

The provisions and clauses are in accordance with FAR Part 12 and FAR Class Deviation 25-21 for FAR Part 12 in Support of Executive Order on Restoring Common Sense to Federal Procurement.

The full text of any provision, clause or deviation may be accessed electronically at this/these address(es): [FAR Overhaul - Part 52 | Acquisition.GOV](#)

Please note, DHS Deviations may be applicable to any/all clauses, please verify at: [FAR Overhaul - FAR Part Deviation Guidance | Acquisition.GOV](#)

To locate a deviation, navigate to the specific FAR Part in question and review the corresponding Department of Homeland Security (DHS) deviation section for that Part, where all active deviations are identified and maintained.

## FAR PROVISIONS

### 52.252-1 Solicitation Provisions Incorporated by Reference.

As prescribed in 52.107(a), insert the following provision:

#### Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): [FAR Overhaul - Part 52 | Acquisition.GOV](#).

(End of provision)

| FAR Provisions |                                                                                                                                            |               |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <u>Number</u>  | <u>Title</u>                                                                                                                               | <u>Source</u> |
| 52.203-18      | Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation             | Statute       |
| 52.204-7       | System for Award Management—Registration                                                                                                   | Statute       |
| 52.209-11      | Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law                             | Statute       |
| 52.212-1       | Instructions to Offerors—Commercial Products and Commercial Service                                                                        | Statute       |
| 52.212-2       | Evaluation—Commercial Products and Commercial Services                                                                                     | Statute       |
| 52.217-4       | Evaluation of Options Exercised at Time of Contract Award                                                                                  | Statute       |
| 52.217-5       | Evaluation of Options                                                                                                                      | Statute       |
| 52.219-1       | Small Business Program Representations                                                                                                     | Statute       |
| 52.222-56      | Certification Regarding Trafficking in Persons Compliance Plan                                                                             | Statute       |
| 52.225-25      | Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran-Representation and Certifications | Statute       |

Attachment 2 – Open Market FAR & HSAR Provisions & Clauses  
Kearneysville Commercial Internet Services  
Solicitation # 52800PR2632674

|           |                                                                         |         |
|-----------|-------------------------------------------------------------------------|---------|
| 52.232-32 | Invitation to Propose Financing Terms                                   | Statute |
| 52.240-90 | Security Prohibitions and Exclusions Representations and Certifications | Statute |
| 52.252-5  | Authorized Deviations in Provisions                                     | Statute |

## FAR CLAUSES

### 52.252-2 Clauses Incorporated by Reference.

As prescribed in 52.107(b), insert the following clause:

#### 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): [FAR Overhaul – Part 52 | Acquisition.GOV](#).

(End of clause)

| FAR Clauses   |                                                                                                                          |               |
|---------------|--------------------------------------------------------------------------------------------------------------------------|---------------|
| <u>Number</u> | <u>Title</u>                                                                                                             | <u>Source</u> |
| 52.203-19     | Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements                                       | Statute       |
| 52.204-13     | System for Award Management—Maintenance                                                                                  | Statute       |
| 52.209-6      | Protecting the Government’s Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment | Statute       |
| 52.209-10     | Prohibition on Contracting with Inverted Domestic Corporations                                                           | Statute       |
| 52.217-9      | Option to Extend the Term of the Contract                                                                                | Statute       |
| 52.222-3      | Convict Labor                                                                                                            | EO            |
| 52.222-19     | Child Labor—Cooperation with Authorities and Remedies                                                                    | EO            |
| 52.222-50     | Combating Trafficking in Persons                                                                                         | Statute       |
| 52.222-90     | Addressing DEI Discrimination by Federal Contractors                                                                     | EO            |
| 52.223-23     | Sustainable Products and Services                                                                                        | Statute       |
| 52.224-3      | Privacy Training                                                                                                         | Statute       |
| 52.225-1      | Buy American-Supplies                                                                                                    | Statute       |
| 52.226-8      | Encouraging Contractor Policies to Ban Text Messaging While Driving                                                      | EO            |
| 52.232-18     | Availability of Funds                                                                                                    | Statute       |
| 52.232-29     | Terms for Financing of Commercial Products and Commercial Services                                                       | Statute       |
| 52.232-33     | Payment by Electronic Funds Transfer—System for Award Management                                                         | Statute       |
| 52.232-39     | Unenforceability of Unauthorized Obligations                                                                             | Statute       |
| 52.232-40     | Providing Accelerated Payments to Small Business Subcontractors                                                          | Statute       |
| 52.233-3      | Protest After Award                                                                                                      | Statute       |
| 52.233-4      | Applicable Law for Breach of Contract Claim                                                                              | Statute       |

Attachment 2 – Open Market FAR & HSAR Provisions & Clauses  
Kearneysville Commercial Internet Services  
Solicitation # 52800PR2632674

|           |                                      |         |
|-----------|--------------------------------------|---------|
| 52.240-91 | Security Prohibitions and Exclusions | Statute |
| 52.252-6  | Authorized Deviations in Clauses     | Statute |

**52.212-4 Terms and Conditions—Commercial Products and Commercial Services.**

As prescribed in 12.205(b)(3), insert the following clause:

**Terms and Conditions—Commercial Products and Commercial Services (Deviation Date)**

(a) Definitions. The clause at Federal Acquisition Regulation (FAR) 52.202-1, Definitions, is incorporated by reference.

(b) Inspection/Acceptance. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post acceptance rights—

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

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

(c) Assignment. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(d) Changes. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(e) Disputes. This contract is subject to 41 U.S.C. chapter 71, Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal, or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause FAR 52.233-1, Disputes, which is incorporated in this contract by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(f) Excusable delays. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence. Examples of occurrences include acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. When an excusable delay occurs, the Contractor shall—

(1) Notify the Contracting Officer in writing as soon as possible;

(2) Remedy the delay as quickly as possible; and

(3) Notify the Contracting Officer when the occurrence is over.

(g) Invoice. The Government will handle invoices according to the Prompt Payment Act (31 U.S.C. 3903) and 5 CFR part 1315. The Contractor shall submit invoices to the address designated in the contract to receive invoices. An invoice must include the information required by 5 CFR part 1315.9(b).

(h) Patent indemnity. The Contractor shall indemnify the Government and its officers, employees, and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark, or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payment—

(1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) Prompt payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(3) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date that appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(4) Overpayments. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall—

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected line item or subline item, if applicable;

(D) Contractor point of contact; and

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(5) Interest.(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this

clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) Final decisions. The Contracting Officer will issue a final decision as required by FAR part 33 if—

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see FAR part 32).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a termination for cause.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on—

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures for interest credits prescribed in FAR part 32 in effect on the date of this contract.

(j) Risk of loss. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon—

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) Taxes. The contract price includes all applicable Federal, State, and local taxes and duties.

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

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

(n) Title. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

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

(p) Limitation of liability. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) Compliance with laws unique to Government contracts. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 49 U.S.C. 40118, Government-financed air transportation; and 41 U.S.C. chapter 21 relating to procurement integrity.

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

(1) The schedule of supplies/services;

(2) The Disputes, Payments, Invoice, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause;

(3) Other contract clauses incorporated in the solicitation or contract;

(4) Addenda to this solicitation or contract;

(5) Solicitation provisions incorporated in the solicitation;

(6) Other paragraphs of this clause;

(7) Other documents, exhibits, and attachments; and

(8) The specification.

(s) Unauthorized obligations.

(1) Except as stated in paragraph (s)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such clause is unenforceable against the Government.

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

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

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

(t) Comptroller General examination of record. This paragraph applies if this contract was awarded using other than sealed bid procedures and is in excess of the simplified acquisition threshold on the date of award of this contract.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor’s directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices, at all reasonable times, the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR part 4, longer period required by statute, or periods specified in other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of

claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This clause does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(u) Incorporation by reference. The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

**52.217-9 Option to Extend the Term of the Contract.**

As prescribed in 17.208(g), insert a clause substantially the same as the following:

Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

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

(End of clause)

**52.222-90 Addressing DEI Discrimination by Federal Contractors.**

As prescribed in 22.2203, insert the following clause:

Addressing DEI Discrimination by Federal Contractors

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

*Program participation* means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

*Racially discriminatory diversity, equity, and inclusion (DEI) activities* means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or allocation or deployment of an entity's resources.

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

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

- (2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;
- (3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;
- (4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and
- (5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.
- (6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).
- (c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of clause)

**52.224-3 Privacy Training.**

As prescribed in 24.302 , insert the following clause:

Privacy Training (Jan 2017)

- (a) Definition. As used in this clause, "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource).
- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who-
  - (1) Have access to a system of records;
  - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
  - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.3 and 39.105).
- (c) (1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-

- (i) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;
  - (ii) The appropriate handling and safeguarding of personally identifiable information;
  - (iii) The authorized and official use of a system of records or any other personally identifiable information;
  - (iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information;
  - (v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and
  - (vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).
- (2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
- (f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will-
- (1) Have access to a system of records;
  - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
  - (3) Design, develop, maintain, or operate a system of records.

*(End of clause)*

#### **52.224-3 Privacy Training – Alternate I (DEVIATION)**

- (a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource).

- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—
  - (1) Have access to a system of records;
  - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
  - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.3 ).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
- (f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—
  - (1) Have access to a system of records;
  - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
  - (3) Design, develop, maintain, or operate a system of records.

(End of clause)

**52.232-18 Availability of Funds.**

As prescribed in 32.706-1(a), insert the following clause:

**Availability of Funds (Apr 1984)**

Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

### FAR DEVIATIONS

The DHS FAR Class Deviations below have been identified and will flow down to the resultant order.

| <b><u>Number</u></b> | <b><u>Deviation Reference</u></b>                                                                                                    | <b><u>P/C</u></b> |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| 52.204-7             | System for November Award Management (AUG 2025) (DEVIATION 25-19), (effective 28, 2025)                                              | P                 |
| 52.212-1             | Instructions to Offerors—Commercial Products and Commercial Services (Aug 2025) (DEVIATION 25-21) (effective November 28, 2025)      | P                 |
| 52.212-2             | Evaluation—Commercial Products and Commercial Services (Aug 2025) (DEVIATION 25-21) (effective November 28, 2025)                    | P                 |
| 52.219-1             | Small Business Program Representations (OCT 2025) (DEVIATION 26-03)                                                                  | P                 |
| 52.222-56            | CERTIFICATION REGARDING TRAFFICKING IN PERSONS COMPLIANCE PLAN (OCT 2020)                                                            | P                 |
| 52.240-90            | Security Prohibitions and Exclusions Representations and Certifications (AUG 2025) (DEVIATION 25-23) (effective November 28, 2025)   | P                 |
| 52.204-13            | System for Award Management Maintenance. (AUG 2025) (DEVIATION 25-19), (effective November 28, 2025)                                 | C                 |
| 52.204-13 ALT I      | <i>Alternate I</i> (AUG 2025) (DEVIATION 25-19) (effective November 28, 2025).                                                       | C                 |
| 52.204-19            | Incorporation by Reference of Representations and Certifications (DEC 2014) (effective November 28, 2025)                            | C                 |
| 52.212-4             | Contract Terms and Conditions—Commercial Products and Commercial Services (Aug 2025) (DEVIATION 25-21) (effective November 28, 2025) | C                 |
| 52.219-28            | Postaward Small Business Program Rerepresentation (OCT 2025) (DEVIATION 26-03) (effective November 28, 2025)                         | C                 |
| 52.222-19            | CHILD LABOR-COOPERATION WITH AUTHORITIES AND REMEDIES (OCT 2025) (DEVIATION 26-10) (EFFECTIVE NOVEMBER 28, 2025)                     | C                 |
| 52.222-3             | CONVICT LABOR (JUNE 2003)                                                                                                            | C                 |
| 52.222-50            | COMBATING TRAFFICKING IN PERSONS (NOV 2021)                                                                                          | C                 |
| 52.222-50            | <i>Alternate I</i> (Oct 2025) (Deviation 26-10) (effective November 28, 2025).                                                       | C                 |
| 52.224-3             | <i>Privacy Training – Alternate I (DEVIATION)</i>                                                                                    | C                 |
| 52.232-40            | Providing Accelerated Payments to Small Business Subcontractors                                                                      | C                 |
| 52.233-3             | Protest after Award (AUG 2025) (DEVIATION 25-25) (effective November 28, 2025)                                                       | C                 |
| 52.233-4             | Applicable Law for Breach of Contract Claim (AUG 2025) (DEVIATION 25-25), (effective November 28, 2025)                              | C                 |
| 52.240-91            | Security Prohibitions and Exclusions (AUG 2025) (DEVIATION 25-23) (effective November 28, 2025)                                      | C                 |

|           |                                                                         |   |
|-----------|-------------------------------------------------------------------------|---|
| 52.240-91 | Alternate I (AUG 2025) (DEVIATION 25-23) (effective November 28, 2025). | C |
|-----------|-------------------------------------------------------------------------|---|

**FAR Class Deviation 25-01** applies to all [solicitations and contracts](#) to implement Executive Order (E.O.) 14173, Ending Illegal Discrimination and Restoring Merit-Based Opportunity, and E.O. 14168, Defending Women From Gender Ideology Extremism and Restoring Biological Truth to the Federal Government. This class deviation supersedes Acquisition Alert 25-06, Revoked: E.O. 11246, Equal Opportunity Employment.

The following provisions and clauses **SHALL NOT** be included:

- 52.222-9, Apprentices and Trainees
- 52.222-21, Prohibition of Segregated Facilities
- 52.222-22, Previous Contracts and Compliance Reports
- 52.222-23, Notice of Requirement for Affirmative Action to Ensure Equal Employment Opportunity for Construction
- 52.222-24, Preaward On-Site Equal Opportunity Compliance Evaluation
- 52.222-25, Affirmative Action Compliance
- 52.222-26, Equal Opportunity
- 52.222-27, Affirmative Action Compliance Requirements for Construction
- 52.222-29, Notification of Visa Denial

The following provisions and clauses **SHALL** be included, if applicable:

- 52.204-8, Annual Representations and Certifications (JAN 2025) (DEVIATION FEB 2025)
- 52.222-6, Construction Wage Rate Requirements (AUG 2018) (DEVIATION FEB 2025)
- 52.222-11, Subcontracts (Labor Standards) (MAY 2014) (DEVIATION FEB 2025)
- 52.222-12, Contract Termination—Debarment (MAY 2014) (DEVIATION FEB 2025)
- 52.244-6, Subcontracts for Commercial Products and Commercial Services (JAN 2025) (DEVIATION FEB 2025)

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations. Examples include 52.222-25, Affirmative Action Compliance, and paragraph (d) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services. Additional examples include 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services, and 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services).

Contracting officers **will not consider** the following representations when making award decisions or enforce requirements:

- Paragraph (d) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services;
- Paragraphs (b)(33), (b)(34), (e)(1)(ix), and (e)(1)(x) of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services;
- Paragraphs (e)(1)(ii)(I) and (e)(1)(ii)(J) of Alternate II of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services; and
- Paragraphs (a)(1)(vii) and (a)(1)(viii) of 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services).

Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

**FAR Class Deviation 25-02** waives the FAR requirement to use project labor agreements for large-scale construction projects.

**FAR Class Deviation 25-03** addresses contracting officer actions to implement E.O. 14148 Initial Rescissions of Harmful Executive Orders and Action and E.O.14208 Ending Procurement and Forced Use of Paper Straws.

The following provisions and clauses **SHALL NOT** be included:

- 52.204-8 Annual Representations and Certifications (JAN 2025)
- 52.223-1 Biobased Product Certification (MAY 2024)
- 52.223-2 Reporting of Biobased Products Under Service and Construction Contracts (MAY 2024)
- 52.223-10 Waste Reduction Program (MAY 2024)
- 52.223-19, Compliance with Environmental Management Systems (MAY 2011)
- 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation (DEC 2016)
- 52.223-23, Sustainable Products and Services (MAY 2024)

The following provisions and clauses **SHALL** be included, if applicable:

- 52.204-8 Annual Representations and Certifications (JAN 2025) (DEVIATION FEB 2025)
- 52.223-1 Biobased Product Certification (MAY 2024) (DEVIATION FEB 2025)

- 52.223-2 Reporting of Biobased Products Under Service and Construction Contracts (MAY 2024) (DEVIATION FEB 2025)
- 52.223-10 Waste Reduction Program (MAY 2024) (DEVIATION FEB 2025)
- 52.223-23, Sustainable Products and Services (MAY 2024) (DEVIATION FEB 2025)

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations, including 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation, and paragraph (t) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services. Components shall not consider or use these representations.

Contracting officers **will not consider** the following representations when making award decisions or enforce requirements:

- Paragraph (d) and (t) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services;
- Paragraphs (b)(33), (b)(34), (e)(1)(ix), and (e)(1)(x) of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services. **Additionally, per this deviation, in paragraph (b)(46), E.O. 14057 does not apply;**
- Paragraphs (e)(1)(ii)(I) and (e)(1)(ii)(J) of Alternate II of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services; and
- Paragraphs (a)(1)(vii) and (a)(1)(viii) of 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services). **Additionally, per this deviation, in paragraph (b)(1)(xvii), E.O. 14057 does not apply.**

Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

#### **HSAR Clauses:**

##### **3052.240-71 Contractor employee access.**

As prescribed in (HSAR) 48 CFR 3040.370-4(a), insert the following clause with appropriate alternates:

**CONTRACTOR EMPLOYEE ACCESS (JULY 2023)**  
**(HSAR DEVIATION 25-12) (effective November 3, 2025)**

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or

dissemination controls. This definition includes the following CUI categories and subcategories of information:

- (1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical Facility Anti-Terrorism Standards,” and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual “Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information” dated September 2008);
- (2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII’s implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;
- (3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, “Protection of Sensitive Security Information,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, “Sensitive Security Information (SSI)” and, within the Transportation Security Administration, TSA MD 2810.1, “SSI Program”;
- (4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;
- (5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;
- (6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;
- (7) Information Systems Vulnerability Information (ISVI) means:
  - (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise

architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to 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; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

- (A) Truncated SSN (such as last 4 digits);
- (B) Date of birth (month, day, and year);
- (C) Citizenship or immigration status;
- (D) Ethnic or religious affiliation;

- (E) Sexual orientation;
- (F) Criminal history;
- (G) Medical information; and
- (H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(End of clause)

ALTERNATE II  
(JULY 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident

Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

**3052.240-72 Safeguarding of Controlled Unclassified Information.**

As prescribed in (HSAR) 48 CFR 3040.370-4(b), insert the following clause:

**SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)  
(HSAR DEVIATION 25-12) (effective November 3, 2025)**

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

*Adequate Security* means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

*Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116-283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to 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; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

- (A) Truncated SSN (such as last 4 digits);
- (B) Date of birth (month, day, and year);
- (C) Citizenship or immigration status;
- (D) Ethnic or religious affiliation;
- (E) Sexual orientation;
- (F) Criminal history;
- (G) Medical information; and
- (H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

*Federal information* means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

*Federal information system* means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

*Handling* means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

*Incident* means an occurrence that—

- (1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- (2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

*Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

*Information Security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

- (1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (3) Availability, which means ensuring timely and reliable access to and use of information.

*Information System* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

*(b) Handling of Controlled Unclassified Information.*

- (1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>.
- (2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.
- (3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.
- (4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

*(c) Incident Reporting Requirements.*

- (1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Subcontractors are

required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Unique Entity Identifier (UEI);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
- (v) Contracting Officer POC (address, telephone, and email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms, or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the government PII or SPII contained within the system; and
- (xiii) Any additional information relevant to the incident.

*(d) Incident Response Requirements.*

- (1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.
- (2) 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 incidents.
- (3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
  - (i) Inspections;
  - (ii) Investigations;
  - (iii) Forensic reviews;
  - (iv) Data analyses and processing; and
  - (v) Revocation of the Authority to Operate (ATO), if applicable.
- (4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.
- (5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

*(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information.*

Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

*(f) Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

*(g) Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user’s responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer’s Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(End of clause)