AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 9

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00003	See Block 16C		

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
DETENTION COMPLIANCE AND REMOVALS ICE Office of Acquisition Management 500 12th St SW WASHINGTON DC 20024	70CDCR	ICE/Detention Compliance & Removals ICE Office of Acquisition Management 500 12th St SW Washington DC 20024	ICE/DCR

8. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

GEO GROUP INC THE
ATTN [redacted]
4955 TECHNOLOGY WAY
BOCA RATON FL 334313367

CODE JMLKZZ1NL2Z6 FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

X 10A. MODIFICATION OF CONTRACT/ORDER NO. 70CDCR25D00000009

10B. DATED *(SEE ITEM 13)* 03/18/2025

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended , by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted ; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted , such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation data, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D. OTHER *(Specify type of modification and authority)* FAR 52.216-25 - Contract Definitization

E. IMPORTANT: Contractor ☒ is not ☐ is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION *(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

UEI: JMLKZZ1NL2Z6

Contracting Officer's Representative (COR)

[redacted]

Contracting Officer

[redacted]

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*	16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*
[redacted], Executive Vice President	[redacted]
15B. [redacted] sign)	15C. DATE SIGNED 11/21/2025
Prev	16C. DATE SIGNED 11/21/2025

STANDARD FORM 30 (REV. 11/2016)
Prescribed by GSA FAR (48 CFR) 53.243

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Contract Specialist [redacted] The purpose of this modification is the following: 1) Update Attachment 01: Performance Work Statement (PWS) including updating the standards to National Detention Standards (NDS) 2025 2) Update Attachment 03: North Lake Staffing Plan 1800 3) Add the level of effort associated with the case processing specialists required per PWS Section 1.9. 4) Incorporate Dept of Labor wage determinations for Detroit and Grand Rapids Attachments 06B and 06C All services shall be performance in accordance with the terms and conditions of this IDIQ as the following attachments Attachments to this IDIQ include: Attachment 1: Performance Work Statement (PWS) Attachment 2: Anticipated Transportation Routes Attachment 3: Staffing Plan Attachment 4: Detention Services Cost Statement (DSCS) Attachment 5: Quality Assurance Surveillance Plan (QASP) Attachment 5A: CDR Template Attachment 6: Wage Determination 2015-4881 rev 29 Attachment 7: Detention-Transportation Template - unlocked* Attachment 8: G-391 Upload Template Attachment 8A: G-391 Data Collection Categories and Descriptions Attachment 9: Prison Rape Elimination Act Regulations Attachment 10: Personal Property Operations Handbook, February 2019 Attachment 11: Virtual Attorney Visitation Attachment 12: ICE Firearms and Use of Force Handbook (by reference - contains law enforcement sensitive information) Attachment 13: Contract Detention Facility Design Standards Attachment 14: EOIR Design Standards Continued ...				

NAME OF OFFEROR OR CONTRACTOR
GEO GROUP INC THE

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Attachment 15: IHSC Design Standard, June 2023 Attachment 16: Structured Cable Plant Standard, January 2025 Attachment 17: Small Business Subcontracting Plan The total value of this IDIQ does not change, remaining [redacted] Period of Performance: 03/18/2025 to 07/20/2027 Change Item 0004 to read as follows(amount shown is the total amount):				
0004	Monthly Transportation Services 07/21/2025 - 11/20/2025: [redacted]month 11/21/2025 - 07/20/2026: [redacted]month Based on an estimated [redacted] miles annually (Attachment 02) Firm Fixed Price Period of Performance: 07/21/2025 - 07/20/2026 Obligated Amount: $0.00 Product/Service Code: S206 Product/Service Description: HOUSEKEEPING- GUARD Change Item 0006 to read as follows(amount shown is the total amount):				[redacted]
0006	Services associated with undefinitized contract action. These services were performed prior to definitization in accordance with the base IDIQ award as well as modification P00001. The total ceiling value of these services was [redacted] at award. Actual costs of these services are captured in task order 70CDCR25FR0000037. The total ceiling value of this CLIN decreases: From: [redacted] By: [redacted] To: [redacted] Period of Performance: 03/18/2025 - 07/20/2025 Obligated Amount: $0.00 Continued ...				[redacted]

NAME OF OFFEROR OR CONTRACTOR
GEO GROUP INC THE

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Code: S206 Product/Service Description: HOUSEKEEPING- GUARD Add Item 0007 as follows:				
0007	Case Processing Specialists - [redacted] FTE North Lake: [redacted] CPS - [redacted] hr regular pay & [redacted] Overtime (OT) [redacted] Supervisor - [redacted] hr regular pay & [redacted] OT Grand Rapids: [redacted] CPS [redacted] hr regular pay & [redacted] OT [redacted] Supervisor [redacted] hr regular pay [redacted] OT Detroit: [redacted] CPS - [redacted] hr regular pay & [redacted] OT [redacted] Supervisor - [redacted] hr regular pay & [redacted] OT Total Estimated Value of this CLIN is [redacted] Period of Performance: 11/21/2025 - 07/20/2026 Obligated Amount: $0.00 Product/Service Code: S206 Product/Service Description: HOUSEKEEPING- GUARD Change Item 1004 to read as follows(amount shown is the total amount):				[redacted]
1004	Monthly Transportation Services - [redacted] onth Based on an estimated [redacted] miles annually (Attachment 02) Firm Fixed Price Period of Performance: 07/21/2026 - 07/20/2027 Obligated Amount: $0.00 Product/Service Code: S206 Product/Service Description: HOUSEKEEPING- GUARD Add Item 1006 as follows:				[redacted]
1006	Case Processing Specialists - [redacted] FTE North Lake: Continued ...				[redacted]

NAME OF OFFEROR OR CONTRACTOR
GEO GROUP INC THE

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	[redacted] CPS - [redacted]hr regular pay & [redacted] OT [redacted] Supervisor - [redacted]hr regular pay &[redacted] OT Grand Rapids: [redacted] CPS - [redacted]hr regular pay & [redacted]OT [redacted] Supervisor - [redacted]hr regular pay & [redacted] OT Detroit: [redacted] CPS - [redacted]hr regular pay & [redacted] OT [redacted] Supervisor - [redacted]hr regular pay & [redacted] OT Total Estimated Value of this CLIN is [redacted] Period of Performance: 07/21/2026 - 07/20/2027 Obligated Amount: $0.00 Product/Service Code: S206 Product/Service Description: HOUSEKEEPING- GUARD :::: :::: :::: :::: :::: There shall be no public disclosures regarding this agreement made by the Service Provider (or any subcontractors) without review and approval of such disclosure by ICE. Notwithstanding the period of performance indicated above, the funding provided in this award is the amount presently available for payment and allotted for this indefinite delivery indefinite quantity (IDIQ) contract. The service provider agrees to perform to the point that does not exceed the total amount currently allotted to the items currently funded under this IDIQ. The service provider is not authorized to continue to work on those item(s) beyond that point. The Government will not be obligated to reimburse the service provider in excess of the amount allotted to those item(s) for performance beyond the funding allotted. ERO INVOICE INSTRUCTIONS: Beginning December 9, 2024 all invoicing procedures will take place on www.IPP.gov. Vendors must be registered www.IPP.gov. Registration on www.IPP.gov is required to receive payment. Invoices will not be accepted by any other method. 1. The contractor shall be active in the System Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	for Award Management (www.SAM.gov) for invoice processing. Besides the information identified below, a proper invoice shall also include; contractor's Unique Entity Identifier (UEI) number; the ICE Program Office; and state whether the invoice is "INTERIM" or "FINAL". 2. In accordance with Contract Clauses, FAR 52.212-4 (g) (1), Contract Terms and Conditions - Commercial Items, or FAR 52.232-25 (a) (3), Prompt Payment, as applicable, the information required with each invoice submission is as follows: "...An invoice must include- (i) Name and address of the Contractor. The name, address and UEI number on the invoice MUST match the information in both the Contract/Agreement and the information in SAM; (ii) Unique Entity Identifier (UEI) number; (iii) Invoice date and number; (iv) Contract number, line items and, if applicable, the order number; (v) Description, quantity, unit of measure, unit price and extended price of the items delivered; (vi) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading; (vii) Terms of any discount for prompt payment offered; (viii) Remit to Address; (ix) Name, title, and phone number of persons to notify in event of defective invoice; (x) ICE Program Office designated on the order/contract/agreement; and (xi) Whether the invoice is "Interim" or "Final" 3. Invoice submission: The above information will be required to complete the invoice submission requirements within IPP. Please refer to www.IPP.gov for additional information on Getting Started, Benefits, Features, and Enrollment. (xii). Electronic Funds Transfer (EFT) banking information in accordance with 52.232-33 Payment by Electronic Funds Transfer - System for Award Management or 52-232-34, Payment by Electronic Funds Transfer - Other than System for Award Management. 3. Invoice Supporting Documentation. To ensure payment, the vendor must submit supporting documentation which provides substantiation for Continued ...				

NAME OF OFFEROR OR CONTRACTOR
GEO GROUP INC THE

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	the invoiced costs to the Contracting Officer Representative (COR) or Point of Contact (POC) identified in the contract. Invoice charges must align with the contract CLINs. Supporting documentation is required when guaranteed minimums are exceeded and when allowable costs are incurred. Details are as follows: (i). Guaranteed Minimums. If a guaranteed minimum is not exceeded on a CLIN(s) for the invoice period, no supporting documentation is required. When a guaranteed minimum is exceeded on a CLIN (s) for the invoice period, the Contractor is required to submit invoice supporting documentation for all detention services provided during the invoice period which provides the information described below: a. Detention Bed Space Services • Bed day rate; • Detainees check-in and check-out dates; • Number of bed days multiplied by the bed day rate; • Name of each detainee; • Detainees identification information (ii). Allowable Incurred Cost. Fixed Unit Price Items (items for allowable incurred costs, such as transportation services, stationary guard or escort services, transportation mileage or other Minor Charges such as sack lunches and detainee wages): shall be fully supported with documentation substantiating the costs and/or reflecting the established price in the contract and shall be submitted in .pdf format: a. Detention Bed Space Services. For detention bed space CLINs without a GM, the supporting documentation must include: • Bed day rate; • Detainees check-in and check-out dates; • Number of bed days multiplied by the bed day rate; • Name of each detainee; • Detainees identification information b. Transportation Services: For transportation CLINs without a GM, the supporting documentation must include: • Mileage rate being applied for that invoice; Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	• Number of miles; • Transportation routes provided; • Locations serviced; • Names of detainees transported; • Itemized listing of all other charges; and, • for reimbursable expenses (e.g. travel expenses, special meals, etc.) copies of all receipts. c. Stationary Guard Services: The itemized monthly invoice shall state: • The location where the guard services were provided, • The employee guard names and number of hours being billed, • The employee guard names and duration of the billing (times and dates), and • for individual or detainee group escort services only, the name of the detainee(s) that was/were escorted. d. Other Direct Charges (e.g. VTC support, transportation meals/sack lunches, volunteer detainee wages, etc.): 1) The invoice shall include appropriate supporting documentation for any direct charge billed for reimbursement. For charges for detainee support items (e.g. meals, wages, etc.), the supporting documentation should include the name of the detainee(s) supported and the date(s) and amount(s) of support. (iii) Firm Fixed-Price CLINs. Supporting documentation is not required for charges for FFP CLINs. 4. Safeguarding Information: As a contractor or vendor conducting business with Immigration and Customs Enforcement (ICE), you are required to comply with DHS Policy regarding the safeguarding of Sensitive Personally Identifiable Information (PII). Sensitive PII is information that identifies an individual, including an alien, and could result in harm, embarrassment, inconvenience, or unfairness. Examples of Sensitive PII include information such as: Social Security Numbers, Alien Registration Numbers (A-Numbers), or combinations of information such as the individuals name or other Continued ...				

NAME OF OFFEROR OR CONTRACTOR
GEO GROUP INC THE

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	unique identifier and full date of birth, citizenship, or immigration status. As part of your obligation to safeguard information, the follow precautions are required: (i) Email supporting documents containing Sensitive PII in an encrypted attachment with password sent separately to the Contracting Officer Representative assigned to the contract. (ii) Never leave paper documents containing Sensitive PII unattended and unsecure. When not in use, these documents will be locked in drawers, cabinets, desks, etc. so the information is not accessible to those without a need to know. (iii) Use shredders when discarding paper documents containing Sensitive PII. (iv) Refer to the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information (March 2012) found at http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf for more information on and/or examples of Sensitive PII. Invoices without the above information may be returned for resubmission.				

SECTION B:
SUPPLIES OR SERVICES AND PRICES/COSTS

B.1. GENERAL

The contractor shall provide all management, supervision, labor, and materials necessary to perform the services identified in the Performance Work Statement (PWS). This requirement is structured as a single award Indefinite Delivery, Indefinite Quantity (IDIQ) contract.

B.2. CONTRACT PRICING

Please see Section B above.

B.3. MINIMUM AND MAXIMUM QUANTITIES

In accordance with FAR 16.504(a)(4)(ii), the minimum and maximum quantity the government will acquire under this contract is as follows:

Minimum: The minimum pricing limitation is the total price of performance prior to definitization.

Maximum: The maximum for the IDIQ contract is [redacted] based on the proposed total value of the IDIQ for the entire ordering period.

B.4. FUNDING

Funding will be obligated unilaterally at the task order level. The government anticipates issuing one task order annually for the required services.

[END OF SECTION B]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION C:
DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1. PERFORMANCE WORK STATEMENT (PWS)

The PWS attached to this solicitation; see *Attachment 01 – Performance Work Statement; Attachment 02 – Anticipated Transportation Routes.*

[END OF SECTION C]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION D:
PACKING AND MARKING

D.1. PACKING AND MARKING

No packing or marking requirements are applicable to this requirement.

[END OF SECTION D]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION E:
INSPECTION AND ACCEPTANCE

E.1. CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

The following clauses are incorporated by reference:

Number	Title	Date
52.246-4	Inspection of Services—Fixed-Price	Aug 1996
52.246-6	Inspection—Time-and-Material and Labor-Hour—Alternate I	May 2001

E.2. INSPECTION AND ACCEPTANCE

The government will conduct inspection and acceptance for all rendered services including deliverables. See:

Attachment 01 – Performance Work Statement
Attachment 05 – Quality Assurance Surveillance Plan

E.3. CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS)

In accordance with Federal Acquisition Regulation (FAR) Subpart 42.15, it is anticipated that past performance evaluations will be entered into CPARS, the governmentwide evaluation reporting tool for all past performance reports on contracts and orders. For more information regarding CPARS, please visit http://www.cpars.gov/.

E.4. QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Services will be evaluated in accordance with the metrics outlined in the QASP (Attachment 5 and 5A).

[END OF SECTION E]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION F:
DELIVERIES OR PERFORMANCE

F.1. CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

The following clauses are incorporated by reference:

Number	Title	Date
52.242-15	Stop-Work Order	Aug 1989

F.2. PERIOD OF PERFORMANCE

This contract has a two-year or 24-month period of performance from the effective date of definitization.

The period of performance is **03/18/2025 through 07/20/2027**

F.3. PLACE OF PERFORMANCE

North Lake Processing Facility
1805 West 32nd Street
Baldwin, Michigan 49304-9076

F.4. LIST OF DELIVERABLES

For a complete list of deliverables see Attachment 01 – PWS Section 1.35 - Deliverables

[END OF SECTION F]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION G:
CONTRACT ADMINISTRATION DATA

G.1. CONTRACT ADMINISTRATION

Notwithstanding the contractor's responsibility for total management responsibility during the performance of this contract, the administration of the contract will require maximum coordination between ICE and the contractor.

The Government points of contact for this resulting contract are identified on the coversheet.

G.2. CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The following individual is designated as the COR for this requirement and is authorized by the Contracting Officer (CO) to perform specific contract administration functions such as inspection and acceptance of services and other functions of a technical nature:

The Government points of contact for this resulting contract are identified on the coversheet.

The CORs will represent the CO in the administration of technical details within the scope of the TO. The CORs are also responsible for the final inspection and acceptance of all TO deliverables and reports. The CORs are not otherwise authorized to make any representations or commitments of any kind on behalf of the CO or the Government. The CORs do not have authority to alter the contractor's obligations or to change the contract specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify task order obligations or the specification, changes will be issued in writing and signed by the CO.

G.3. INVOICE INSTRUCTIONS

Invoicing instructions will be provided at the task order level.

[END OF SECTION G]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION H:
SPECIAL CONTRACT REQUIREMENTS

H.1. PERFORMANCE-BASED SERVICES CONTRACTING (PBSC)

Through the direction of the Office of Management and Budget (OMB), Office of Federal Procurement Policy (OFPP), performance-based contracting techniques will be applied to TOs issued under this contract to the "maximum extent practicable." For information about PBSC, refer to OFPP's Best Practices Handbook located at www.whitehouse.gov/omb.

Performance based contracts for service must include:

a) Performance requirements that define the work in measurable, mission-related terms;
b) Performance standards (i.e., quality, quantity, timeliness) tied to the performance requirements; and
c) A Government QASP or other suitable plan that describes how the Contractor's performance will be measured against the performance standards or service level agreements (SLAs).

H.2. DISCLOSURE OF INFORMATION – OFFICIAL USE ONLY

Each officer or employee of the contractor or subcontractor at any tier to whom "Official Use Only" information may be made available or disclosed, shall be notified in writing by the contractor that "Official Use Only" information disclosed to that individual can be used only for a purpose, and to the extent authorized herein, and that further disclosure of any such "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to 10-years, or both.

H.3. CONTRACTOR'S INSURANCE AND FAR 52.228-10

The contractor shall maintain insurance in an amount not less than [redacted] to protect the contractor from claims under workman compensation acts and from any other claims for damages for personal injury, including death which may arise from operations under this contract whether such operations by the contractor itself or by any subcontractor or anyone directly or indirectly employed by either business entity. The contractor shall maintain general liability insurance: bodily injury liability coverage written on a comprehensive form of policy of at least [redacted] per occurrence is required.

Additionally, an automobile liability insurance policy providing for bodily injury and property damage liability covering automobiles operated in the United States (U.S.) shall provide coverage of at least [redacted] per person and [redacted] per occurrence for bodily injury and [redacted] per occurrence for property coverage. Certificates of such insurance shall be subject to the approval of the CO for adequacy of protection. All insurance certificates required under this contract shall

provide 30-days' notice to the government of any contemplated cancellation. The contractor shall provide that all staff having access to alien monies and valuables are bonded in an amount sufficient to ensure reimbursement to the alien by the contractor in case of loss.

H.4. ICE INFORMATION GOVERNANCE AND PRIVACY REQUIREMENTS (JUL 2017)

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), 52.224-3 Privacy Training – Alternate I (DEVIATION), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive 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 DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework 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 telework authorizations.

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.

Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), 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 sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24-hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights
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 are 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.

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

H.5. COMPLIANCE WITH DHS SECURITY POLICY TERMS AND CONDITIONS

All hardware, software, and services provided under this task order must be compliant with *DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018' for NSS Collateral (Unclass, Secret or Top-Secret Collateral).*

H.6. ENCRYPTION COMPLIANCE TERMS AND CONDITIONS

If encryption is required, the following methods are acceptable for encrypting sensitive information:

a) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b) National Security Agency (NSA) Type 2 or Type 1 encryption.
c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the *Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems*).

H.7. SECURITY REVIEW TERMS AND CONDITIONS

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

H.8. INTERCONNECTION SECURITY AGREEMENT (ISA) TERMS AND CONDITIONS

Interconnections between DHS/ICE and non-DHS/ICE IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnection security agreements.

H.9. PERSONAL IDENTIFICATION VERIFICATION (PIV) CREDENTIAL COMPLIANCE TERMS AND CONDITIONS

a) Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

H.10. FEDRAMP

1) FedRAMP IT Systems Security Requirements

a) The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the contractor/Cloud Service Provider (CSP) shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

b) The CSP shall maintain a security management continuous monitoring environment that meets or exceeds the requirements outlined in the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

2) FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.
b) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
c) The contractor shall also comply with any additional FedRAMP privacy requirements.
d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, contractor shall be responsible for the following privacy and security safeguards:
    i. The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception—Disclosure to a Consumer Agency for purposes of C&A verification.
    ii. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72-hours. The program of inspection shall include, but is not limited to: Authenticated and unauthenticated operating system/network vulnerability scans Authenticated and unauthenticated we b application vulnerability scans Authenticated and unauthenticated database application vulnerability scans Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.
    iii. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
    iv. If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

3) Sensitive Information Storage

Sensitive But Unclassified (CUI) information, data, and/or equipment will only be disclosed to authorize personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

4) Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as CUI information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The government retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The government-owned data must be available to the Government upon request within one-business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

5) Security Classification

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level unless a higher level is specified.

6) Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government, and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-1, 52.227-2, 52.227-3, 52.227-11, 52.227-14, 52.227-16.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the CO.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

7) Disclosure of Information

Any information made available to the Contractor by the Government shall be used only for carrying out the provisions 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 the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

8) FedRAMP Security Requirements Overview:

a) The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

b) The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.
c) FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.
d) The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.
e) Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the contractor to issue their own authority to operate.
f) The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

9) FedRAMP Security Compliance Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST SP 800-53, Revision 4. The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

10) Required FedRAMP Policies and Regulations

The contractor shall comply with FedRAMP Security Assessment Framework – describing a general security Assessment Framework for the Federal Risk and Authorization Management Program (FedRAMP). This document details the security assessment process which must be used to achieve FedRAMP compliance. Download here:

https://www.fedramp.gov/rev5/documents-templates/

11) Assessment and Authorization

DHS/ICE may choose to cancel the contract/award and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

12) Assessment of the System

a) The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- POA&M Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.

b) Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

c) The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf). Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

d) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a POA&M document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.

e) The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30-days and all moderate risk vulnerabilities must be mitigated within 30-days from the

date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

13) Authorization of System

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

14) Reporting and Continuous Monitoring

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

All deliverables shall be labeled appropriately (such as "Controlled Unclassified Information" (CUI)). External transmission/dissemination of labeled deliverables to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."

15) Non-Repudiation

The Cloud Service Provider vendor shall provide a system that is capable of implementing NIST SP 800-53 Control AU-10 approved controls, which provides for origin authentication, data integrity, and signer non-repudiation. This binds the identity of the information producer with the information to and provides the means for authorized individuals to determine the identity of the producer of the information.

16) Identification and Authentication (Organizational Users)

The vendor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support multi-factor authentication including user ID and Password, digital certificate, PIV or smart card, PIN, tokens, etc.

17) Identification and Authentication (Non-Organizational Users)

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor-designated personnel the ability to perform management duties on the system.

18) Incident Reporting Timeframes

Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (U.S.-CERT) in accordance with U.S.-CERT "Incident Categories and Reporting Timeframes" in, Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to U.S.-CERT within 1-hour of detection regardless of the incident category reporting timeframe.

19) Media Transport

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas. Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using an approved encryption mode; non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper.

Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through appropriate actions such as logging and a documented chain of custody form.

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard 12 drives, and SD cards) must be encrypted using an approved encryption mode. All Federal Agency data residing on laptop computing devices must be protected with approved encryption software.

20) Boundary Protection

The CSP/Reseller shall route all external connections through a Trusted Internet Connection (TIC).

21) Protection of Information At Rest

The CSP shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2.

22) Security Alerts, Advisories, and Directives

The CSP/Reseller shall provide a list of their personnel, identified by name and role, with system [redacted] administration, monitoring, and/or security responsibilities that are to receive security alerts, [redacted] advisories, and directives. This list shall include ICE SOC.

H.11. PRIVACY EXPECTATIONS

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

H.12. CONTRACTOR IT SECURITY ACCREDITATION

Within 6-months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

H.13. SUPPLY CHAIN RISK MANAGEMENT TERMS AND CONDITIONS

The Contractors supplying the Government hardware and software shall provide the manufacturer's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNs number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed. Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

(i) How risks from the supply chain will be identified;
(ii) What processes and security measures will be adopted to manage these risks to the system or system components; and
(iii) How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR/CO) 30-days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents a risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market, "previously used) components only with formal Government approval. Such components shall be procured from their original source and have them shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “end of life"). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one-calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

H.14. REQUIRED PROTECTIONS FOR DHS/ICE SYSTEMS HOSTED IN NON-DHS/ICE DATA CENTERS

1) Security Authorization Terms and Conditions

A Security Authorization of any infrastructure directly in support of DHS/ICE information system shall be performed as a general support system (GSS) prior to DHS/ICE occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization (SA) shall be performed in accordance with DHS/ICE Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of DHS/ICE information system.

At the beginning of the contract, and upon request thereafter (generally at the deployment of a new system or renewal of a System Authority to Operate), the contractor/Cloud Service Provider (CSP) shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS/ICE applies in the SA process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into DHS/ICE POA&M Management Process. ICE shall use DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by DHS/ICE POA&M Management Process.

CSP procedures shall be subject to periodic, unannounced assessments by DHS/ICE officials. The documented physical aspects associated with CSP activities shall also be subject to such assessments. Inspections of CSP physical facilities will be scheduled in advance and coordinated with the provider in accordance with their facility procedures. On a periodic basis, DHS and its Components, including DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten-working days' notice, at the request of the Government, the CSP and reseller shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS/ICE information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS/ICE, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS/ICE in the event of a security incident.

2) Enterprise Security Architecture Terms and Conditions

The CSP shall utilize and adhere to DHS/ICE Enterprise Security Architecture in accordance with applicable laws and DHS/ICE policies to the satisfaction of DHS/ICE COR.

3) Continuous Monitoring Terms and Conditions

The CSP shall participate in the DHS/ICE Continuous Monitoring methodologies and, shall provide a Continuous Monitoring capability over their resources as required by FedRAMP. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the CSP shall adhere to all ITAR and FedRAMP continuous monitoring requirements and ensure that DHS/ICE can implement and integrate the following processes:

a) Asset Management
b) Vulnerability Management
c) Configuration Management
d) Malware Management
e) Log Integration
f) Security Information Event Management (SIEM) Integration
g) Patch Management
h) Providing near-real-time security status information to DHS/ICE SOC Specific Protections Terms and Conditions
   i) Specific protections that shall be provided by the CSP include, but are not limited to the following:

Specific Operations Terms and Conditions

The Contractor shall operate a SOC to provide security for the below mentioned services. The CSP shall support regular reviews with DHS/ICE Information Security Office to coordinate and synchronize the security posture of the CSP hosting facility with that of DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The CSP staff shall also analyze the information generated

by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the CSP staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the CSP facility SOC shall adhere to the incident response plan.

4) **Computer Incident Response Services Terms and Conditions**
The CSP shall provide Computer Incident Response Team (CIRT) services. The CSP shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS/ICE-specific incident response plan that adheres to DHS/ICE policy and procedure for reporting incidents. The CSP shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The CSP shall notify DHS/ICE SOC of any incident in accordance with the Incident Response Plan and work with DHS/ICE throughout the incident duration.

5) **Network Intrusion Detection Systems (NIDS) and Monitoring Terms and Conditions**
The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets for their facility(s). The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be made available to DHS/ICE upon request. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

6) **Physical and Information Security and Monitoring Terms and Conditions**
The CSP shall provide a facility using appropriate protective measures to provide for physical security. All facilities will be located within the United States. The CSP shall maintain a process to control physical access to all DHS/ICE IT assets. DHS/ICE IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS/ICE security office upon request.

7) **Vulnerability Assessments Terms and Conditions**
The CSP and reseller shall provide all information from any managed device to DHS/ICE, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

8) **Anti-malware (e.g., virus, spam) Terms and Conditions**
The CSP shall design, implement, monitor, and manage to provide comprehensive anti-malware service. The CSP shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, when changes are required. A summary of alerts shall be reported to DHS/ICE SOC in weekly status report. If an abnormality or anomaly is identified, the CSP shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

9) **Log** Retention **Terms and Conditions**
Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180-days and offline for three-years.

H.15. PATCH MANAGEMENT TERMS AND CONDITIONS

The CSP, or software vendor (for certain Software-as-a-Service (SaaS) offerings), shall perform patch management services to all Platform-as-a-Service (PaaS) and SaaS offerings managed by the CSP, or in cases where the SaaS offering is hosted by an independent third-party, the third-party will be responsible for providing the patch management services. The CSP shall push patches that are required by vendors and DHS/ICE system owner. This is to ensure that the infrastructure and applications that directly support DHS/ICE information system are current in their release and that all security patches are applied. The CSP and software vendor shall be informed by DHS/ICE which patches are required by DHS/ICE through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS/ICE utilizes to fulfill their mission, shall be tested by DHS/ICE. However, the CSP and software vendor(s) shall be responsible for deploying patches to their products as directed by DHS/ICE. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the CSP prior to deployment in a test environment.

[END OF SECTION H]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION I:
CONTRACT CLAUSES

I.1. FAR CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

Notice:
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, 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation, and Offeror Representations and Certifications—Commercial Products and Commercial Services, including paragraph (t). 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 enforcing 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

- 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 update their entity registration to remove these representations in SAM.

The following clauses and/or provisions are incorporated by reference.

Number	Title	Date
52.202-1	Definitions	Jun 2020
52.203-3	Gratuities	Apr 1984
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	Jun 2020
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	Jan 2017
52.204-13	System for Award Management Maintenance	Oct 2018

52.204-18	Commercial and Government Entity Code Maintenance	Aug 2020
52.204-19	Incorporation by Reference of Representations and Certifications	Dec 2014
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	Nov 2015
52.215-8	Order of Precedence—Uniform Contract Format	Oct 1997
52.216-18	Ordering: Such orders may be issued from **date of IDIQ award** through **IDIQ end date**.	Aug 2020
52.216-19	Order Limitations: (a) The guaranteed minimum (b) (1) The IDIQ Ceiling (b) (2) The IDIQ ceiling (b) (3) Not applicable	Oct 1995
52.216-22	Indefinite Quantity: (d) the IDIQ end date	Oct 1995
52.219-16	Liquidated Damages - Subcontracting Plan	Sep 2021
52.223-3	Hazardous Material Identification & Material Safety Data—Alternate I	Feb 2021
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.227-1	Authorization and Consent	Jun 2020
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	Jun 2020
52.227-3	Patent Indemnity	Jun 2020
52.227-11	Patent Rights—Ownership by the Contractor	May 2014
52.227-14	Rights in Data—General	May 2014
52.227-16	Additional Data Requirements	Jun 1987
52.232-1	Payments	Apr 1984
52.232-8	Discounts for Prompt Payment	Feb 2002
52.232-9	Limitation on Withholding of Payments	Apr 1984
52.232-11	Extras	Apr 1984
52.232-18	Availability of Funds	Apr 1984
52.232-23	Assignment of Claims	May 2014
52.232-39	Unenforceability of Unauthorized Obligations	Jun 2013
52.233-1	Disputes—Alternate 1	May 2014
52.233-3	Protest after Award	Aug 1996
52.233-4	Applicable Law for Breach of Contract Claim	Oct 2004
52.237-3	Continuity of Services	Jan 1991
52.242-13	Bankruptcy	Jul 1995
52.243-1	Changes—Fixed Price--Alternate I	Apr 1984
52.243-3	Changes—Time-and-Materials or Labor-Hours	Sep 2000
52.244-2	Subcontracts	Jun 2020
52.249-2	Termination for Convenience of the Government (Fixed-Price)	Apr 2012
52.249-8	Default (Fixed-Price Supply and Service)	Apr 1984

I.2. FAR CLAUSES AND/OR PROVISIONS INCORPORATED BY FULL TEXT

The following clauses and/or provisions are incorporated by full text.

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (DEVIATION 20-05) (JUL 2024)

(a) Definitions. As used in this clause- Kaspersky Lab covered article means any hardware, software, or service that–

(1) Is developed or provided by a Kaspersky Lab covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab covered entity.

Kaspersky Lab covered entity means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any Kaspersky Lab covered article. The Contractor is prohibited from—

(1) Providing any Kaspersky Lab covered article that the Government will use on or after October 1, 2018; and

(2) Using any Kaspersky Lab covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) Reporting requirement.

(1) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting

Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at NDAA Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 3-business days from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10-business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a Kaspersky Lab covered article, any reasons that led to the use or submission of the Kaspersky Lab covered article, and any additional efforts that will be incorporated to prevent future use or submission of Kaspersky Lab covered articles.

(a) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (DEVIATION 2020-05) (DEC 2020)

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

"Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

> (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
>
> (ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115–232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at NDAA_Incidents@hq.dhs.gov, with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one-business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10-business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.212-4 Contract Terms and Conditions—Commercial Products and Commercial Services (Nov 2023)

(a) 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.

(b) 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.

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

(d) 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 at Federal Acquisition Regulation (FAR) 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) Definitions. The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(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 such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) Invoice. (1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include-

(i) Name and address of the Contractor;

(ii) Invoice date and number;

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

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

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

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

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

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

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

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

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

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

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

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C.3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR Part 1315.

(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) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) 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 which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) 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; and

(D) Contractor point of contact.

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

(6) 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 33.211 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 32.607-2).

(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 default termination.

(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 prescribed in FAR 32.608-2 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 hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges 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. 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 hereunder 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) Other compliances. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) 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; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

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

(1) The schedule of supplies/services.

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

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments.

(9) The specification.

(t) [Reserved]

(u) Unauthorized Obligations. (1) Except as stated in paragraph (u)(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:

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

(v) 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)

Alternate I (Nov 2021). When a time-and-materials or labor-hour contract is contemplated, substitute the following paragraphs (a), (e), (i), (l), and (m) for those in the basic clause.

(a) Inspection/Acceptance. (1) The Government has the right to inspect and test all materials furnished and services performed under this contract, to the extent practicable at all places and times, including the period of performance, and in any event before acceptance. The Government may also inspect the plant or plants of the Contractor or any subcontractor engaged in contract performance. The Government will perform inspections and tests in a manner that will not unduly

delay the work.

(2) If the Government performs inspection or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish and shall require subcontractors to furnish all reasonable facilities and assistance for the safe and convenient performance of these duties.

(3) Unless otherwise specified in the contract, the Government will accept or reject services and materials at the place of delivery as promptly as practicable after delivery, and they will be presumed accepted 60-days after the date of delivery, unless accepted earlier.

(4) At any time during contract performance, but not later than 6-months (or such other time as may be specified in the contract) after acceptance of the services or materials last delivered under this contract, the Government may require the Contractor to replace or correct services or materials that at time of delivery failed to meet contract requirements. Except as otherwise specified in paragraph (a)(6) of this clause, the cost of replacement or correction shall be determined under paragraph (i) of this clause, but the "hourly rate" for labor hours incurred in the replacement or correction shall be reduced to exclude that portion of the rate attributable to profit. Unless otherwise specified below, the portion of the "hourly rate" attributable to profit shall be 10 percent. The Contractor shall not tender for acceptance materials and services required to be replaced or corrected without disclosing the former requirement for replacement or correction, and, when required, shall disclose the corrective action taken. [Insert portion of labor rate attributable to profit.]

(5)(i) If the Contractor fails to proceed with reasonable promptness to perform required replacement or correction, and if the replacement or correction can be performed within the ceiling price (or the ceiling price as increased by the Government), the Government may-

(A) By contract or otherwise, perform the replacement or correction, charge to the Contractor any increased cost, or deduct such increased cost from any amounts paid or due under this contract; or

(B) Terminate this contract for cause.

(ii) Failure to agree to the amount of increased cost to be charged to the Contractor shall be a dispute under the Disputes clause of the contract.

(6) Notwithstanding paragraphs (a)(4) and (5) above, the Government may at any time require the Contractor to remedy by correction or replacement, without cost to the Government, any failure by the Contractor to comply with the requirements of this contract, if the failure is due to-

(i) Fraud, lack of good faith, or willful misconduct on the part of the Contractor's managerial personnel; or

(ii) The conduct of one or more of the Contractor's employees selected or retained by the Contractor after any of the Contractor's managerial personnel has reasonable grounds to believe that the employee is habitually careless or unqualified.

(7) This clause applies in the same manner and to the same extent to corrected or replacement

materials or services as to materials and services originally delivered under this contract.

(8) The Contractor has no obligation or liability under this contract to correct or replace materials and services that at time of delivery do not meet contract requirements, except as provided in this clause or as may be otherwise specified in the contract.

(9) Unless otherwise specified in the contract, the Contractor's obligation to correct or replace Government-furnished property shall be governed by the clause pertaining to Government property.

(e) Definitions. (1) The clause at FAR 52.202-1, Definitions, is incorporated herein by reference. As used in this clause-

(i) "Direct materials" means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.

(ii) "Hourly rate" means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are-

(A) Performed by the contractor;

(B) Performed by the subcontractors; or

(C) Transferred between divisions, subsidiaries, or affiliates of the contractor under a common control.

(iii) "Materials" means-

(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the contractor under a common control;

(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;

(C) Other direct costs (e.g., incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.);

(D) The following subcontracts for services which are specifically excluded from the hourly rate: [Insert any subcontracts for services to be excluded from the hourly rates prescribed in the schedule.]; and

(E) Indirect costs specifically provided for in this clause.

(iv) "Subcontract" means any contract, as defined in FAR subpart 2.1, entered into with a subcontractor to furnish supplies or services for performance of the prime contractor a subcontract including transfers between divisions, subsidiaries, or affiliates of a contractor or subcontractor. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(i) Payments. (1) Work performed. The Government will pay the Contractor as follows upon the submission of commercial invoices approved by the Contracting Officer:

(i) Hourly rate.

(A) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the contract by the number of direct labor hours performed. Fractional parts of an hour shall be payable on a prorated basis.

(B) The rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by individuals that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.

(C) Invoices may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer) to the Contracting Officer or the authorized representative.

(D) When requested by the Contracting Officer or the authorized representative, the Contractor shall substantiate invoices (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment, individual daily job timecards, records that verify the employees meet the qualifications for the labor categories specified in the contract, or other substantiation specified in the contract.

(E) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis.

(1) If no overtime rates are provided in the Schedule and the Contracting Officer approves overtime work in advance, overtime rates shall be negotiated.

(2) Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract.

(3) If the Schedule provides rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.

(ii) Materials.

(A) If the Contractor furnishes materials that meet the definition of a commercial product at FAR 2.101, the price to be paid for such materials shall not exceed the Contractor's established catalog or market price, adjusted to reflect the-

(1) Quantities being acquired; and

(2) Any modifications necessary because of contract requirements.

(B) Except as provided for in paragraph (i)(1)(ii)(A) and (D)(2) of this clause, the Government will reimburse the Contractor the actual cost of materials (less any rebates, refunds, or discounts received by the contractor that are identifiable to the contract) provided the Contractor-

(1) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or

(2) Makes these payments within 30-days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.

(C) To the extent able, the Contractor shall-

(1) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and

(2) Give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that are identifiable to the contract.

(D) Other Costs. Unless listed below, other direct and indirect costs will not be reimbursed.

(1) Other Direct Costs. The Government will reimburse the Contractor on the basis of actual cost for the following, provided such costs comply with the requirements in paragraph (i)(1)(ii)(B) of this clause: *None.*

(2) Indirect Costs (Material Handling, Subcontract Administration, etc.). The Government will reimburse the Contractor for indirect costs on a pro-rata basis over the period of contract performance at the following fixed price: *$0.*

(2) Total cost. It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule and the Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30-days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during the performance of this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performance of this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.

(3) Ceiling price. The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the Contractor in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.

(4) Access to records. At any time before final payment under this contract, the Contracting Officer (or authorized representative) will have access to the following (access shall be limited to the listing below unless otherwise agreed to by the Contractor and the Contracting Officer):

(i) Records that verify that the employees whose time has been included in any invoice meet the qualifications for the labor categories specified in the contract;

(ii) For labor hours (including any subcontractor hours reimbursed at the hourly rate in the schedule), when timecards are required as substantiation for payment-

(A) The original timecards (paper-based or electronic);

(B) The Contractor's timekeeping procedures;

(C) Contractor records that show the distribution of labor between jobs or contracts; and

(D) Employees whose time has been included in any invoice for the purpose of verifying that these employees have worked the hours shown on the invoices.

(iii) For material and subcontract costs that are reimbursed on the basis of actual cost-

(A) Any invoices or subcontract agreements substantiating material costs; and

(B) Any documents supporting payment of those invoices.

(5) Overpayments/Underpayments. Each payment previously made shall be subject to reduction to the extent of amounts, on preceding invoices, that are found by the Contracting Officer not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. The Contractor shall promptly pay any such reduction within 30-days unless the parties agree otherwise. The Government within 30-days will pay any such increases, unless the parties agree otherwise. The Contractor's payment will be made by check. If the Contractor becomes aware of a duplicate invoice payment or that the Government has otherwise overpaid on an 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; and

(D) Contractor point of contact.

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

(6)(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, and then at the rate applicable for each six-month period as established 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 33.211 if-

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt in a timely manner;

(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 32.607-2).

(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 default termination.

(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 prescribed in FAR 32.608-2 in effect on the date of this contract.

(viii) Upon receipt and approval of the invoice designated by the Contractor as the "completion invoice" and supporting documentation, and upon compliance by the Contractor with all terms of this contract, any outstanding balances will be paid within 30-days unless the parties agree otherwise. The completion invoice, and supporting documentation, shall be submitted by the Contractor as promptly as practicable following completion of the work under this contract, but in no event later than 1-year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(7) Release of claims. The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions.

(i) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible to exact statement by the Contractor.

(ii) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6-years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(iii) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(8) 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.

(9) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(10) 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.

(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 hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid an amount for direct labor hours (as defined in the Schedule of the contract) determined by multiplying the number of direct labor hours expended before the effective date of termination by the hourly rate(s) in the contract, less any hourly rate payments already made to the Contractor plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system that have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.

(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. 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.

(End of clause)

FAR 52.212-5 Contract Terms and Conditions Required to Implement Statutes or Executive Orders – Commercial Products and Commercial Services (JAN 2025)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

☒ (1) 52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017)

☒ (2) 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (DEC 2023)**[See deviation below.]

☒ (3) 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (NOV 2021)**[See deviation below.]

☒ (4) 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)

☒ (5) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (MAR 2023)

☒ (6) 52.233-3 Protest After Award (AUG 1996)

☒ (7) 52.233-4 Applicable Law for Breach of Contract Claim (OCT 2004)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

☒ (1) 52.203-6 Restrictions on Subcontractor Sales to the Government (JUN 2020)

☒ Alternate I (NOV 2021)

☒ (2) 52.203-13 Contractor Code of Business Ethics and Conduct (NOV 2021)

☐ (3) 52.203-15 Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUNE 2010)

☒ (4) 52.203-17 Contractor Employee Whistleblower Rights (NOV 2023)

☒ (5) 52.204-10 Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020)

☐ (6) [Reserved]

☐ (7) 52.204-14 Service Contract Reporting Requirements (OCT 2016)

☒ (8) 52.204-15 Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016)

☒ (9) 52.204-27 Prohibition on a ByteDance Covered Application (JUN 2023)

☐ (10) 52.204-28 Federal Acquisition Supply Chain Security Act Orders – Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts. (DEC 2023)

☐ (11) 52.204-30 Federal Acquisition Supply Chain Security Act Orders – Prohibition (DEC 2023)

☐ Alternate I (DEC 2023) of 52.204-30

☒ (12) 52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded. (JAN 2025)

☒ (13) 52.209-9 Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018)

☐ (14) [Reserved]

☐ (15) 52.219-3 Notice of HubZone Set-Aside of Sole-Source Award (OCT 2022)

☐ (16) 52.219-4 Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2022)

☐ (17) [Reserved]

☐ (18) 52.219-6 Notice of Total Small Business Set-Aside (NOV 2020)

☐ Alternate I (MAR 2020)

☐ (19) 52.219-7 Notice of Partial Small Business Set-Aside (NOV 2020)

☐ Alternate I (MAR 2020)

☒ (20) 52.219-8 Utilization of Small Business Concerns (JAN 2025)

☒ (21) 52.219-9 Small Business Subcontracting Plan (JAN 2025)

☐ Alternate I (NOV 2016)

☒ Alternate II (NOV 2016)

☐ Alternate III (JUN 2020)

☐ Alternate IV (JAN 2025)

☐ (22) 52.219-13 Notice of Set-Aside of Orders (MAR 2020)

☐ Alternate I (MAR 2020)

☐ (23) 52.219-14 Limitations on Subcontracting (OCT 2022)**

☒ (24) 52.219-16 Liquidated Damages – Subcontracting Plan (SEP 2021)

☐ (25) 52.219-27 Notice of Set-Aside for, or Sole-Source Award to, Service-Disabled Veteran-Owned Small Business (SDVOSB) Concerns Eligible Under the SDVOSB Program Set-Aside (FEB 2024)

☐ (26) 52.219-28 Postaward Small Business Program Rerepresentation (JAN 2025)

☐ Alternate I (MAR 2020)

☐ (27) 52.219-29 Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (OCT 2022)

☐ (28) 52.219-30 Notice of Set-Aside for, or Sole-Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (OCT 2022)

☐ (29) 52.219-32 Orders Issued Directly Under Small Business Reserves (MAR 2020)

☐ (30) 52.219-33 Nonmanufacturer Rule (SEP 2021)

☒ (31) 52.222-3 Convict Labor (JUN 2003)

☐ (32) 52.222-19 Child Labor – Cooperation with Authorities and Remedies (JAN 2025)

☐ (33) ~~52.222-21 Prohibition of Segregated Facilities (APR 2015)~~

☐ (33) ~~52.222-26 Equal Opportunity (SEP 2016) (E.O. 11246)~~

☐ ~~(33) Alternate I (FEB 1999)~~

☒ (35) 52.222-35 Equal Opportunity for Veterans (JUN 2020)

☐ Alternate I (JUL 2014)

☒ (36) 52.222-36 Equal Opportunity for Workers with Disabilities (JUN 2020)

☐ Alternate I (JUL 2014)

☒ (37) 52.222-37 Employment Reports on Veterans (JUN 2020)

☒ (38) 52.222-40 Notification of Employee Rights Under the National Labor Relations Act (DEC 2010)

☒ (39) 52.222-50 Combating Trafficking in Persons (NOV 2021)

☐ Alternate I (MAR 2015)

☒ (40) 52.222-54 Employment Eligibility Verification (JAN 2025) (Executive Order 12989)

☐ (41) 52.223-9 Estimate of Percentage of Recovered Material Content for EPA-Designated Products (MAY 2008)

☐ Alternate I (MAY 2008)

☐ (42) 52.223-11 Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (MAY 2024)

☐ (43) 52.223-12 Maintenance, Service, Repair or Disposal of Refrigeration Equipment and Air Conditioners (MAY 2024)

☐ (44) 52.223-20 Aerosols (MAY 2024)

☐ (45) 52.223-21 Foams (MAY 2024)

☒ (47) 52.224-3 Privacy Training (JAN 2017)* [See deviation below.]

☒ Alternate 1 (JAN 2017)

☐ (48) 52.225-1 Buy American – Supplies (OCT 2022)

☐ Alternate I (OCT 2022)

☐ (49) 52.225-3 Buy American – Free Trade Agreements – Israeli Trade Act (NOV 2023)

☐ Alternate I [Reserved]

☐ Alternate II (DEC 2022)

☐ Alternate III (FEB 2024)

☐ Alternate IV (OCT 2022)

☐ (50) 52.225-5 Trade Agreements (NOV 2023)

☒ (51) 52.225-13 Restrictions on Certain Foreign Purchases (FEB 2021)

☒ (52) 52.225-26 Contractors Performing Private Security Functions Outside the United States (OCT 2016)

☐ (53) 52.226-4 Notice of Disaster or Emergency Area Set-Aside (NOV 2007)

☐ (54) 52.226-5 Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007)

☒ (55) 52.226-8, Encouraging Contractor Policies to Ban Text Messaging While Driving (MAY 2024)

☐ (56) 52.229-12 Tax on Certain Foreign Procurements (FEB 2021)

☐ (57) 52.232-29 Terms for Financing of Purchases of Commercial Items (NOV 2021)

☐ (58) 52.232-30 Installment Payments for Commercial Items (NOV 2021)

☒ (59) 52.232-33 Payment by Electronic Funds Transfer—System for Award Management (OCT 2018)

☐ (60) 52.232-34 Payment by Electronic Funds Transfer—Other than System for Award Management (JUL 2013)

☐ (61) 52.232-36 Payment by Third Party (MAY 2014)

☒ (62) 52.239-1 Privacy or Security Safeguards (AUG 1996)

☒ (63) 52.240-1, Prohibition on Unmanned Aircraft System Manufactured or Assembled by American Security Drone Act-Covered Foreign Entities (NOV 2024)

☒ (64) 52.242-5 Payments to Small Business Subcontractors (JAN 2017)

☐ (65) 52.247-64 Preference for Privately Owned U.S.-Flag Commercial Vessels (NOV 2021)

☐ Alternate I (APR 2003)

☐ Alternate II (NOV 2021)

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

☒ (1) 52.222-41 Service Contract Labor Standards (AUG 2018)

☒ (2) 52.222-42 Statement of Equivalent Rates for Federal Hires (MAY 2014)

☒ (3) 52.222-43 Fair Labor Standards Act and Service Contract Labor Standards—Price Adjustment (Multiple Year and Option Contracts) (AUG 2018)

☐ (4) 52.222-44 Fair Labor Standards Act and Service Contract Act—Price Adjustment (MAY 2014)

☐ (5) 52.222-51 Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (MAY 2014)

☐ (6) 52.222-53 Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014)

☒ (7) 52.222-55 Minimum Wages for Contractor Workers Under Executive Order 14026 (JAN 2022)*

☒ (8) 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2022)

☐ (9) 52.226-6 Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020)

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, as defined in FAR 2.101, on the date of award of this contract, and does not contain the clause at 52.215-2, Audit and Records-Negotiation.

(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 subpart 4.7, Contractor Records Retention, of the 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 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.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1), in a subcontract for commercial products or commercial services. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (NOV 2021) (41 U.S.C. 3509).

(ii) 52.203-17, Contractor Employee Whistleblower Rights (NOV 2023) (41 U.S.C. 4712).

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

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

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

(vi) 52.204-27 Prohibition on a ByteDance Covered Application (JUN 2023)

(vii) (A) 52.204-30 Federal Acquisition Supply Chain Security Act Orders – Prohibition (DEC 2023) (Pub. L. 115-390, title II).

1) (B) Alternate I (DEC 2023) of 52.204-30.

(viii) 52.219-8, Utilization of Small Business Concerns (JAN 2025) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of the subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

~~(ix) 52.222-21, Prohibition of Segregated Facilities (APR 2015)~~

~~(x) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246)~~

(xi) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).

(xii) 52.222-36, Equal Opportunity for Workers with Disabilities (JUN 2020) (29 U.S.C. 793).

(xiii) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212)

(xiv) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xv) 52.222-41, Service Contract Labor Standards (AUG 2018) (41 U.S.C. chapter 67).

(A) 52.222-50, Combating Trafficking in Persons (NOV 2021) (22 U.S.C. chapter 78 and E.O 13627).

(B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O 13627).

(xvi) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xvii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xviii) 52.222-54, Employment Eligibility Verification (JAN 2025) (E.O.12989).

(xix) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (JAN 2022). *

(xx) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2022) (E.O. 13706).

(A) 52.224-3, Privacy Training (JAN 2017) (5U.S.C. 552a).

(B) Alternate I (JAN 2017) of 52.224-3.

(xxi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxiii) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) (31 U.S.C. 3903 and 10 U.S.C 3801). Flow down required in accordance with paragraph (c) of 52.232-40.

(xxiv) 52.232-40, Prohibition on Unmanned Aircraft Systems Manufactured or Assembled by American Security Drone Act-Covered Foreign Entities (Nov 2024) (Sections 1821-1826, Pub. L. 118-31, 41 U.S.C. 3901 note prec.).

(xxv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (NOV 2021) 46 U.S.C. 55305 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

FAR 52.219-14 Limitations on Subcontracting (JULY 2023) (DEVIATION JULY 2023)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) *Definition. Similarly situated entity*, as used in this clause, means a first-tier subcontractor, including an independent contractor, that

(1) Has the same small business program status as that which qualified the prime contractor for the award (e.g., for a small business set-aside contract, any small business concern, without regard to its socioeconomic status); and

(2) Is considered small for the size standard under the North American Industry Classification System (NAICS) code the prime contractor assigned to the subcontract.

(c) *Applicability*. This clause applies only to

(1) Contracts that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(3) Contracts that have been awarded on a sole-source basis in accordance with subparts 19.8, 19.13, 19.14, and 19.15;

(4) Orders expected to exceed the simplified acquisition threshold and that are.

(i) Set aside for small business concerns under multiple-award contracts, as described in 8.405-5 and 16.505(b)(2)(i)(F); or

(ii) Issued directly to small business concerns under multiple-award contracts as described in 19.504(c)(1)(ii);

(5) Orders, regardless of dollar value, that are.

(i) Set aside in accordance with subparts 19.8, 19.13, 19.14, or 19.15 under multiple award contracts, as described in 8.405-5 and 16.505(b)(2)(i)(F); or

(ii) Issued directly to concerns that qualify for the programs described in subparts 19.8, 19.13, 19.14, or 19.15 under multiple-award contracts, as described in 19.504(c)(1)(ii); and

(6) Contracts using the HUBZone price evaluation preference to award to a HUBZone small business concern unless the concern waived the evaluation preference.

(d) *Independent contractors*. An independent contractor shall be considered a subcontractor.

(e) *Limitations on subcontracting*. By submission of an offer and execution of a contract, the Contractor agrees to the following requirements in the performance of a contract assigned a North American Industry Classification System (NAICS) code applicable to this contract:

(1) *Services (except construction).* It will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding certain other direct costs and certain work performed outside the United States (see paragraph (e)(1)(i)), to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts that are not similarly situated entities. Any work that a similarly situation entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract.

(i) The following services may be excluded from the 50 percent limitation:

(A) Other direct costs, to the extent they are not the principal purpose of the acquisition and small business concerns do not provide the service. Examples include airline travel, work performed by a transportation or disposal entity under a contract assigned the environmental remediation NAICS code (562910), cloud computing services, or mass media purchases.

(B) Work performed outside the United States on awards made pursuant to the Foreign Assistance Act of 1961, or work performed outside the United States required to be performed by a local contractor.

(2) *Supplies (other than procurement from a nonmanufacturer of such supplies).* It will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime amount that cannot be exceeded. When a contract includes both supplies and services, the 50 percent limitation shall apply only to the supply portion of the contract.

(3) *General construction*. It will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will act amount that cannot be exceeded.

(4) *Construction by special trade contractors*. It will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 75 percent subcontract amount that that cannot be exceeded.

The Contractor shall comply with the limitations on subcontracting as follows:

(5) For contracts, in accordance with paragraphs (c)(1), (2), (3), and (6) of this clause

[*Contracting Officer check as appropriate.*]

☐ By the end of the base term of the contract and then by the end of each subsequent option period; or
☒ By the end of the performance period for each order issued under the contract.

(6) For orders, in accordance with paragraphs (c)(4) and (5) of this clause, by the end of the performance period for the order.

(f) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(1) In a joint venture comprised of a small business protégé and its mentor approved by the Small Business Administration, the small business protégé shall perform at least 40 percent of the work performed by the joint venture. Work performed by the small business protégé in the joint venture must be more than administrative functions.

(2) In an 8(a) joint venture, the 8(a) participant(s) shall perform at least 40 percent of the work performed by the joint venture. Work performed by the 8(a) participants in the joint venture must be more than administrative functions.

(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 24.1 and

39.105).

(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)

52.252-2 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 address: https://www.acquisition.gov.

(End of clause)

I.3. HSAM CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (July 2023)

The Contractor agrees to comply with any provision or clause that is incorporated herein by

reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(a) *Provisions.*

3052.219-72, Evaluation of Prime Contractor Participation in the DHS Mentor-Protégé Program

(b) *Clauses.*

3052.203-70, Instructions for Contractor Disclosure of Violations 3052.204-71 Contractor Employee Access—Alternate II 3052.204-72 Safeguarding of Controlled Unclassified Information 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents
3052.205-70 Advertisement, Publicizing Awards, and Releases 3052.215-70 Key Personnel or Facilities
*3052.219-71 DHS Mentor-Protégé Program 3052.242-72, Contracting Officer's Representative

(End of clause)

***HSAR 3052.219-71 DHS Mentor-Protégé Program (DEVIATION) (Apr 2024)**

(a) Large businesses are encouraged to participate in the DHS Mentor-Protégé program for the purpose of providing developmental assistance to eligible protégé entities to enhance their capabilities and increase their participation in DHS contracts.

(b) The program consists of:

(1) Mentor firms, which are large prime contractors capable of providing developmental assistance;

(2) Protégé firms, are small businesses, veteran-owned small businesses, service-disabled veteran-owned small businesses, HUBZone small businesses, small-disadvantaged businesses, and women-owned small business concerns, Historically Black Colleges and Universities, and Minority Serving Institutions; and

(3) Mentor-Protégé agreements, approved by the DHS Office of Small and Disadvantaged Business Utilization (OSDBU).

(c) Mentor participation in the program means providing business developmental assistance to aid protégés in developing the requisite expertise to effectively compete for and successfully perform DHS contracts and subcontracts.

(d) Large business prime contractors serving as mentors in the DHS Mentor-Protégé program are eligible for a post-award incentive for subcontracting plan credit. The mentor may receive small business subcontracting credit for costs it incurs to provide assistance to a protégé. The mentor may

use this additional credit towards attaining its subcontracting plan participation goal under the same or another DHS contract. The amount of credit given to a mentor firm for these protégé developmental assistance costs shall be calculated on a dollar-for-dollar basis and reported in the Summary Subcontract Report via the Electronic Subcontracting Reporting System (eSRS) at www.esrs.gov. For example, a mentor/large business prime contractor would report a $10,000 subcontract to the protégé subcontractor and $5,000 of developmental assistance to the protégé as $15,000. The Mentor and Protégé will submit a signed joint statement agreeing on the dollar value of the developmental assistance and the Summary Subcontract Report.

(e) Contractors interested in participating in the program are encouraged to contact the DHS OSDBU for more information.

(End of clause)

I.4. HSAM CLAUSES AND/OR PROVISIONS INCORPORATED BY FULL TEXT

3052.204-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

(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, the 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)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) *Authority to Operate*. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3-years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(i) *Security Authorization Package*. The SA package shall be developed using the

government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30-days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3-years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90-days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3-business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1-year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

3052.216-74 Settlement of letter contract (DEC 2003)

(a) This contract constitutes the definitive contract contemplated by letter contract 70CDCR25D00000009 issued on 03/18/2025. It supersedes the letter contract and its modification P00001. To the extent there are inconsistencies between the definitive contract and the letter contract, the former governs.

(b) The cost(s) and fee(s), or price(s), established in this definitive contract represents full and complete settlement of task order.

Payment of the fee agreed upon or profit withheld pending definitization of the letter contract, may start immediately at the rate and times stated within this contract.

(End of clause)

SPECIAL CLAUSE INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

(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 SECTION I]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION J:
LIST OF ATTACHMENTS

J.1. LIST OF ATTACHMENTS

The following is a list of all attachments associated with this requirement.

Attachments	
Attachment 1	Performance Work Statement (PWS)
Attachment 2	Anticipated Transportation Routes
Attachment 3	Staffing Plan
Attachment 4	Detention Services Cost Statement (DSCS)
Attachment 5	Quality Assurance Surveillance Plan (QASP)
Attachment 5A	CDR Template
Attachment 6A	Wage Determination 2015-4881
Attachment 6B	Wage Determination 2015-4839
Attachment 6C	Wage Determination 2015-4847
Attachment 7	Detention-Transportation Template – unlocked*
Attachment 8	G-391 Upload Template
Attachment 8A	G-391 Data Collection Categories and Descriptions
Attachment 9	Prison Rape Elimination Act Regulations
Attachment 10	Personal Property Operations Handbook, February 2019
Attachment 11	Virtual Attorney Visitation
Attachment 12	ICE Firearms and Use of Force Handbook *(by reference – contains law enforcement sensitive information)*
Attachment 13	Contract Detention Facility Design Standards
Attachment 14	EOIR Design Standards
Attachment 15	IHSC Design Standard, June 2023
Attachment 16	Structured Cable Plant Standard, January 2025
Attachment 17	Small Business Subcontracting Plan

**When this document is submitted it must be password protected as it will include sensitive information. Contractor shall work with the COR to determine the password*

[END OF SECTION J]