SECTION II – STATEMENT OF WORK
REGULATORY SUPPORT SERVICES

1.0 BACKGROUND

The Acquisition Policy and Legislation (APL) branch under the DHS Office of the Chief Procurement Officer is responsible for establishing departmentwide procurement regulations. Specifically, APL is responsible for updating the Homeland Security Acquisition Regulation (HSAR) to address current statutory and regulatory requirements (i.e., rulemaking). When APL issues a rulemaking, it must abide by the requirements of the Regulatory Flexibility Act (RFA), Executive Order (E.O.) 12866 *Regulatory Planning and Review*, the Office of Management and Budget (OMB) Circular A-4 *Regulatory Analysis*, and E.O. 13563 *Improving Regulation and Regulatory Review*.

- The RFA requires federal agencies to consider the effects of their regulations on small businesses and other small entities. If a regulation is expected to have a "significant economic impact on a substantial number of small entities," the RFA requires the issuing agency to consider regulatory impacts and alternatives, with the goal of minimizing significant economic impacts on small entities.
- E.O. 12866 establishes the guiding principles agencies must follow when developing regulations, including encouraging the use of cost-benefit analysis, risk assessment and performance-based regulatory standards. The E.O. grants the Office of Information and Regulatory Affairs (OIRA), not the agency, authority to make the final determination of which rules are considered to be significant. For all significant rulemakings, the agencies must provide OIRA with the text of the regulation, a statement of need, and "an assessment of costs and benefits of the regulatory action."
- OMB Circular A-4 provides guidance to federal agencies on the development of regulatory analysis required under E.O. 12866, such as the cost benefit analysis, which informs the agency and the public whether the benefits of a rule are likely to justify the costs, or which of the various possible alternatives would be the most cost effective.
- E.O. 13563 supplements and affirms the requirements of E.O. 12866, and sets out "principles and requirements designed to promote public participation, improve integration and innovation, increase flexibility, ensure scientific integrity, and increase retrospective analysis of existing rules."

2.0 SCOPE

The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items necessary to provide regulatory support services as defined in Section 3.4 Task 4 – Regulatory Support of the BPA statement of work (SOW). HSAR Class Deviations are accessible at https://www.dhs.gov/publication/current-hsardeviations and FAR Class Deviations are accessible at https://www.dhs.gov/publication/currentfar-deviations. The HSAR is accessible at https://www.dhs.gov/publication/hsar.

3.0 TASKS

3.1 TASK 1: PROPOSED AND FINAL RULE TO IMPLEMENT HSAR CLASS DEVIATION 13-01 "APPLICABILITY OF THE "KISSELL AMENDMENT" TO DEPARTMENT OF HOMELAND SECURITY ACQUISITIONS"

3.1.1 Proposed Rule – During the comment period, the contractor shall provide technical writing support and comment processing support for responses to any internal and external passbacks. **(LABOR HOUR)**

3.1.2 Proposed Rule – The contractor shall attend meetings with commenters or other third parties, when requested, regarding the proposed rule, particularly in those instances when DHS expects that the outside party will provide additional data or comment upon the economic analysis or data contained in the proposing release. **(LABOR HOUR)**

3.1.3 Final Rule – The contractor shall prepare an economic analysis of the final rule, addressing comments received during the comment period, including any significant policy alternatives suggested by commenters that are not recommended for adoption, and other comments received relevant to the economic effects of the proposed rule; as well as realistic alternatives to the approach chosen. **(FIRM FIXED PRICE)**

3.2 TASK 2: PROPOSED AND FINAL RULE TO IMPLEMENT THE MAKE PPE IN AMERICA ACT

3.2.1 Proposed Rule – During the comment period, the contractor shall provide technical writing support and comment processing support for responses to any internal and external passbacks. **(LABOR HOUR)**

3.2.2 Proposed Rule – The contractor shall attend meetings with commenters or other third parties, when requested, regarding the proposed rule, particularly in those instances when DHS expects that the outside party will provide additional data or comment upon the economic analysis or data contained in the proposing release. **(LABOR HOUR)**

3.2.3 Final Rule – The contractor shall prepare an economic analysis of the final rule, addressing comments received during the comment period, including any significant policy alternatives suggested by commenters that are not recommended for adoption, and other comments received relevant to the economic effects of the proposed rule; as well as realistic alternatives to the approach chosen. **(FIRM FIXED PRICE)**

~~3.3 TASK 3: PROPOSED AND FINAL RULE TO IMPLEMENT EO 14035 "DIVERSITY, EQUITY, INCLUSION, AND ACCESSIBILITY IN THE FEDERAL WORKFORCE"~~

~~3.3.1 Proposed Rule—During the comment period, the contractor shall provide technical writing support and comment processing support for responses to any internal and external passbacks. (LABOR HOUR)~~

~~3.3.2 Proposed Rule—The contractor shall attend meetings with commenters or other third parties, when requested, regarding the proposed rule, particularly in those instances when DHS expects that the outside party will provide additional data or comment upon the economic analysis or data contained in the proposing release. (LABOR HOUR)~~

~~3.3.3 Final Rule—The contractor shall prepare an economic analysis of the final rule, addressing comments received during the comment period, including any significant policy alternatives suggested by commenters that are not recommended for adoption, and other comments received relevant to the economic effects of the proposed rule; as well as realistic alternatives to the approach chosen. (FIRM FIXED PRICE)~~

3.4 TASK 4: PROPOSED RULE TO IMPLEMENT HSAR CLASS DEVIATION 23-02 "IMPLEMENTATION OF THE HOMELAND PROCUREMENT REFORM ACT"

3.4.1 The contractor shall prepare an explanation of the policy and the economic rationale for regulatory action, including the problem to be addressed, the goals sought to be achieved, and a high-level discussion of the likely elements of the economic analyses (e.g., the nature and scale of expected market impacts from the main regulatory alternatives under consideration, and the impact on small entities), and additional data needs. **(FIRM FIXED PRICE)**

3.4.2 The contractor shall complete the economic analyses of the most likely economic consequences of the rule, to include a discussion on the economic baseline used to measure the likely economic impact of the rule in terms of potential benefits and costs; and evaluation of the reasonable alternatives to the proposed regulatory approach, including alternatives to not pursuing the rule. Analyses shall be consistent with the standards of the RFA, E.O. 12866, OMB Circular A-4, and E.O. 13563. The contractor shall collaborate with DHS throughout the course of writing the proposed rule to ensure it is structured to impose the least burden on society, while meeting the objectives of the agency. **(FIRM FIXED PRICE)**

3.4.3 The contractor shall provide technical writing support and comment processing support for responses to any internal and external passbacks. **(LABOR HOUR)**

4.0 PERIOD OF PERFORMANCE

The period of performance is September 19, 2023 to September 18, 2024.

5.0 PLACE OF PERFORMANCE

The work to be performed under this contract shall be performed at the contractor's facility.

6.0 TRAVEL

Travel is not anticipated under this requirement.

7.0 DELIVERABLES

The Contractor shall provide all deliverables in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows OS and Microsoft Office Applications, Adobe Acrobat, and any successor/updated applications). All technical writing shall be in accordance with the Federal Register Drafting Handbook.

TASK	REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	**Task 3.1.1**	Technical Writing & Comment Processing Support	5 business days after receipt of comment(s)	COR
2	**Task 3.1.2**	Meetings	As needed	COR
3	**Task 3.1.3**	Regulatory Economic Analysis for Final Rule	3 months after request	COR
5	**Task 3.2.1**	Technical Writing & Comment Processing Support	5 business days after receipt of comment(s)	COR
5	**Task 3.2.2**	Meetings	As needed	COR
6	**Task 3.2.3**	Regulatory Economic Analysis for Final Rule	3 months after request	COR

TASK	REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
~~7~~	~~Task 3.3.1~~	~~Technical Writing & Comment Processing Support~~	~~5 business days after receipt of comment(s)~~	~~COR~~
~~8~~	~~Task 3.3.2~~	~~Meetings~~	~~As needed~~	~~COR~~
~~9~~	~~Task 3.3.3~~	~~Regulatory Economic Analysis for Final Rule~~	~~3 months after request~~	~~COR~~
10	**Task 3.4.1**	Explanation of Policy & Economic Rationale for HSAR Class Deviation 13-01	2 months after award	COR
11	**Task 3.4.2**	Regulatory Economic Analysis for HSAR Class Deviation 23-02	5 months after award	COR
12	**Task 3.4.3**	Technical Writing & Comment Processing Support	5 business days after receipt of comment(s)	COR
13	**Section 10.0**	Progress Reports	3rd of every month	COR
14	**Section 10.0**	Progress Meetings	Upon Request	COR

8.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance, if applicable. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

Generally, the COR will have 8 business days to review deliverables and make comments. The Contractor shall have no more than 8 business days to make corrections and re-deliver. Shorter time periods (i.e., 5 business days) may be required of both parties for regulatory support services work if supporting an inflexible regulatory timeframe.

9.0 GOVERNMENT FURNISHED RESOURCES

The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract, and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data, and documents to outside parties without the prior and explicit consent of the Contracting Officer.

10.0 PROGRESS REPORTS & MEETINGS

The contractor shall provide a monthly progress report to the COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours used (if applicable), an assessment of technical progress, schedule status, and any Contractor concerns or recommendations for the previous reporting period.

The contractor shall be available to meet with the COR(s) upon request to present deliverables, discuss progress, exchange information, and resolve emergent technical problems and issues. These meetings shall take place via teleconference.

11.0 CONTRACTOR PERSONNEL

The contractor shall provide qualified personnel and the management, quality control, and supervision necessary to perform all requirements specified in this SOW. Contractor personnel must meet the following minimum requirements.
Subject matter experience and expertise in macro- and micro-economics and policy, including but not limited to impact assessments; cost-benefit analysis, pricing, supply, demand, and labor markets; quantitative and qualitative data collection, analysis and research using original and secondary data and sources; and recent and emerging economic trends.
The contractor shall have demonstrated experience and expertise addressing requirements in the following:

- E.O. 12866, "Regulatory Planning and Review" (September 30, 1993)
- E.O. 13563, "Improving Regulation and Regulatory Review," (January 18, 2011)
- Regulatory Flexibility Act (RFA 5 U.S.C. 601-612)
- Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA)
- Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1501-1571)
- OMB Circular A-4, Regulatory Analysis (September 17, 2003)
- Administrative Procedure Act
- Improving Regulation and Regulatory Review (E.O. 13563),
- Collection of Information (Paperwork Reduction Act (44 U.S.C. 3501-3520))
- Information Quality Act (Data Quality Act (Pub. L. 106-554, 114 Stat. 2763A-153))

- Proper Consideration of Small Entities in Agency Rulemaking (E.O. 13272))

12.0 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

1. QUALIFIED PERSONNEL

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

2. KEY PERSONNEL

Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace Key Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement:

- Regulatory Economist

3. REPLACEMENT OF KEY PERSONNEL

Before replacing any individual designated as Key by the Government, the Contractor must notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes must possess qualifications equal to or superior to those of the Key person being replaced. The Contractor must not replace Key Contractor personnel without acknowledgment from the Contracting Officer.

4. CONTINUITY OF SUPPORT

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

5. EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify

themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

6. EMPLOYEE CONDUCT

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

1.6.1 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion (via the Contracting Officer*), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

13.0 OTHER APPLICABLE CONDITIONS

13.1 SECURITY

Contractor access to unclassified, but Security Sensitive Information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

13.2 REQUESTS FOR EXCEPTION TO U.S. CITIZENSHIP REQUIREMENT

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or

through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS OCSO.

This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

14.0 POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

- Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.
- Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigation s will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement , addition, subcontractor employee, or vendor:
  a. Standard Form 85P, "Questionnaire for Public Trust Positions"
  b. FD Form 258, "Fingerprint Card" (2 copies)
  c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
  d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Report Pursuant to the Fair Credit Reporting Act"
- Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.
- DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as

assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office. No employee of the Contractor shall be allowed to EOD and/or access sensitive information or systems without a favorable EOD decision or suitability determination.

- Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.
- The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.
- When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Depa1iment security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).
- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- Your POC at the Security Office is:
  DHS OCSO/PSD Security Customer Service Center
  [redacted]

SECTION III – TASK ORDER ADMINISTRATION

1. Contract Administration

1.1 Contracting Officer

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds and authorize revisions of the terms and conditions of this order The Contracting Officer shall authorize any such revision in writing. If the contractor makes any changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the order to cover any increases in changes that may result. The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the order in accordance with its terms and conditions.

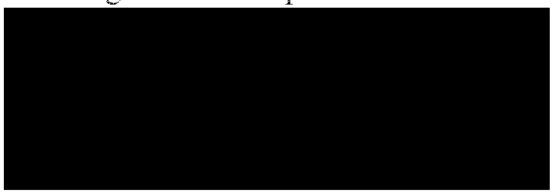
The Contracting Officer is:

The Contract Specialist is:

1.2 Contracting Officer's Representative (COR)

The Contracting Officer will designate a COR to assist in monitoring the work under this order. The COR is responsible for the technical administration of the order and technical liaison between the Contractor and the Government. The COR is not authorized to change the scope of work or specifications stated in the order, to make any commitments, or otherwise obligate the Government or authorize any changes which affect the order price, delivery schedule, period of performance, or other terms and conditions.

The Contracting Officer's Representative is:



SECTION IV: INVOICE AND PAYMENT PROVISIONS AND GOVERNMENT ACCEPTANCE PERIOD

1. Invoices shall be prepared in accordance with Federal Acquisition Regulation (FAR) 52.212-4, Contract Terms and Conditions – Commercial Items. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

    a) Cover sheet identifying DHS;
    b) Order Number;
    c) Modification Number, if any;
    d) UEI Number;
    e) Dates of provided services; and
    f) Associated Contract Line Item Number (CLIN).

2. Invoices shall be submitted electronically to [redacted] with a courtesy copy to the Contracting Officer and the COR. Invoices shall be submitted in monthly arrears.

    In addition to submitting invoices to the email address above, the Contractor shall also copy the Contracting Officer ([redacted] the Contract Specialist [redacted] and the Contracting Officer's Representative [redacted] on all invoice submissions.

3. Government Acceptance Period

3.1 The COR will review deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance, if applicable. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

3.2 In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

3.3 The timeline for review is provided in Section II, Section 2.4: Constraints.

SECTION V – SPECIAL CONTRACT REQUIREMENTS

All Special Contract Requirements of the Offeror's DHS BPA remain unchanged and in full force and effect.

SECTION VI - CONTRACT CLAUSES

All terms, conditions, and clauses of the Offeror's DHS BPA remain unchanged and in full force and effect.

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 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 to the Contracting

Officer, unless elsewhere in this contract are established procedures for reporting the information; 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 Contracting Officer for the indefinite delivery contract and the Contracting Officer(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)

52.217-8 Option to Extend Services. (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

(End of clause)

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 Public Law 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 (Anumbers),
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-andtraining-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 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)

3052.204–73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents (July 2023)

(a) *Definitions.* 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.

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

(2) 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:

(i) Truncated SSN (such as last 4 digits);

(ii) Date of birth (month, day, and year);

(iii) Citizenship or immigration status;

(iv) Ethnic or religious affiliation;

(v) Sexual orientation;

(vi) Criminal history;

(vii) Medical information; and

(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

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

(b) *PII and SPII Notification Requirements.* (1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (*e.g.,* credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

(ii) A description of the types of PII or SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (*i.e.,* those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of 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 clause)