SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE 1 OF
	Page 1 of 27 34

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
	07/28/2026		SV0222-26	07/28/2026

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No collect calls)*	8. OFFER DUE DATE/ LOCAL TIME
	Wesley Newell		08/21/2026 2:00 PM

9. ISSUED BY CODE CUM1

CUMBERLAND SIGN
14601 BURBRIDGE RD SE
CUMBERLAND MD 21502-8724

10. THIS ACQUISITION IS

- [ ] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [x] UNRESTRICTED OR
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] EDWOSB
- [ ] 8 (A)
- [ ] SET ASIDE: % FOR:

NAICS: 333248

SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING
[X] SEE SCHEDULE			14. METHOD OF SOLICITATION: [ ] RFQ [ ] IFB [x] RFP

15. DELIVER TO CODE CUM1

CUMBERLAND SIGN
14601 BURBRIDGE RD SE
CUMBERLAND MD 21502-8724

16. ADMINISTERED BY CODE CUM1

CUMBERLAND SIGN
14601 BURBRIDGE RD SE
CUMBERLAND MD 21502-8724

17a. CONTRACTOR/ OFFEROR CODE 391014499 FACILITY CODE

UNDETERMINED SOURCE
NA BLANK
WASHINGTON DC 20534

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE

UNICOR FPI CENTRAL ACCOUNTS PAYABLE
PO BOX 11849
LEXINGTON, KY 40578-1849

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

[ ] 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED — [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	See Section B 1620000386				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA

UNICOR FUNDS 15X4500 FUNDS SHALL BE OBLIGATED BY INDIVIDUAL DELIVERY ORDERS AND NOT BY THE CONTRACT ITSELF

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		Wesley Newell	07/28/2026

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

SV0222-26 Digital License Plate Printer

SAM.gov Solicitation Posting: 08/03/2026
Questions Deadline: 8/11/2026 5PM EST
Proposal Deadline: 8/21/2026 2PM EST

Terms of delivery are f.o.b. origin to:

Unicor, Federal Prison Industries, Inc.
14601 Burbridge Road se
Cumberland, MD 21502

Solicitation is issued as a one-time purchase, firm fixed price procurement.

Questions pertaining to this solicitation will only be addressed in writing via email to: *Wesley.newell2@usdoj.gov*.

For a list, description and total estimated quantities of all items, refer to Section B.

Vendors shall submit signed and dated offers by email to: Wesley.Newell2@usdoj.gov
OMB Clearance 1103-0018.

Offer must indicate Solicitation No. SV0222-26, time specified for receipt of offer, name, address and telephone number of Offeror, technical description of the items being offered in sufficient detail to evaluate compliance with the requirements in the solicitation, terms of any expressed warranty, price and any discount terms. Offer must include acknowledgment of all amendments, if any.

THE FOLLOWING INFORMATION IS REQUIRED TO BE COMPLETED BY THE OFFEROR:

SAM UNIQUE ENTITY NUMBER:_____

VENDOR'S POINT OF CONTACT: _____

VENDOR'S TELEPHONE NUMBER: _____

VENDOR'S EMAIL ADDRESS: _____

VENDOR'S BUSINESS SIZE (i.e. SMALL, LARGE, ETC.): _____

By submission of an offer, the Offeror acknowledges the requirement that a prospective awardee shall be registered in the SAM database (System Award Management) prior to submitting a proposal, during performance and through final payment of any contract resulting from this solicitation.

_____ Signature

The Administrative Contracting officer is Wesley Newell at Wesley.Newell2@usdoj.gov.

SECTION B
SUPPLIES OR SERVICES AND PRICES/COSTS

Item No.	SUPPLIES OR SERVICE	Quantity	U/M	UNIT PRICE	AMOUNT IN US$	Delivery Date
00001	Digital License Plate Printer	1	EA			09/30/2026

The Contractor shall supply a digital license plate printing system consisting of a printer that will either use inkjet technology to print process color UV-curable polymer ink direct to rolls of reflective license plate sheeting or thermal transfer ribbon printing technology. This printer shall be capable of printing the license plate image using the four (4) primary printing ink colors cyan, magenta, yellow & black, along with additional functionality for customizable color. The printer should be capable of printing the license plate images in a continuous indexing print queue. The printer will not be connected to agency network.

The printer shall accommodate license plate sheeting substrates wound on and dispensed from a supply roll and shall be capable of accurately printing:

- Full color license plate graphics at fixed intervals on blank (unprinted) sheeting.
    - High contrast cue marks may be printed as part of the graphic for further processing downstream in a license plate blanking line; and
- Full color license plate graphics registered to pre-printed cue marks; and
- Variable data registered to pre-printed cue marks on preprinted sheeting.

The printer shall accommodate rolls of reflective license plate sheeting wound on diameter cores. The roll of sheeting will be loaded onto a supply spindle with may include an air-actuated expansion mandrel to secure the roll. The printed roll will be automatically rewound onto a core installed on a take-up spindle with an air-actuated expansion mandrel. The printer should contain a connection for compressed air if required to operate these mandrels.

The printer may contain a splice table with pneumatically actuated hold-down clamps for fast roll changes, reduced downtime and minimal material waste.

Software included with this system shall provide image processing, color management, and related graphics functions. The software platform will also include a printer management module, providing printer setup, calibration, maintenance functionality, and the capability to integrate variable data on fixed plate backgrounds to change serial numbers, font, etc.

The software modules to be supplied will also provide the following:

- Database Software
    - Allows for storage of data related plates printed, print jobs in progress, current status, shipping, and orders
    - Feeds variable data to fields in the license plate template.

    - Captures license plate data and content during the production process.
- Data Integration Software
    - Utilize printing templates with fields defined in the database.
    - Build a run list comprising entire print jobs printed by the system.
- RIP Software
    - Provides automated utilities to receive and process order files or run list files
- Print Management Software
    - Print manager that sends the print jobs to the printer.
    - Allows operators to manage and monitor print jobs, get printer status, control printer functions and complete printer maintenance tasks.
    - Windows-based User Interface.

All console software (where a user must be logged in) must be configured and tested for functionality with non-elevated privileges. The software must function without local or network administrator permission unless it runs as a Windows service.

All software should be compatible with the Windows 11 Professional/Enterprise desktop operating system.

All software must function in a “closed” network environment, with no permanent external connectivity required for licensing activation, software functionality, or software updates.

The potential vendor should advise of their capabilities to provide randomized plate number generation and management. Specifically noting the following:

- A randomly generated seven-character format of 1 number followed by 2 letters and 4 numbers. For example, 1AE5634, 9BK7812 etc.

Duplicate prevention

- The system should include functionality to identify potential duplicates prior to printing to prevent duplication across all license plates produced by the system.

External system data synchronization

- The vendor should provide a solution from file/data transfer for synchronization with an external system. This could be done via APIs and/or file exports with batch synchronization.

- The potential vendor should provide information on both capabilities, as the current system is not planned for any external connectivity, and thus batch synchronization may be the only option.

The printer should be capable of printing a combination of background graphics and variable data, in any order, on demand in process color. This capability shall include the printing of variable license plate content: license plate images, text, and barcodes.

Print jobs shall be initiated from the print management component of the software including automated processes and manual print jobs. The print management software will allow users to build, process and manage license plate print jobs as well as to control printer functions, settings and maintenance features. There will be role-based security for controlling user access to different functionalities in the system.

The printer shall be capable of processing and printing a full roll of 12" standard automobile license plate graphics or 7" motorcycle license plates. The system shall have a RIP function where a specified directory can be configured to be monitored for files being placed. This will automate the initiation of the license plate processes. The processing of orders, graphic design, jobs, and tracking should be possible while the printer is printing.

The vendor should list all software and hardware accessories and additional components included in the system, which would have no additional cost beyond what is quoted.

Print jobs may be initiated manually by the operator, or automatically by copying a PDF print file to a hot folder. Multiple print files may be queued for the successive printing of license plate print jobs, including during actual printing.

The system shall be capable of printing at selectable print resolutions of 600 dpi or higher. If the throughput of the printer changes as the resolution is updated, then the potential vendor should specify the throughput at each of the resolution standards.

Installation and Testing

- The submitted proposal shall include a full description of the installation services that will be provided.
- This would include hardware installation, setup, configuration, fine tuning, calibration, and a documented quality control review of the hardware installation after setup and testing.
- This would include software installation, configuration, and testing.
- This would include collaboration with UNICOR staff on testing and troubleshooting during the implementation of computer access restrictions after software functionality has been tested and verified.

Training

- The submitted proposal shall include a description and number of days of operator training to be performed onsite at the Federal Correctional Institution, Cumberland, Maryland. This training shall be conducted with UNICOR staff and the machine/software operators.
- This training shall include the standard operation of the equipment, as well as end user approved maintenance according to manufacturer recommendations.
- This training shall include software installation, configuration, operation, and troubleshooting.
- The proposal package shall also include information regarding the option for additional days of training if desired by UNICOR. The additional onsite training that is quoted could be immediately after the included days have been exhausted, or within 6 months of the initial installation.
    - Note: This will not be an evaluation factor and is for informational purposes only and is not part of this solicitation or award.

Warranty

- The submitted proposal shall include a full description of the warranty, including the terms and conditions, as well as the duration.
- The proposal shall provide an identification and distinction between the manufacturer warranty, any 3rd party warranty offered by the proposer, if any of the terms, conditions, or duration are different.
- Any end user actions that may violate the warranty should also be disclosed.

Support

- The submitted proposal shall include a full description of the customer service support provided. The description would entail:
    - Telephone support provided
    - Onsite support provided
    - Email support provided
    - Standard response time for telephone support
    - Hours that support is available via telephone or email
    - Costs for telephone, onsite, and email support outside of warranty coverage, to include travel labor rates and repair labor rates.

SECTION B:

Unicor is looking to procure:

One (1) digital license plate printer.

The Contractor shall supply a digital license plate printing system consisting of a printer that will either use inkjet technology to print process color UV-curable polymer ink direct to rolls of reflective license plate sheeting or thermal transfer ribbon printing technology. This printer shall be capable of printing the license plate image using the four (4) primary printing ink colors cyan, magenta, yellow & black, along with additional functionality for customizable color. The printer should be capable of printing the license plate images in a continuous indexing print queue. The printer will not be connected to agency network.
The printer shall accommodate license plate sheeting substrates wound on and dispensed from a supply roll and shall be capable of accurately printing:

- Full color license plate graphics at fixed intervals on blank (unprinted) sheeting.
    - High contrast cue marks may be printed as part of the graphic for further processing downstream in a license plate blanking line; and
- Full color license plate graphics registered to pre-printed cue marks; and
- Variable data registered to pre-printed cue marks on preprinted sheeting.

The printer shall accommodate rolls of reflective license plate sheeting wound on diameter cores. The roll of sheeting will be loaded onto a supply spindle with may include an air-actuated expansion mandrel to secure the roll. The printed roll will be automatically rewound onto a core installed on a take-up spindle with an air-actuated expansion mandrel. The printer should contain a connection for compressed air if required to operate these mandrels.
The printer may contain a splice table with pneumatically actuated hold-down clamps for fast roll changes, reduced downtime and minimal material waste.
Software included with this system shall provide image processing, color management, and related graphics functions. The software platform will also include a printer management module, providing printer setup, calibration, maintenance functionality, and the capability to integrate variable data on fixed plate backgrounds to change serial numbers, font, etc.
The software modules to be supplied will also provide the following:

- Database Software
    - Allows for storage of data related plates printed, print jobs in progress, current status, shipping, and orders
    - Feeds variable data to fields in the license plate template.
    - Captures license plate data and content during the production process.
- Data Integration Software
    - Utilize printing templates with fields defined in the database.
    - Build a run list comprising entire print jobs printed by the system.
- RIP Software
    - Provides automated utilities to receive and process order files or run list files
- Print Management Software
    - Print manager that sends the print jobs to the printer.
    - Allows operators to manage and monitor print jobs, get printer status, control printer functions and complete printer maintenance tasks.
    - Windows-based User Interface.

All console software (where a user must be logged in) must be configured and tested for functionality with non-elevated privileges. The software must function without local or network administrator permission unless it runs as a Windows service.
All software should be compatible with the Windows 11 Professional/Enterprise desktop operating system.
All software must function in a "closed" network environment, with no permanent external connectivity required for licensing activation, software functionality, or software updates.
The potential vendor should advise of their capabilities to provide randomized plate number generation and management. Specifically noting the following:

- A randomly generated seven-character format of 1 number followed by 2 letters and 4 numbers. For example, 1AE5634, 9BK7812 etc.

Duplicate prevention

- The system should include functionality to identify potential duplicates prior to printing to prevent duplication across all license plates produced by the system.

External system data synchronization

- The vendor should provide a solution from file/data transfer for synchronization with an external system. This could be done via APIs and/or file exports with batch synchronization.
    - The potential vendor should provide information on both capabilities, as the current system is not planned for any external connectivity, and thus batch synchronization may be the only option.

The printer should be capable of printing a combination of background graphics and variable data, in any order, on demand in process color. This capability shall include the printing of variable license plate content: license plate images, text, and barcodes.
Print jobs shall be initiated from the print management component of the software including automated processes and manual print jobs. The print management software will allow users to build, process and manage license plate print jobs as well as to control printer functions, settings and maintenance features. There will be role-based security for controlling user access to different functionalities in the system.
The printer shall be capable of processing and printing a full roll of 12" standard automobile license plate graphics or 7" motorcycle license plates. The system shall have a RIP function where a specified directory can be configured to be monitored for files being placed. This will automate the initiation of the license plate processes. The processing of orders, graphic design, jobs, and tracking should be possible while the printer is printing.
The vendor should list all software and hardware accessories and additional components included in the system, which would have no additional cost beyond what is quoted.
Print jobs may be initiated manually by the operator, or automatically by copying a PDF print file to a hot folder. Multiple print files may be queued for the successive printing of license plate print jobs, including during actual printing.
The system shall be capable of printing at selectable print resolutions of 600 dpi or higher. If the throughput of the printer changes as the resolution is updated, then the potential vendor should specify the throughput at each of the resolution standards.
Installation and Testing

- The submitted proposal shall include a full description of the installation services that will be provided.
- This would include hardware installation, setup, configuration, fine tuning, calibration, and a documented quality control review of the hardware installation after setup and testing.
- This would include software installation, configuration, and testing.
- This would include collaboration with UNICOR staff on testing and troubleshooting during the implementation of computer access restrictions after software functionality has been tested and verified.

Training

- The submitted proposal shall include a description and number of days of operator training to be performed onsite at the Federal Correctional Institution, Cumberland, Maryland. This training shall be conducted with UNICOR staff and the machine/software operators.
- This training shall include the standard operation of the equipment, as well as end user approved maintenance according to manufacturer recommendations.
- This training shall include software installation, configuration, operation, and troubleshooting.
- The proposal package shall also include information regarding the option for additional days of training if desired by UNICOR. The additional onsite training that is quoted could be immediately after the included days have been exhausted, or within 6 months of the initial installation.

- Note: This will not be an evaluation factor and is for informational purposes only and is not part of this solicitation or award.

Warranty

- The submitted proposal shall include a full description of the warranty, including the terms and conditions, as well as the duration.
- The proposal shall provide an identification and distinction between the manufacturer warranty, any 3rd party warranty offered by the proposer, if any of the terms, conditions, or duration are different.
- Any end user actions that may violate the warranty should also be disclosed.

Support

- The submitted proposal shall include a full description of the customer service support provided. The description would entail:
  - Telephone support provided
  - Onsite support provided
  - Email support provided
  - Standard response time for telephone support
  - Hours that support is available via telephone or email
  - Costs for telephone, onsite, and email support outside of warranty coverage, to include travel labor rates and repair labor rates.

PART I: INFORMATION

This is a combined synopsis/solicitation for commercial items prepared in accordance with the format in Subpart 12.6 as supplemented with additional information included in this notice. This announcement constitutes the only solicitation; offers are being requested and a written solicitation will not be issued. The solicitation number is SV0222-26 and this solicitation is issued as a Request For Quote (RFQ). The North American Industry Classification System code is 333248 Printing Equipment Manufacturing.

The proposed offer and price should be valid for a minimum of 60 days in order to allow proper evaluation before award.

NOTICE TO GOVERNMENT WHEN CONTRACTOR(S) DELAYS:
In the event the contractor(s) encounter difficulty in meeting performance requirements, or when there is an anticipated difficulty in complying with the delivery terms or completion dates, or whenever the contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely delivery/performance of this contract, the contractor must immediately notify the Field Administrative Contracting Officers at UNICOR Cumberland or in writing, giving pertinent details. This information will not be construed as a waiver by the Government of the required delivery schedule, or the Governments rights to impose consideration against delinquencies or other remedies provided by this contract.

INVOICES ARE TO BE EMAILED TO:
Accounts.payable@usdoj.gov

PART II: FAR CLAUSES

52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020)

Alternate I (Nov 2021). As prescribed in 3.503-2 , substitute the following paragraph in place of paragraph (b) of the basic clause:
(b) The prohibition in paragraph (a) of this clause does not preclude the Contractor from asserting rights that are otherwise authorized by law or regulation. For acquisitions of commercial products or commercial services, the prohibition in paragraph (a) applies only to the extent that any agreement restricting sales by subcontractors results in the Federal Government being treated differently from any other prospective purchaser for the sale of the commercial product(s) and commercial service(s).

52.203-17, Contractor Employee Whistleblower Rights (Nov 2023)
52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements. (Jan 2017)
52.209-6, Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded. (July 2026)
52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (July 2026)
52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (July 2026)
52.212-4, Contract Terms and Conditions - Commercial Products And Commercial Services (NOV 2023).
52.219-4, Notice of Price Evaluation preference for HUBZone Small Business Concerns (July 2026)
52.219-8, Utilization of Small Business Concerns (July 2026)
52.219-9, Small Business Subcontracting Plan (July 2026)
52.219-16, Liquidated Damages-Subcontracting Plan (July 2026)
52.222-3, Convict Labor (July 2026)

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

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

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

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

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

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

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

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

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

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

(End of clause)

52.222-19, Child Labor-Cooperation with Authorities and Remedies (Deviation Date)
52.222-35 Equal Opportunity for Veterans.

Equal Opportunity for Veterans

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

"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran," and "recently separated veteran" have the meanings given at Federal Acquisition Regulation (FAR) 22.1301.

(b) Equal opportunity requirements. The Contractor must abide by the requirements of 38 U.S.C. 4212(a)(1) and (2). These requirements prohibit discrimination against qualified protected veterans and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor must insert the terms of this clause in subcontracts valued at or above the threshold specified in FAR 22.1302-1(a)(2) on the date of subcontract award, unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor must act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

(End of clause)

52.222-36, Equal Opportunity for Workers with Disabilities (July 2026)
52.222-37, Employment Reports on Veterans (July 2026)
52.222-40, Notification of Employee Rights Under the National Labor Relations Act (July 2026)
52.222-50, Combating Trafficking in Persons (July 2026)
52.222-90, Addressing DEI Discrimination by Federal Contractors (July 2026)
52.223-23, Sustainable Products (July 2026)

52.225-5, Trade Agreements (July 2026)

52.225-6, Trade Agreement Certificate (July 2026)

52.226-8, Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024)

52.229-11, Tax on Certain Foreign Procurements – Notice and Representation (July 2026)

52.229-12, Tax on Certain Foreign Procurements (July 2026)

52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct 2018)

52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023)

52.233-3 Protest After Award (July 2026)

52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004)
52.240-91, Security Prohibitions and Exclusions (July 2026)
52.240-93, Basic Safeguarding of Covered Contractor Information Systems (July 2026)
52.244-6, Subcontracts for Commercial Products and Commercial Services (July 2026)
52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (July 2026)
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):

52.252-6, Authorized Deviation in Clauses (NOV 2020).

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Local Level Economic Price Adjustment clause (48 CFR Chapter 16) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation. (END OF CLAUSE)

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.[1] Applicable SORNs published by other agencies may be accessed through those agencies' websites or by searching the Federal Digital System (FDsys) available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

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

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

information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of remote work authorizations.

(3) Prior Approval Required to Hire Subcontractors

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

(4) Separation Checklist for Contractor Employees

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

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

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

[1] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4). "[T]he term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

B. Privacy Training, Safeguarding, and Remediation

(1) Required Security and Privacy Training for Contractors

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

available to all new users of DOJ's computer network and to trainees at the conclusion of DOJ-OPCL-CS-0005.

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

(2) Safeguarding PII Requirements

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

(3) Non-Disclosure Agreement Requirement

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

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

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

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

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

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

administration of the contract in the invoices as needed.

(5) Reporting Actual or Suspected Data Breach

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

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

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

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

i. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.[6] Date, time, and location of the incident.
ii. Amount, type, and sensitivity of information that may have been lost or compromised, accessed without authorization, etc.
iii. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.[7]

iv. Names and classification of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
v. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.[8]
vi. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
vii. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

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

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

(6) Victim Remediation

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

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

a) The Contractor must ensure that all employees and Subcontractors that have access to PII as well as to those involved in the creation, use, dissemination and/or destruction of PII take the *DOJ Records and Information Training for New Employees (RIM)* training course or another training approved by the Contracting Officer or COR. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. The

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

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

(2) Records Creation, Ownership, and Disposition

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

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

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

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

D. Data Privacy and Oversight

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

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

(2) Requirements for Contractor IT Systems Hosting Government Data

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

(3) Requirement to Support Privacy Compliance

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

requirements and format for the PIA.

b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy risk assessment and documentation, the Contractor shall provide adequate support to DOJ to ensure DOJ can complete any required assessment, and IPA, PIA, SORN, or other supporting documentation to support privacy compliance. The Contractor shall work with

personnel from the program office, OPCL, the Office of the Chief Information Officer (OCIO), and the Office of Records Management and Policy to ensure that the privacy assessments and documentation are kept on schedule, that the answers to questions in the documents are thorough and complete, and that questions asked by the OPCL and other offices are answered in a timely fashion. The Contractor must ensure the completion of required PIAs and documentation of privacy controls consistent with federal law and standards, e.g. NIST 800-53, Rev. 5; and compliance with the Privacy Act of 1974, E-Government Act of 2002, Federal Information Security Modernization Act of 2014, and key OMB guidelines, e.g., OMB Circular A-130.

(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.

U.S. Department of Justice Departmental Provisions and Clauses
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.

U.S. Department of Justice Departmental Provisions and Clauses

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.
U.S. Department of Justice Departmental Provisions and Clauses
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).
U.S. Department of Justice Departmental Provisions and Clauses
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.
U.S. Department of Justice Departmental Provisions and Clauses
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

U.S. Department of Justice Departmental Provisions and Clauses

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

U.S. Department of Justice Departmental Provisions and Clauses

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)
2852.233-70 PROTESTS FILED DIRECTLY WITH THE DEPARTMENT OF JUSTICE (JAN 1998)
(a) The following definitions apply in this provision:
(1) "Agency Protest Official" means the official, other than the contracting officer, designated to review and decide procurement protests filed with a contracting activity of the Department of Justice.
(2) "Deciding Official" means the person chosen by the protestor to decide the agency protest; it may be either the Contracting Officer or the Agency Protest 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) A protest filed directly with the Department of Justice must:
(1) Indicate that it is a protest to the agency.
(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.
(c) An interested party filing a protest with the Department of Justice has the choice of requesting either that the Contracting Officer or the Agency Protest Official decide the protest.
(d) The decision by the Agency Protest Official is an alternative to a decision by the Contracting Officer. The Agency Protest Official will not consider appeals from the Contracting Officer's decision on an agency protest.
(e) The deciding official must conduct a scheduling conference with the protestor within five (5) days after the protest is filed. The scheduling conference 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.
(f) Oral conferences may take place either by telephone or in person. Other parties may attend at the discretion of the deciding official.

(g) The protestor has only one opportunity to support or explain the substance of its protest. Department of Justice procedures do not provide for any discovery. The deciding official may request additional information from either the agency or the protestor. The deciding official will resolve the protest through informal presentations or meetings to the maximum extent practicable.
(h) An interested party may represent itself or be represented by legal counsel. The Department of Justice will not reimburse the protester for any legal fees related to the agency protest.
(i) The Department of Justice will stay award or suspend contract performance in accordance with FAR 33.103(f). The stay or suspension, unless over-ridden, remains in effect until the protest is decided, dismissed, or withdrawn.
(j) The deciding official will make a best effort to issue a decision on the protest within twenty (20) days after the filing date. The decision may be oral or written.
(k) The Department of Justice may dismiss or stay proceeding on an agency protest if a protest on the same or similar basis is filed with a protest forum outside the Department of Justice.*]*

JAR 2852.201-70 CONTRACTING OFFICER'S REPRESENTATIVE (COR) (JAN 1985)
(a) Michael Southern, telephone 301-784-1000 is hereby designated to act as Contracting Officer's Representative (COR) under this contract.

(b) The COR is responsible, as applicable, for: receiving all deliverables, inspecting and accepting the supplies or services provided hereunder in accordance with the terms and conditions of this contract; providing direction to the contractor which clarifies the contract effort fills in details or otherwise serves to accomplish the contractual Scope of Work; evaluating performance; and certifying all invoices/vouchers for acceptance of the supplies or services furnished for payments.

(c) The COR does not have the authority to alter the contractor's obligations under the contract, and/or modify any of the expressed terms, conditions, specifications, or cost of the agreement. If as a result of technical discussions, it is desirable to alter/change contractual obligations or the Scope of Work, the Contracting Officer shall issue such changes in writing and signed.

PART III: PROVISIONS

52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions (July 2026)

52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation (July 2026)

52.204-7, System for Award Management (Nov 2024)

52.212-1, Instructions to Offerors – Commercial Products and Commercial Services (Sept 2023).

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

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

Meets technical specifications, price, past performance, and delivery time.

Technical and *past performance*, when combined, are: *More important than price.*

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

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

(END OF PROVISION)

52.215-6, Place of Performance (OCT 1997)

(a) The Offeror or respondent, in the performance of any contract resulting from this solicitation, o intends, o 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
_____	_____
_____	_____

52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products (July 2026)
52.240-90, Security Prohibitions and Exclusions Representations and Certifications (July 2026)

52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The Offeror is cautioned that the listed provisions may include blocks that must be completed by the Offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the Offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at www.acquisition.gov.

PART IV: PROPOSAL SUBMISSION REQUIREMENTS

Each proposal package shall consist of the following completed and signed documents: SF1449, all amendments issued, three Business Management Questionnaires of recent and relevant contracts for the same or similar items in accordance with FAR 52.212-1(b)(10) for past performance evaluation.

Any amendments issued to this solicitation shall be synopsized in the same manner as this solicitation and must be acknowledged by each Offeror. Offeror must hold prices firm for 60 calendar days from the date specified for receipt of offers. Offers or modifications to offers received at the address specified for the receipt of offers after the exact time specified may not be considered.

Questions regarding this requirement may be addressed in writing to Wesley Newell, at Wesley.Newell2@usdoj.gov. All FAR forms, clauses and provisions necessary to submit an offer may be accessed at the following web site: http://acquisition.gov/far. This combined synopsis/solicitation and necessary forms are available on web site: http://www.SAM.gov.