Dated: January 9, 2017.

Sylvia M. Burwell,

Secretary, Department of Health and Human Services.

[FR Doc. 2017–00700 Filed 1–18–17; 8:45 am]

BILLING CODE 4165–15–P

DEPARTMENT OF HOMELAND SECURITY

48 CFR Parts 3001, 3002, 3024, and 3052

[Docket No. DHS–2017–0008]

RIN 1601–AA79

Homeland Security Acquisition Regulation (HSAR); Privacy Training (HSAR Case 2015–003)

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 require contractors to complete training that addresses the protection of privacy, in accordance with the Privacy Act of 1974, and the handling and safeguarding of Personally Identifiable Information and Sensitive Personally Identifiable Information.

DATES: Interested parties should submit written comments to one of the addresses shown below on or before March 20, 2017, to be considered in the formation of the final rule.

ADDRESSES: Submit comments identified by HSAR Case 2015–003, Privacy Training, using any of the following methods:

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

Submit comments via the Federal eRulemaking portal by entering ''HSAR Case 2015–003'' under the heading ''Enter Keyword or ID'' and selecting ''Search.'' Select the link ''Submit a Comment'' that corresponds with ''HSAR Case 2015–003.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''HSAR Case 2015–003'' 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. Candace Lightfoot, 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 *http://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. Candace Lightfoot, Procurement Analyst, DHS, Office of the Chief Procurement Officer, Acquisition Policy and Legislation at (202) 447–0882 or email *HSAR@hq.dhs.gov.* When using email, include HSAR Case 2015–003 in the ''Subject'' line.

SUPPLEMENTARY INFORMATION:

I. Background

DHS contracts currently require contractor and subcontractor employees to complete privacy training before accessing a Government system of records; handling Personally Identifiable Information (PII) or Sensitive PII (SPII); or designing, developing, maintaining, or operating a Government system of records. This training is completed upon award of the procurement and at least annually thereafter.

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

This proposed rule standardizes the Privacy training requirement across all DHS contracts by amending the HSAR to:

(1) Add the terms ''personally identifiable information'' and ''sensitive personally identifiable information'' at HSAR 3002.1, Definitions. The definition of ''personally identifiable information'' is taken from OMB Circular A–130 Managing Information as a Strategic Resource,[1] published July 27, 2016. The definition of ''sensitive personally identifiable information'' is derived from the DHS lexicon, Privacy Incident Handling Guidance, and the Handbook for Safeguarding Sensitive Personally Identifiable Information. These definitions are necessary because these terms appear in proposed HSAR 3024.70, Privacy Training and HSAR 3052.224–7X, Privacy Training.

(2) Add a new subpart at HSAR 3024.70, Privacy Training addressing the requirements for privacy training. HSAR 3024.7001, Scope identifies the applicability of the subpart to contracts and subcontracts. HSAR 3024.7002, Definitions defines the term ''handling.'' The definition of ''handling'' was developed based upon a review of definitions for the term developed by other Federal agencies. HSAR 3024.7003, Policy identifies when contractors and subcontracts are required to complete the DHS privacy training. This subsection also requires the submission of training completion certificates for all contractor and subcontractor employees as a record of compliance. HSAR 3024.7004, Contract Clause, identifies when Contracting Officers must insert HSAR 3052.224–7X Privacy Training in solicitations and contracts. DHS welcomes respondents to offer their views on the following questions in particular:

A. What burden, if any, is associated with the requirement to complete DHS-developed privacy training?

B. What value, if any, is associated with providing industry the flexibility to develop its own privacy training given a unique set of Government requirements?

(3) Amend sub paragraph (b) of the HSAR 3052.212–70, Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items to add HSAR 3052.224–7X, Privacy Training. This change is necessary because HSAR 3052.224–7X is applicable to the acquisition of commercial items; and

(4) Add a new subsection at HSAR 3052.224–7X, Privacy Training to provide the text of the proposed clause. The proposed clause requires contractor and subcontractor employees to complete privacy training before accessing a Government system of records; handling Personally Identifiable Information (PII) or Sensitive PII (SPII); or designing, developing, maintaining, or operating a Government system of records. The 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 privacy training requirement shall be submitted via email notification not later than October 31st of each year. The contractor shall attach training certificates to the email

[1] OMB Circular A–130 *Managing Information as a Strategic Resource* is accessible at *https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.*

notification and the email notification shall state that the required training has been completed for all contractor and subcontractor employees.

These proposed revisions to the HSAR are necessary to ensure contractors and subcontractors properly handle PII and SPII. This includes PII and SPII contained in a system of records consistent with subsection (e) Agency requirements, and subsection (m) Government contractors, of the Privacy Act of 1974, Section 552a of title 5, United States Code (5 U.S.C. 552a).

Other applicable authorities that address the responsibility for Federal agencies to ensure appropriate handling and safeguarding of PII include the following Office of Management and Budget (OMB) memoranda and policies: OMB Memorandum M–07–16, ''Safeguarding Against and Responding to the Breach of Personally Identifiable Information'' issued May 22, 2007; OMB Memorandum M–10–23, ''Guidance for Agency Use of Third-Party Web sites and Applications'' issued June 25, 2010 (this memorandum contains the most current definition of PII, and clarifies the definition provided in M–07–16); OMB Circular No. A–130 ''Managing Information as a Strategic Resource,'' which identifies significant requirements for safeguarding and handling PII and reporting any theft, loss, or compromise of such information. DHS has also developed internal guidance that addresses the handling and protection of PII, including the DHS Privacy Incident Handling Guidance and the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information. The DHS Privacy Incident Handling Guidance informs DHS and its components, employees, senior officials, and contractors of their obligation to protect PII, and establishes policies and procedures defining how they must respond to the potential loss or compromise of PII. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information sets minimum standards for how DHS personnel and contractors should handle SPII in paper and electronic form during their work activities.

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). E.O. 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, was 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 to be properly trained on the requirements, applicable laws, and appropriate safeguards designed to ensure the security and confidentiality of PII before access a Government system of records; handle PII or SPII; or design, develop, maintain, or operate a system of records on behalf of the Government. Although the Privacy Act of 1974 has been in place for over 40 years, the rapidly changing information security landscape requires the Federal government to strengthen its contracts to ensure that contractor and subcontractor employees comply with the Act and are aware of their responsibilities for safeguarding PII and SPII. 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 all contractor and subcontractor employees that will have access to a Government system of records; handle PII or SPII; or design, develop, maintain, or operate a system of records on behalf of the Government, complete training that addresses the requirements for the protection of privacy and the handling and safeguarding of PII and SPII. The purpose of this proposed rule is to require contractors to identify its employees who require access, ensure that those employees complete privacy 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 rule is to require contractor and subcontractor employees to complete Privacy training before accessing a Government system of records; handling PII and/or SPII; or designing, developing, maintaining, or operating a Government system of records. This proposed rule requires contractors to identify who will be responsible for completing privacy training, and to emphasize and create awareness of the critical importance of privacy training in an effort to reduce the occurrences of privacy incidents.

The training imposed by this proposed rule is required by the provisions of the Privacy Act (5 U.S.C. 552a), Title III of the E-Government Act of 2002 and the Federal Information Security Modernization Act (FISMA) of 2014. This proposed rule requires contractors to identify its employees and subcontractor employees who require access to PII and SPII, ensure that those employees complete privacy training before being granted access to such information and annually thereafter, provide the Government evidence of the completed training, and maintain evidence of completed training.

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 a Government system of records; handle PII or Sensitive PII; or design, develop, maintain, or operate a system of records on behalf of the Government. The estimated number of small entities to which the rule will apply is 6,628 respondents of which 4,162 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 and ''R'' Professional, Administrative and Management Support. 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. DHS minimized the burden associated with this proposed rule by developing the training and making it publicly accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors.* DHS has also minimized burden by providing automatically generated certificates at the conclusion of the training. Training shall be completed within thirty (30) days of contract award and on an annual basis thereafter. Initial training certificates for each contractor and subcontractor employee shall be provided to the Government not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual privacy training requirement shall be submitted via email 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 that the required training has been completed for all contractor and subcontractor employees and include copies of the training certificates.

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.

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 2015–003), 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 at four (4). The estimated annual total burden hours are as follows:

Title: Homeland Security Acquisition Regulation: Privacy Training.

Type of Request: New Collection.

Number of Respondents: 6,628.

Responses per Respondent: 4.

Annual Responses: 26,512.

Average Burden per Response: Approximately 0.50.

Annual Burden Hours: 13,256.

Needs and Uses: DHS needs the information required by 3052.224–7X, Privacy Training to properly track contractor compliance with the training 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–2017–0008], including suggestions for reducing this burden, not later than March 20, 2017 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 Security Training, in the ''Subject'' line.

List of Subjects in 48 CFR Parts 3001, 3002, 3024 and 3052

Government procurement.

Therefore, DHS proposes to amend 48 CFR parts 3001, 3002, 3024 and 3052 to read as follows:

■ 1. The authority citation for 48 CFR parts 3001, 3002, 3024, and 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.

PART 3001—FEDERAL ACQUISITION REGULATIONS SYSTEM

Subpart 3001.1—Purpose, Authority, Issuance

■ 2. Amend section 3001.106 by revising paragraph (a) to add a new OMB Control Number as follows:

3001.106 OMB Approval under the Paperwork Reduction Act.

(a) * * *

OMB Control No. 1600–0022 (Privacy Training)

* * * * *

PART 3002—DEFINITIONS OF WORDS AND TERMS

■ 3. Amend section 3002.101 by adding, in alphabetical order, the definitions: for ''Personally Identifiable Information (PII),'' and ''Sensitive Personally Identifiable Information (SPII)'' to read as follows:

* * * * *

''Personally Identifiable Information (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.

* * * * *

''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.

(1) Examples of stand-alone SPII 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.

(2) 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:

(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

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

(3) 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.

PART 3024—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

■ 4. Amend part 3024 by adding subpart 3024.70:

Subpart 3024.70—Privacy Training

3024.7001 Scope.

This section applies to contracts and subcontracts where contractor and subcontractor employees require access to a Government system of records; handle Personally Identifiable Information (PII) or Sensitive PII (SPII); or design, develop, maintain, or operate a Government system of records.

3024.7002 Definitions.

As used in this subpart—

''Handling'' means any use of Personally Identifiable Information (PII) or Sensitive PII (SPII), including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

3024.7003 Policy.

(a) Contractors are responsible for ensuring that contractor and subcontractor employees complete DHS privacy training initially upon award of the procurement, and at least annually thereafter, before contractor and subcontractor employees—

(1) Access to a Government system of records;

(2) Handle PII or SPII; or

(3) Design, develop, maintain, or operate a system of records on behalf of the Government.

(b) The contractor shall ensure employees identified in paragraph (a) of this section 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 for inclusion in the contract file.

(c) Each contractor and subcontractor employee who requires access to a Government system of records; handles PII or SPII; or designs, develops, maintains, or operates a Government system of records, shall be granted access or allowed to retain such access only if the individual has completed Department of Homeland Security privacy training requirements.

3024.7004 Contract Clause.

Contracting officers shall insert the clause at (HSAR) 48 CFR 3052.224–7X, Privacy Training, in solicitations and contracts when contractor and subcontractor employees may have access to a Government system of records; handle PII or SPII; or design, develop, maintain, or operate a system of records on behalf of the Government.

PART 3052—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 5. Amend paragraph (b) of section 3052.212–70 to add 3052.224–7X Privacy 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) * * *

_____3052.224–7X Privacy Training

■ 6. Amend part 3052 by adding section 3052.224–7X Privacy Training, to read as follows:

3052.224–7X Privacy training.

As prescribed in (HSAR) 48 CFR 3024.7004 contract clause, insert the following clause:

Privacy Training (DATE)

(a) The Contractor shall ensure that all Contractor and subcontractor employees complete the Department of Homeland Security (DHS) training titled, Privacy at DHS: Protecting Personally Identifiable Information accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors,* before such employees—

(1) Access a Government system of records;

(2) Handle personally identifiable information or sensitive personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records on behalf of the Government.

(b) 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 or subcontractor employees assigned to the contract shall complete the training before accessing the information identified in paragraph (a) of this clause. The Contractor shall maintain copies of the 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) via email notification not later than thirty (30) days after contract award or assignment to the contract. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the Contracting Officer and/or COR via email 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 complete the training and state the required Privacy training has been completed for all Contractor and subcontractor employees.

(c) The Contractor shall insert the substance of 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. 2017–00752 Filed 1–18–17; 8:45 am]

BILLING CODE 9110–9B–P

DEPARTMENT OF HOMELAND SECURITY

48 CFR Parts 3001, 3002, 3004, and 3052

[Docket No. DHS–2017–0006]

RIN 1601–AA76

Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information (HSAR Case 2015–001)

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 modify a subpart, remove an existing clause and reserve the clause number, update an existing clause, and add a new contract clause to address requirements for the safeguarding of Controlled Unclassified Information (CUI).

DATES: Comments on the proposed rule should be submitted in writing to one of the addresses shown below on or before March 20, 2017, to be considered in the formation of the final rule.

ADDRESSES: Submit comments identified by HSAR Case 2015–001, Safeguarding of Controlled Unclassified Information, using any of the following methods:

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

Submit comments via the Federal eRulemaking portal by entering ''HSAR Case 2015–001'' under the heading ''Enter Keyword or ID'' and selecting ''Search.'' Select the link ''Submit a Comment'' that corresponds with ''HSAR Case 2015–001.'' Follow the instructions provided at the ''Submit a Comment'' screen. Please include your name, company name (if any), and ''HSAR Case 2015–001'' 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 2015–001 in the ''Subject'' line.

SUPPLEMENTARY INFORMATION:

I. Background

The purpose of this proposed rule is to implement adequate security and privacy measures to safeguard Controlled Unclassified Information (CUI) and facilitate improved incident reporting to DHS. This proposed rule does not apply to classified information. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information. Recent high-profile breaches of Federal information further demonstrate the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts. This proposed rule strengthens and expands existing HSAR language to ensure adequate security for CUI that is accessed by contractors; collected or maintained by contractors on behalf of an agency; and/or for Federal information systems that collect, process, store or transmit such information. The proposed rule identifies CUI handling requirements as well as incident reporting requirements, including timelines and required data elements. The proposed rule also includes inspection provisions and post-incident activities and requires certification of sanitization of Government and Government-Activity related files and information. Additionally, the proposed rule requires that contractors have in place procedures and the capability to notify and provide credit monitoring services to any individual whose Personally Identifiable Information (PII) or Sensitive PII (SPII) was under the control of the contractor or resided in the information system at the time of the incident.

This rule addresses the safeguarding requirements specified in the Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 3551, *et seq.*), Office of Management and Budget (OMB) Circular A–130, *Managing Information as a Strategic Resource,*[1] relevant National Institutes of Standards and Technology (NIST) guidance, Executive Order 13556, *Controlled Unclassified Information* [2] and its implementing regulation at 32 CFR part 2002,[3] and the following OMB Memoranda: M–07–16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information;* M–14–03, *Enhancing the Security of Federal Information and Information Systems;* and Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management as identified in various OMB Memoranda.[4] Ongoing efforts by OMB and DHS with regard to implementation of FISMA, such as the issuance of Binding Operational Directives, and DHS implementation of the CUI program, may require future HSAR revisions in this area. DHS intends to harmonize the HSAR to be consistent with the requirements of these ongoing efforts.

II. Discussion and Analysis

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

[1] OMB Circular A–130 *Managing Information as a Strategic Resource* is accessible at *https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.*

[2] Executive Order 13556 *Controlled Unclassified Information* is accessible at *https://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf.*

[3] 32 CFR part 2002 is accessible at *https://www.gpo.gov/fdsys/pkg/FR-2016-09-14/pdf/2016-21665.pdf.*

[4] These memoranda include M–03–19, M–04–25, M–05–15, M–06–20, M–07–19, M–08–212, M–09–29, M–10–15, M–11–33, M–12–20, M–14–04, M–15–01, M–16–03, and M–16–04. These memoranda can be accessed at: *https://www.whitehouse.gov/omb/memoranda_default.*