9110-9B

DEPARTMENT OF HOMELAND SECURITY

48 CFR Parts 3001, 3002, 3039 and 3052

Docket No. DHS-2017-0007

RIN 1601-AA78

Homeland Security Acquisition Regulation (HSAR); Information Technology Security Awareness Training (HSAR Case 2015-002)

AGENCY: Office of the Chief Procurement Officer, Department of Homeland Security (DHS).

ACTION: Proposed rule.

SUMMARY: DHS is proposing to amend the Homeland Security Acquisition Regulation (HSAR) to add a new subpart, update an existing clause, and add a new contract clause to standardize information technology security awareness training and DHS Rules of Behavior requirements for contractor and subcontractor employees who access DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting controlled unclassified information (CUI).

DATES: Interested parties should submit written comments to one of the addresses shown below on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], to be considered in the formation of the final rule.

ADDRESSES: Submit comments identified by HSAR Case 2015-002, Information Technology Security Awareness Training, using any of the following methods:

- Regulations.gov: *http://www.regulations.gov*.

Submit comments via the Federal eRulemaking portal by entering "HSAR Case 2015–002" under the heading "Enter Keyword or ID" and selecting "Search." Select the link "Submit a Comment" that corresponds with "HSAR Case 2015-002." Follow the instructions provided at the "Submit a Comment" screen. Please include your name, company name (if any), and "HSAR Case 2015–002" on your attached document.

- Fax: (202) 447-0520
- Mail: Department of Homeland Security, Office of the Chief Procurement Officer, Acquisition Policy and Legislation, ATTN: Ms. Shaundra Duggans, 245 Murray Drive, Bldg. 410 (RDS), Washington, DC 20528.

Comments received generally will be posted without change to *http://www.regulations.gov*, including any personal information provided. To confirm receipt of your comment(s), please check www.regulations.gov, approximately two to three days after submission to verify posting (except allow 30 days for posting of comments submitted by mail).

FOR FURTHER INFORMATION CONTACT: Ms. Shaundra Duggans, Procurement Analyst, DHS, Office of the Chief Procurement Officer, Acquisition Policy and Legislation at (202) 447-0056 or email *HSAR@hq.dhs.gov*. When using email, include HSAR Case 2015-002 in the "Subject" line.

SUPPLEMENTARY INFORMATION:

I. Background

DHS contracts currently require contractor and subcontractor employees to complete information technology (IT) security awareness training before accessing DHS

information systems and information resources. This training is initially completed upon award of the procurement and at least annually thereafter. DHS contracts also require such employees to sign the DHS Rules of Behavior (RoB) before access is provided to DHS information systems and information resources. The DHS RoB is a document that defines the responsibilities and obligations imposed on all individuals with access to DHS information systems and information resources. The DHS RoB holds users accountable for actions taken while accessing DHS information systems and using DHS information resources capable of collecting, processing, storing or transmitting controlled unclassified information (CUI).

DHS is proposing to (1) include IT security awareness training and RoB requirements in the HSAR and (2) make the training and RoB more easily accessible by hosting them on a public website. This approach ensures all applicable DHS contractors and subcontractors are subject to the same IT security awareness training and RoB requirements while removing the need for Government intervention to provide access to the IT security awareness training and RoB.

This rule proposes to standardize the IT security awareness training and DHS RoB requirements across DHS contracts by amending the HSAR to:

(1) Add the terms "controlled unclassified information," "information resources" and "information system" to HSAR 3002.1, Definitions and remove the definition of the term "sensitive information" at HSAR 3002.1, Definitions. The definition of "controlled unclassified information" is taken from its implementing regulation at 32 CFR Part 2002. The definitions of "information resources" and "information system" are derived from 44 U.S.C. 3502(6) and 44 U.S.C. 3502(8) respectively. The definition of "sensitive

information" is removed because it is being replaced with "controlled unclassified information" consistent with Executive Order 13556 and its implementing regulation at 32 CFR Part 2002. These definitions are necessary because these terms appear in proposed HSAR 3039.70 Information Technology Security Awareness Training and HSAR 3052.239-7X, Information Technology Security Awareness Training.

(2) Add a new subpart at 3039.70, Information Technology Security Awareness Training. HSAR 3039.7001, Scope, identifies the applicability of the subpart to contracts and subcontracts where contractor and subcontractor employees may have access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI. HSAR 3039.7002, Policy, subparagraph (a) requires contractors and subcontractors that may have access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI to complete IT security awareness training initially upon award of the procurement and annually thereafter. This subsection requires the contractor to maintain evidence that the training has been completed and provide copies of the training completion certificates to the contracting officer. Subparagraph (b) requires contractor and subcontractor employees to sign the DHS RoB before receiving access to DHS information systems and/or information resources and before contractor-owned and/or operated information systems can be used to collect, process, store, or transmit CUI. This subsection requires the contractor to maintain signed copies of the DHS Rob and provide signed copies to the contracting officer. HSAR 3039.7003, Contract Clause, identifies when contracting

officers must insert HSAR 3052.239-7X, Information Technology Security Awareness Training, in solicitations and contracts.

(3) Amend subparagraph (b) of the clause at HSAR 3052.212-70, Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items, to add HSAR 3052.239-7X Information Technology Security Awareness Training. This change is necessary because HSAR 3052.239-7X is applicable to the acquisition of commercial items.

(4) Add a new subsection at HSAR 3052.239-7X, Information Technology Security Awareness Training, to provide the text of the proposed clause. The proposed clause requires contractor and subcontractor employees to complete IT security awareness training before accessing DHS information systems/information resources and before contractor-owned and/or operated information systems are used to collect, process, store, or transmit CUI. Training shall be completed within thirty (30) days of contract award and on an annual basis thereafter. The contractor shall maintain copies of training certificates for all contractor and subcontractor employees as a record of compliance and provide copies of the training certificates to the contracting officer. Subsequent training certificates to satisfy the annual IT security awareness training requirement shall be submitted via e-mail notification not later than October 31st of each year. The contractor shall attach training certificates to the email notification and the email notification shall state the required training has been completed for all contractor and subcontractor employees. The proposed clause also requires the contractor to ensure all employees and subcontractor employees sign the DHS RoB before accessing DHS information systems and information resources. The DHS RoB shall also be signed before a contractor-owned

and/or operated information system or information resource can be used to collect, process, store or transmit CUI and before contractor and/or subcontractor employees can access the information system or information resource. The contractor shall maintain signed copies of the DHS RoB for all contractor and subcontractor employees as a record of compliance and provide signed copies of the RoB to the contracting officer not later than thirty (30) days after contract award.

These proposed revisions to the HSAR are necessary to ensure contractors and subcontractors understand their roles and responsibilities in ensuring the security of systems and the confidentiality, integrity, and availability of CUI. They are consistent with the provisions of (1) the Federal Information Security Modernization Act of 2014 (FIMSA) (44 U.S.C. 3551, *et seq.*) and (2) Title 5, Code of Federal Regulations, Part 930, Subpart C, (5 CFR 930.301). 44 U.S.C. 3554(b)(4) requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities; and their responsibilities in complying with agency policies and procedures designed to reduce these risks. 5 CFR 930.301 requires all users of Federal information systems be exposed to security awareness materials at least annually. Users of Federal information systems include employees, contractors, students, guest researchers, visitors, and others who may need access to Federal information systems and applications.

This proposed rule is part of a broader initiative within DHS to (1) ensure contractors understand their responsibilities with regard to safeguarding controlled unclassified information (CUI); (2) contractor and subcontractor employees complete

information technology (IT) security awareness training before access is provided to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources where CUI is collected, processed, stored or transmitted on behalf of the agency; (3) contractor and subcontractor employees sign the DHS RoB before access is provided to DHS information systems, information resources, or contractor-owned and/or operated information systems and information resources where CUI is collected, processed, stored or transmitted on behalf of the agency; and (4) contractor and subcontractor employees complete privacy training before accessing a Government system of records; handling personally identifiable information (PII) and/or sensitive PII information; or designing, developing, maintaining, or operating a system of records on behalf of the Government.

II. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, is subject to review under Section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804. DHS has included a discussion of the estimated costs and benefits of this rule in the Paperwork Reduction Act supporting statement, which can be found in the docket for this rulemaking.

III. Regulatory Flexibility Act

DHS expects this proposed rule may have an impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.*, because the proposed rule requires contractor and subcontractor employees who will need access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting controlled unclassified information (CUI) to be properly trained on the requirements, applicable laws, and appropriate safeguards designed to ensure the security and confidentiality of the information systems and information resources. Therefore, an Initial Regulatory Flexibility Analysis (IRFA) has been prepared consistent with 5 U.S.C. 603, and is summarized as follows:

1. Description of the reasons why action by the agency is being taken.

DHS is proposing to amend the HSAR to require that all contractor and subcontractor employees who will need access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI complete IT security awareness training and sign the DHS RoB before access to such systems and resources is granted. The purpose of this action is to require contractors to identify its employees who require access, ensure that those employees complete IT security awareness training before being granted access and annually thereafter, provide the Government evidence of the completed training, and maintain evidence of completed training in accordance with the records retention requirements of the contract.

2. Succinct statement of the objectives of, and legal basis for, the rule.

The objective of this proposed rule is to require contractor and subcontractor employees to complete IT security awareness training before access is granted to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI.

The training imposed by this rule is required by the provisions of FISMA (44 U.S.C. 3551, *et seq.*) and Title 5, Code of Federal Regulations, Part 930, Subpart C, (5 CFR 930.301). 44 U.S.C. 3554(b)(4) requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities; and their responsibilities in complying with agency policies and procedures designed to reduce these risks. 5 CFR 930.301 requires all users of Federal information systems be exposed to security awareness materials at least annually.

3. Description of and, where feasible, estimate of the number of small entities to which the rule will apply.

This proposed rule will apply to contractor and subcontractor employees who require access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI. The estimated number of small entities to which the rule will apply is 2,185 respondents of which 1,212 are projected to be small businesses.

This estimate is based on a review and analysis of internal DHS contract data and Fiscal Year (FY) 2014 data reported to the Federal Procurement Data System (FPDS). It is anticipated that this rule will be primarily applicable to procurement actions with a Product and Service Code (PSC) of "D" Automatic Data Processing and Telecommunication. PSCs will be adjusted as additional data becomes available through HSAR clause implementation to validate future burden projections.

4. Description of projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary.

The projected reporting and recordkeeping associated with this proposed rule is kept to the minimum necessary to meet the overall objectives. For instance, DHS has minimized the burden by making the IT security awareness training and DHS RoB publicly accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. IT security awareness training shall be completed within thirty (30) days of contract award and on an annual basis thereafter. Training certificates are automatically generated at the conclusion of the training. The DHS RoB shall be signed before contractor and subcontractor employees can access DHS information systems and information. The DHS RoB shall also be signed before a contractor-owned and/or operated information system or information resource can be used to collect, process, store or transmit CUI and before contractor and/or subcontractor employees can access the information system. Initial training certificates for each contractor and subcontractor employee, and signed copies of the RoB, shall be provided to the Government not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the

annual IT security awareness training requirement shall be submitted via e-mail notification not later than October 31st of each year. The contractor shall attach training certificates to the email notification and the email notification shall state the required training has been completed for all contractor and subcontractor employees.

5. Identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap, or conflict with the rule.

There are no rules that duplicate, overlap or conflict with this rule.

6. Description of any significant alternatives to the rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities.

There are no practical alternatives that will accomplish the objectives of the proposed rule. In an effort to reduce duplication and to address common IT security training requirements across Government, DHS has partnered with the Defense Information Systems Agency (DISA) to provide its online IT security awareness training, CyberAwareness Challenge, for DHS contractor and subcontractor employees. Common IT security awareness training provides a streamlined, efficient, and cost-effective solution for DHS to provide IT security awareness training for contractor and subcontractor employees.

DHS will be submitting a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the point of contact specified herein. DHS invites comments from small business concerns and other interested parties on the expected impact of this rule on small entities.

DHS will also consider comments from small entities concerning the existing regulations in subparts affected by this rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610, (HSAR Case 2015-002), in correspondence.

IV. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. chapter 35) applies because this proposed rule contains information collection requirements. Accordingly, DHS will be submitting a request for approval of a new information collection requirement concerning this rule to the Office of Management and Budget under 44 U.S.C. 3501, *et seq.*

A. Public reporting burden for this collection of information is estimated to be approximately 30 minutes (.50 hours) per response to comply with the requirements, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The total annual projected number of responses per respondent is estimated to be four (4). The annual total burden hours are estimated as follows:

Title: Homeland Security Acquisition Regulation: Information Technology Security Awareness Training.

Type of Request: New Collection.

Number of Respondents: 2,185

Responses per Respondent: 4

Annual Responses: 8,740

Average Burden per Response: Approximately 0.50

Annual Burden Hours: 4,370

Needs and Uses: DHS needs the information required by 3052.239-7X, Information Technology Security Awareness Training, to properly track contractor compliance with the training and DHS RoB requirements identified in the clause.

Affected Public: Businesses or other for-profit institutions.

Respondent's Obligation: Required to obtain or retain benefits.

Frequency: Upon award of procurement and annually thereafter.

B. Request for Comments Regarding Paperwork Burden

You may submit comments identified by DHS docket number [DHS-2017-0007], including suggestions for reducing this burden, not later than [insert date 60 days after publication in the FEDERAL REGISTER] using any one of the following methods:

(1) Via the internet at Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

(2) Via email to the Department of Homeland Security, Office of the Chief Procurement Officer, at *HSAR@hq.dhs.gov*.

Public comments are particularly invited on: whether this collection of information is necessary for the proper performance of functions of the HSAR, and will have practical utility; whether our estimate of the public burden of this collection of information is accurate, and based on valid assumptions and methodology; ways to enhance the quality, utility, and clarity of the information to be collected; and ways in which we can minimize the burden of the collection of information on those who are to respond, through the use of appropriate technological collection techniques or other forms of information technology.

Requesters may obtain a copy of the supporting statement from the Department of Homeland Security, Office of the Chief Procurement Officer, Acquisition Policy and Legislation, via email to *HSAR@hq.dhs.gov*. Please cite OMB Control No. 1600-0022, Privacy Training and Information Technology Security Awareness Training, in the "Subject" line.

List of Subjects in 48 CFR Parts 3001, 3002, 3039 and 3052

Government procurement.

Therefore, DHS proposes to amend 48 CFR parts 3001, 3002, 3039 and 3052 as follows:

1. The authority citation for parts 3001 and 3002 is revised to read as follows:

Authority: 5 U.S.C. 301-302, 41 U.S.C. 1707, 41 U.S.C. 1702, 41 U.S.C. 1303(a)(2), 48 CFR part 1, subpart 1.3, and DHS Delegation Number 0702.

PART 3001—FEDERAL ACQUISITION REGULATIONS SYSTEM

2. In section 3001.106 amend paragraph (a) by adding a new OMB Control Number as follows:

3001.106 OMB Approval under the Paperwork Reduction Act.

(a) * * *

OMB Control No. 1600-0022 (Information Technology Security Awareness Training)

* * * * *

PART 3002—DEFINITIONS OF WORDS AND TERMS

3. Amend section 3002.101 by adding, in alphabetical order, the definitions for Controlled Unclassified Information (CUI)," ""Information Resources," and "Information System" to read as follows:

*****

"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 Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. Within the context of DHS, this includes such information which, if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy of individuals. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in Title 6, Code of Federal Regulations, 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 II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29)

as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(3) Sensitive Security Information (SSI) as defined in Title 49, Code of Federal Regulations, 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 his/her designee) to include DHS MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2010.1, "SSI Program";

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

(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 DHS receives pursuant to 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, that is required by that agreement or arrangement to be protected;

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

(i) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information 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;

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of DHS, 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 information that could constitute an indicator of U.S. Government intentions, capabilities, operations, or activities or otherwise threaten operations security;

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

(10) Physical Security Information means reviews or reports illustrating or disclosing DHS 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, which includes information referred to as Personally Identifiable Information (PII). PII 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; and

(12) Sensitive Personally Identifiable Information (SPII) is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements.

(i) Examples of stand-alone PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan.

(ii) Additional examples of SPII include any groupings of information that contain 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

(H) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

(iii) Other PII may be SPII depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not SPII.

*****

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

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

*****

4. Revise part 3039 to read as follows:

PART 3039--ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 3039.70 Information Technology Security Awareness Training

3039.7001 Scope.

3039.7002 Policy.

3039.7003 Contract Clause.

Authority: 5 U.S.C. 301-302, 41 U.S.C. 1707, 41 U.S.C. 1702, 41 U.S.C. 1303(a)(2), 48 CFR part 1, subpart 1.3, and DHS Delegation Number 0702.

3039.7001 Scope.

This section applies to contracts and subcontracts where contractor and subcontractor employees may have access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting controlled unclassified (CUI) information.

3039.7002 Policy.

(a) Contractors and subcontractors that may have access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI shall take IT security awareness training initially upon award of the procurement and annually thereafter. The contractor shall ensure such employees complete the required training, maintain evidence that the training has been completed and provide copies of the training completion certificates to the Contracting Officer and/or Contracting Officer's Representative (COR) for inclusion in the contract file.

(b) The DHS Rules of Behavior (RoB) is a document that informs users of their responsibilities and obligations when accessing DHS information systems and/or information resources. The RoB also informs users that they will be held accountable for actions taken while accessing DHS information systems and/or using DHS information resources. Contractor and subcontractor employees shall sign the DHS RoB before receiving access to DHS information systems and/or information resources. In addition,

contractor and subcontractor employees shall sign the DHS RoB before a contractor-owned and/or operated information system or information resource can be used to collect, process, store or transmit CUI. The contractor shall maintain signed copies of the DHS RoB for all contractor and subcontractor employees as a record of compliance, in accordance with the records retention requirements of the contract, and provide signed copies of the DHS RoB to the Contracting Officer and/or COR for inclusion in the contract file.

3039.7003 Contract Clause.

Contracting officers shall insert the clause at (HSAR) 48 CFR 3052.239-7X, Information Technology Security Awareness Training, in solicitations and contracts where contractor and subcontractor employees, during the course of performance, may gain access to DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI.

PART 3052—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

5. The authority citation for part 3052 is revised to read as follows:

Authority: 5 U.S.C. 301-302, 41 U.S.C. 1707, 41 U.S.C. 1702, 41 U.S.C. 1303(a)(2), 48 CFR part 1, subpart 1.3, and DHS Delegation Number 0702.

Clause 3052.212-70 [Amended]

6. Amend paragraph (b) of section 3052.212-70 to add 3052.239-7X Information Technology Security Awareness Training as follows:

3052.212-70 Contract terms and conditions applicable to DHS acquisition of commercial items.

CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (DATE)

* * * * *

(b) * * *

____3052.239-7X Information Technology Security Awareness Training

7. Amend part 3052 by adding section 3052.239-7X to read as follows:

3052.239-7X Information technology security awareness training.

As prescribed in (HSAR) 48 CFR 3039.7004 contract clause, insert the following clause:

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (DATE)

(a) *Information Technology Security Awareness Training.* The Contractor shall ensure that all employees and subcontractor employees complete information technology (IT) security awareness training before access is provided to DHS information systems and information resources. The Contractor shall also ensure that employees and subcontractor employees complete IT security awareness training before a contractor-owned and/or operated information system or information resource can be used to collect, process, store or transmit controlled unclassified information (CUI). 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 and subcontractor employees assigned to the contract shall complete the training before accessing DHS information systems and information resources or contractor-owned and/or operated information systems and information resources capable of collecting,

processing, storing or transmitting CUI under the contract. IT security awareness 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. Initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer and/or Contracting Officer's Representative (COR) not later than thirty (30) days after contract award or assignment to the contract. Subsequent training certificates to satisfy the annual IT security awareness training requirement shall be submitted to the Contracting Officer and/or COR via e-mail notification not later than October 31st of each year. The Contractor shall attach training certificates to the email notification and the email notification shall list all Contractor and subcontractor employees required to take the training and state the required IT security awareness training has been completed for all Contractor and subcontractor employees.

(b) *Rules of Behavior.* The Contractor shall ensure that all employees and subcontractor employees sign the DHS Rules of Behavior (RoB) before access is provided to DHS information systems and information resources. The Contractor shall also ensure that employees and subcontractor employees sign the DHS RoB before a contractor-owned and/or operated information system or information resource can be used to collect, process, store or transmit CUI and before access to the contractor-owned and/or operated information system or information resource is provided to the employee. The RoB shall be signed within thirty (30) days of contract award. Any new Contractor employees and subcontractor employees assigned to the contract shall also sign the DHS RoB before accessing DHS information systems and information resources or contractor-

owned and/or operated information systems and information resources capable of collecting, processing, storing or transmitting CUI. The DHS RoB is accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The Contractor shall maintain signed copies of the DHS RoB for all Contractor and subcontractor employees as a record of compliance. Signed copies of the RoB shall be provided to the Contracting Officer and/or COR not later than thirty (30) days after contract award or assignment to the contract. The DHS RoB will be reviewed annually and the COR will provide notification when a review is required.

(c) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower-tier subcontracts.

(End of clause)

Soraya Correa

Chief Procurement Officer, Department of Homeland Security

[FR Doc. 2017-00754 Filed: 1/18/2017 8:45 am; Publication Date: 1/19/2017]