shall assume that the Government has no prior knowledge of the firms' experiences and will base its evaluation on the information presented in the Offeror's proposal.

Evaluation Factor 1 – Technical Approach (Volume I)

Within the page limit outlined above, the proposal shall contain details to indicate the Offeror's ability to deliver performance of the requirements within the SOW without a high degree of risk. The Offeror shall provide a detailed narrative discussing the proposed process and procedures to plan and perform the work required to achieve a quality solution to the requirements outlined in the SOW. The Offeror's Technical Approach shall be presented in the following order, with subsections and parts. Additional guidance is as follows:

The Offeror shall provide a detailed narrative discussing the proposed process and procedures to plan and perform the work required to achieve all the tasks specified in the SOW.

The Offeror shall include a table of contents, cross referencing each SOW task to the applicable page number(s) within the proposal which addresses how the performance objectives shall be achieved.

The Government will evaluate the Offeror's transition-in approach to assess how well it addresses a transition in period that includes a timeline of scheduled events (to occur throughout the 30-day period) which are clearly tied to the Offeror's ability to reach full operating capacity at the end of the transition period.

The Offeror shall provide, for evaluation, the following items with proposal submission under Volume I:

1. Transition-In Plan
2. Transition-Out Plan

Volume I Management Approach

Evaluation Factor 2 – Management Approach

Within the page limit outlined above, the proposal shall contain details to indicate the Offeror's ability to deliver performance of the requirements within the SOW without a high degree of risk.

The Government will evaluate how well the Offeror's management approach and business model clearly outlines how the Offeror plans to accomplish requirements in SOW. The Government will evaluate how well the Offeror's approach addresses their plan for recruiting, training, and retention of qualified personnel to fill vacant positions and maintain continuity of personnel throughout the life of the contract.

The Government will evaluate how well the organizational structure and staffing plan clearly outline staffing levels that align qualified personnel by proposed labor category and staffing information to support the proposed level of effort. The Government will evaluate whether the level of effort and the mix of labor quoted is sufficient to meet SOW requirements. The Government will evaluate how well the staffing plan addresses how the Offeror will manage employee absenteeism as it relates to impact on operations and SOW requirements. The Government will evaluate whether the proposed staffing structure specifically addresses the Offeror's approach to staffing positions requiring appropriate security clearances and certification levels as described in the SOW.

The Offeror shall provide, for evaluation, the following items with proposal submission under

Volume I:

1. Staffing Plan
2. Organizational Chart
3. Letters of Commitment and Resumes for any proposed Key Personnel

Volume III Past Performance

Evaluation Factor 3 – Past Performance

A. Offerors shall provide information on no more than three (3) previous contracts performed for federal, state, and local government agencies and/or commercial customers, for which the offeror's efforts are recent and relevant to the efforts required by this RFP and which demonstrates their ability to perform their proposed effort. Offerors shall also provide information on problems encountered on the identified contracts and the offeror's corrective actions. If the offeror has no recent or relevant Past Performance, the offeror shall state so.

(1) "Recent" is defined as occurring within the last three years prior to the RFP closing date. Recent is further defined as those contracts in which efforts have been performed for at one year. [1-year performance requirement applies to referenced efforts that have already been completed within three (3) years of the date that proposals are due as well as referenced efforts that are still ongoing. In other words, both types of references (those completed and those still ongoing) must have at least 1-year of performance to be considered recent.]

(2) "Relevant" is defined as a contract of similar scope, magnitude, and complexity to the requirements as set forth in this solicitation.

- **Scope**: Experience in the areas defined in the SOW.

- **Magnitude**: The measure of the similarity of the volume, dollar value and/or duration of the work actually performed under the offeror's submitted contracts to the SOW.

- **Complexity**: The measure of the similarity of technical difficulty, managerial intricacy, and/or required coordination of efforts and disciplines performed by the offeror in its submitted contracts to the SOW. For complexity, not only will the tasks performed by the offeror be considered, but also the offeror's ability to coordinate tasks (e.g., concurrent performance requirements).

B. Offerors shall provide the following information for each reference listing:

•Agency Name;

• Contract and/or Task Order Number and Date of Award;

• Contract Period of Performance;

• Point of Contact (individual with knowledge of contract performance) include their name, phone number, and email address;

• Total Contract Value;

• Contract Type

• Description of Work

Volume II: Price Proposal

Evaluation Factor 4 – Price

The Pricing proposal will include a comprehensive summary of all pricing information for the proposed services to include SOW requirements. The Offeror shall submit a price proposal utilizing Attachment 2 Pricing Schedule. Offerors shall complete the entire worksheet, to include items describing proposed pricing data for contract performance. The price proposal shall include a detailed Basis of Estimate (BOE) that describes the methodology and rationale used to develop proposed pricing. The BOE shall clearly relate all proposed costs to the requirements outlined in the Technical Approach and Management Approach. The Offeror shall state all ground rules and assumptions used to derive, develop, or calculate prices.

This section of the proposal shall consist of sufficient cost/pricing data to enable the Government to perform a comprehensive price analysis of the proposed price of the work. The Government will separately evaluate quoted prices to determine that the prices are fair and reasonable. Offerors shall detail all costs supporting the price for the base period and all option periods. All total dollar amounts provided shall be rounded to the nearest cent.

Additional guidance is as follows:

a. The Offeror shall clearly explain the approach to deriving and calculating the proposed prices. The Contract Line-Item Numbers (CLINs) for services is to include all labor, resources, etc.

b. The Offeror shall provide the basis of estimated information that is consistent with and traceable to the Offeror's Technical Approach/Management Approach. This includes describing the tasks identified in the proposal and labor hours (by labor category) required to complete those tasks.

c. The price proposal shall be submitted to the Government in the original Microsoft Excel format. PDF versions of the pricing information are not acceptable. The Offeror shall submit all electronic documents for Microsoft Office suite products without the use of "macros".

Section M: Evaluation Factors

M.1: Basis for Award

The Government will select the best value by conducting a tradeoff among all the evaluation factors. A single Firm Fixed Price Contract will be awarded to the Offeror who is deemed responsible. The Government will evaluate proposals based on the evaluation factors below.

The Government reserves the right to conduct negotiations if it is determined that it will be in the best interest of the Government to do so. Negotiations, if necessary, will be conducted in accordance with FAR 15.204-2. If the Government does enter into negotiations, they may be held only with those Offerors determined to be in the competitive range. If the Contracting Officer determines that the number of proposals that will otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit efficient competition among the most highly rated proposals. An award will be made to the Offeror whose proposal conforms to the terms and conditions of the solicitation and award may be made to other than the lowest priced or other than the highest technically rated offer.

Relative Importance and Trade-Offs:

The Government will base the determination of best value on the evaluation factors identified below, which are listed in descending order of importance.

1. **Technical Approach**
2. **Management Approach**
3. **Past Performance**
4. **Price**

Factors 1-3 when combined are significantly more important than price. However, in cases where technical competence between Offerors is considered approximately the same, then price could increase in importance.

DOJ will base its award decision using a best value tradeoff analysis that results in the most advantageous acquisition for the Government. The tradeoff process allows the agency to trade the benefits of a proposal with a lower price for a proposal with a higher price that is technically superior, when doing so is most advantageous to the Government. In addition, the subcontracting plan will be evaluated for acceptability and must be determined acceptable for an offeror to remain eligible for award.

M.2. Factor 1: Technical Approach

The Government will evaluate the extent to which the Offeror, through a detailed narrative, demonstrates its knowledge, understanding, and capability to meet all requirements described in the Statement of Work (SOW). The Government will further evaluate the extent to which the Offeror proposes efficient and effective techniques, methodologies, procedures, and tools for accomplishing the performance objectives specified in the SOW.

M.3. Factor 2: Management Approach

The Government will evaluate the Offeror's Management Approach to determine the extent to which the Offeror demonstrates a clear, comprehensive, and effective plan for managing all requirements of the Statement of Work (SOW). The evaluation will consider whether the

Offeror's proposed management structure, processes, staffing, and resource allocations are adequate to ensure successful performance throughout the period of performance.

The Government will evaluate:

a. the extent to which the Offeror, through its detailed narrative, demonstrates its knowledge, understanding, and ability to effectively manage the requirements of the SOW. This includes the Offeror's approach to organizing, supervising, coordinating, and controlling all work efforts to ensure timely, accurate, and compliant completion of tasks.

b. The Government will evaluate the Offeror's approach to identifying, mitigating, and managing risks that may impact performance. This includes the adequacy of proposed mitigation strategies, contingency planning, and the Offeror's ability to proactively address potential performance challenges.

c. The extent to which the Offeror demonstrates quality control processes relates to the requirements of the SOW to ensure service quality, accuracy, and customer satisfaction

d. Organizational Structure and Staffing: The Government will evaluate the extent to which the Offeror's proposed staffing levels, labor categories, qualifications, expertise, and years of experience are sufficient and appropriate to successfully perform the SOW requirements. This includes an assessment of management personnel, key staff, and the adequacy of any proposed subcontractor or team partner arrangements.

    1. Resume (s) for the proposed personnel identified as key personnel. The resume (s) at a minimum shall include company name, duties performed by individual, dates of employment, qualifications, experience, skills, availability, and credentials (education and certifications) for the proposed key personnel that demonstrates meeting the requirements detailed in the SOW

e. Roles and responsibilities: The Government will assess how well the proposed Management Approach explains the Offeror's plan to execute the responsibilities outlined in the SOW. This includes the clarity and feasibility of management processes, decision-making structures, internal controls, communication plans, and approaches for ensuring quality, timeliness, and responsiveness.

f. The Government will assess the effectiveness of the Offeror's plan for allocating resources, monitoring performance, ensuring compliance, and maintaining quality throughout the period of performance. This includes the Offeror's internal oversight mechanisms, performance metrics, and methods for ensuring continuous improvement.

The Government will evaluate the Technical Approach and Management Approach factors using the evaluation framework provided in the Table below. The Department of Justice (DOJ) will assess the Offeror's overall technical and management approaches to determine the likelihood that the Offeror will successfully understand, manage, and perform the requirements of the SOW with minimal risk to the Government throughout the period of performance. Based on this

assessment, the Government will assign an adjectival rating in accordance with the adjectival ratings table below, which correlates identified strengths, weaknesses, and associated risk.

High Risk- Significant doubt exists that the Offeror can successfully perform the requirement; weaknesses outweigh strengths.

Medium Risk – Some doubt exists regarding the Offeror's ability to fully meet requirements; however, performance risk is manageable

Low Risk – Little to no doubt exists that the Offeror can successfully perform the requirement. Strengths significantly outweigh weaknesses.

Strength – An aspect of the proposal that increases the likelihood of successful performance

Weakness – A flaw in the proposal that increase risk of unsuccessful performance.

Deficiency- A material failure to meet the requirement of the solicitation to include the SOW that would prevent successful performance.

Technical Capability (Technical and Management Approach, Factors 1 and 2) Rating,

Adjectival Rating	Definition
Outstanding	Proposal indicates an exceptional approach and understanding of the requirements and contains multiple strengths, and risk of unsuccessful performance is low.
Acceptable	Proposal meets requirements and indicates an adequate approach and understanding of the requirements, and risk of unsuccessful performance is no worse than medium.
Unacceptable	Proposal does not meet requirements of the solicitation, and contains one or more deficiencies, and/or risk of unsuccessful performance is high. Proposal is un- awardable.

M.4. Factor 3: Past Performance

The Offeror's Past Performance will be evaluated to assess the offeror's likelihood of successful performance in providing requirements similar in size, scope, and complexity of this RFP. The government may use present and/or past performance data obtained from a variety of sources, not just those identified by the offeror.

There are three aspects to the past performance evaluation: Recency, Relevancy and Quality.

The first aspect of the Past Performance evaluation is recency, as defined in the instructions section above in Section (L) Past Performance Instructions. If an instance of a past performance is deemed "Not Recent," the government will stop evaluation of the past performance reference, and it will not be evaluated for relevancy or quality.

The second aspect of the Past Performance evaluation is relevancy. The government will determine how relevant a recent past performance is to the effort to be acquired through this RFP. The government will consider the following aspects in its relevancy evaluation, as they are defined in the instructions section above: 1) scope, 2) magnitude, and 3) complexity. Each recent past performance reference provided by the offerors will receive one of the relevancy ratings outlined in the table below. If an instance of a past performance reference is deemed "Not Relevant," the government will stop evaluation of the past performance reference, and it will not be evaluated for quality or be included as part of the evaluation of an offeror's performance confidence.

The final aspect of the Past Performance evaluation is the overall quality of the offeror's past performance. The quality of any recent and relevant past performance will be evaluated under the following aspects: 1) Quality (Product or Service) 2) Timeliness (Schedule Performance) 3) Cost Control 4) Management (Business Relations) and 5) Other Remarks (Problem Resolution such as Management of Key Personnel).

After evaluating individual past performance submissions for recency, relevancy, and quality, the government will assign one overall confidence rating for Past Performance as outlined in the table below.

The past performance evaluation conducted in support of this RFP does not establish, create, or change existing records and history of the offeror's past performance on past contracts; rather, the past performance evaluation process gathers information from customers on how the offeror performed those past contracts.
In the case of an offeror who does not provide information on recent or relevant past performance, or where past performance information is not available, the offeror may not be evaluated favorably or unfavorably on this factor. The offeror shall receive the rating of "neutral," meaning the rating is neither favorable nor unfavorable. In a best value tradeoff, the government may determine that a "Substantial Confidence" or "Satisfactory Confidence" past performance rating is worth more than a "Neutral Confidence" past performance rating, as long as the determination is consistent with stated criteria.

A significant achievement, problem, or lack of data in any element can become an important consideration. A negative finding under any element may result in an adverse performance confidence assessment.

Since the government may not contact any or all of the past performance sources provided, it is incumbent upon the offeror to explain the relevance of the data provided. offerors are reminded that while the government may elect to consider data obtained from other sources, the burden of proving good past performance rests with the offerors.

Submitting more recent, relevant, and quality references may result in a higher-confidence rating. Likewise, submitting less than three (3) recent, relevant, and quality references may result in a lower confidence rating.

Ratings definitions for Factor 3 – Past Performance

Past Performance Relevancy	
Rating	Definition
Very Relevant	Present/past performance effort involved essentially the same scope and magnitude of effort and complexities this RFP requires.
Relevant	Present/past performance effort involved similar scope and magnitude of effort and complexities this RFP requires.
Somewhat Relevant	Present/past performance effort involved some of the scope and magnitude of effort and complexities this RFP requires.
Not Relevant	Present/past performance effort involved little or none of the scope and magnitude of effort and complexities this RFP requires.
Performance Confidence Assessments	
Rating	Definition
Substantial Confidence	Based on the offeror's recent and relevant performance record, the government has a high expectation that the offeror will successfully perform the required effort.
Satisfactory Confidence	Based on the offeror's recent and relevant performance record, the government has a reasonable expectation that the offeror will successfully perform the required effort.
Neutral Confidence	No recent or relevant performance record is available or the offeror's performance record is so sparse that no meaningful confidence assessment rating can be reasonably assigned. The offeror may not be evaluated favorably or unfavorably on the factor of past performance.
Limited Confidence	Based on the offeror's recent and relevant performance record, the government has a low expectation that the offeror will successfully perform the required effort.

M.5. Factor 4: Price

The Offeror shall propose a total Firm-Fixed-Price, including a breakdown of all cost elements that make up the total price (e.g., labor breakdown and tasks/deliverables breakdown). The Government will evaluate the Offeror's price proposal in accordance with FAR 15.404-1(b), using applicable price analysis techniques to determine whether the total evaluated price is fair and reasonable. This factor will not receive an adjectival rating but will be evaluated to ensure that the price is reasonable, complete and balanced.
The Government will evaluate the total proposed price, including the base and all option periods, to determine the total evaluated price for award purposes. Evaluation of options does not obligate the Government to exercise any option.

The Government will evaluate price proposals to determine fairness and reasonableness. Prices that are determined to be unreasonably high in relation to the proposed work may result in the overall proposal being considered unacceptable. In terms of "completeness", the Government will consider whether the price covers all the work identified in the SOW and address all items in the Pricing Schedule (Attachment 2, which must be used for evaluation).

The Government will review the Offeror's proposed labor rates, level of effort, staffing pricing, and other elements necessary for program operations to ensure they are accurate and free of apparent errors. The Government will also review all CLIN prices for reasonableness and balance to confirm they reflect an understanding of the requirements and do not contain apparent mistakes. This review is conducted solely to support the Firm-Fixed-Price evaluation and does not constitute a price realism analysis.