U.S. Department of Homeland Security
Safeguarding of Controlled Unclassified Information

Small Entity Compliance Guide

Introduction and Purpose

The U.S. Department of Homeland Security (DHS) has prepared this document as the small entity compliance guide required by section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996. The guide summarizes and explains rules that DHS adopted, but it is not a substitute for any rule. Only the final rule can provide complete and definitive information regarding its requirements.

Overview

On June 21, 2023, DHS issued a final rule at *88 FR 40560* to amend the Homeland Security Acquisition Regulation (HSAR) to identify requirements for controlled unclassified information (CUI). The rule implements security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS. These measures are necessary because of the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information. Persistent and pervasive high-profile breaches of Federal information continue to demonstrate the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts. This final rule strengthens and expands existing HSAR language to ensure adequate security when: (1) contractor and/or subcontractor employees will have access to CUI; (2) CUI will be collected or maintained on behalf of the agency; or (3) Federal information systems, which include contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. Specifically, the final rule:

- Identifies CUI handling requirements and security processes and procedures applicable to Federal information systems, which include contractor information systems operated on behalf of the agency;
- Identifies incident reporting requirements, including timelines and required data elements, inspection provisions, and post-incident activities;
- Requires certification of sanitization of government and government-activity-related files and information; and
- Requires contractors to 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.

The effective date of the final rule is July 21, 2023. This guidance restates some of the information in the final rule, particularly the information related to small entities. However, this guidance does not replace the final regulations; instead, it is a reference for small entities seeking

information concerning the potential impact of the regulations on them. As it relates to this rule specifically, DHS prepared a full Regulatory Impact Assessment (RIA) and Small Entity Analysis (SEA), and each is included in the final rule.

Summary of the Final Rule Provisions

The final rule adopts, with appropriate changes, the regulatory text in the Notice of Proposed Rulemaking (NPRM) published in the Federal Register on January 19, 2017. See Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001); Proposed rule, 82 FR 6429. DHS made several changes in the final rule based on comments received on the proposed rule or as required by the effects of those changes. The final rule makes the following major revisions as compared to the NPRM:

1. HSAR 3052.204–71, *Contractor Employee Access,* is revised as follows:

    - Revised paragraph (a) to remove the definition of "sensitive information" and replace it with the definition of "CUI";
    - Revised paragraph (b) to remove the definition of "information technology resources" and replace it with the definition of "information resources";
    - Replaced all references to "sensitive information" with "CUI" and all references to "information technology resources" with "information resources";
    - Revised paragraph (e) to clarify that both initial and refresher training concerning the protection and disclosure of CUI is required;
    - Revised paragraph (g) of Alternate I to make clear that additional training on certain CUI categories may be required if identified in the contract; and
    - Replaced the reference to "statement of work" in paragraph (h) of Alternate I with "contract."

2. Restructured clause 3052.204–72, *Safeguarding of Controlled Unclassified Information,* as follows:

    - Made the requirements of paragraph (c), *Authority to Operate,* into Alternate I to the basic clause; and
    - Made the requirements of paragraphs (f), *PII and SPII Notification Requirements,* and (g), *Credit Monitoring Requirements,* into a separate clause at 3052.204–73, *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.* This includes clarifying updates to the *PII and SPII Notification Requirements* section.

3. Revised requirements of restructured clause 3052.204–72, *Safeguarding of Controlled Unclassified Information,* as follows:

    - Made clear that both contractors and subcontractors are responsible for reporting known or suspected incidents to the Department;
    - Made clear that subcontractors are required to notify the prime contractor that they have reported a known or suspected incident to the Department;
    - Increased the amount of time a contractor must retain monitoring/packet capture data from 90 days to 180 days; and

- Revised the requirements for when prime contractors must include clause 3052.204–72, *Safeguarding of Controlled Unclassified Information,* in subcontracts.

Entities Subject to the Rule

a. Definition of *Small Entity*

The Regulatory Flexibility Act defines a "small entity" as a (1) small not-for-profit organization; (2) small governmental jurisdiction; or (3) small business. The Department used the entity size standards defined by the U.S. Small Business Administration (SBA), in effect as of August 19, 2019, to classify businesses as small. SBA establishes separate standards for individual 6-digit North American Industry Classification System (NAICS) codes, and standard cutoffs typically are based on either the average number of employees or the average annual receipts. For example, small businesses generally are defined as having fewer than 500, 1,000, or 1,250 employees in manufacturing industries and less than $7.5 million in average annual receipts for nonmanufacturing industries. However, some exceptions do exist, the most notable being that depository institutions (including credit unions, commercial banks, and noncommercial banks) are classified by total assets (small defined as less than $550 million in assets). Small governmental jurisdictions are another noteworthy exception. They are defined as the governments of cities, counties, towns, townships, villages, school districts, or special districts with populations of less than 50,000 people.

b. Number of Small Entities

This final rule applies to DHS contractors that require access to CUI, collect or maintain CUI on behalf of the Government, or operate Federal information systems, which include contractor information systems operated on behalf of the agency that collect, process, store, or transmit CUI. DHS estimated the number of small entities subject to the final rule using Fiscal Year (FY) 2020 Federal Procurement Data System (FPDS) data on unique vendors awarded contracts under the most likely applicable Product and Service Codes (PSCs) in FY 2020. FPDS data indicated that 2,218 unique vendors, were awarded contracts under the most likely applicable PSCs in FY 2020, including small businesses. Of those 2,218 vendors, the Department was able to obtain data matches of revenue or employees for 366 vendors in FY 2020. Of the 366 vendors with employee or revenue matches, the Department identified 265 unique vendors as small. Notwithstanding this estimate, the clauses at HSAR 3052.204-71 *Contractor Employee Access*, 3052.204-72 *Safeguarding of Controlled Unclassified Information*, and 3052.204-73 *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents* apply when they are included in a solicitation and its resultant contract. Small entities must thoroughly review DHS solicitations and contracts to determine if the clauses apply.

c. Projected Impacts to Affected Small Entities

The clauses at HSAR 3052.204-71 *Contractor Employee Access*, 3052.204-72 *Safeguarding of Controlled Unclassified Information*, and 3052.204-73 *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents* have multiple impacts as detailed below. As such, it is imperative that small entities thoroughly review DHS solicitations and contracts to determine if the clauses apply.

- HSAR 3052.204-72 *Safeguarding of Controlled Unclassified Information* requires contractors and/or subcontractors to:

    - Review and understand DHS policies applicable to the handling of CUI;
    - Report all known or suspected incidents within specified timeframes to DHS, including specific data elements;
    - Understand and comply with specific incident response activities DHS may perform when notified of an incident;
    - 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; and
    - When applicable, understand and implement information system security requirements, identified through the DHS developed Security Requirements Traceability Matrix, before a contractor information system operated on behalf of the agency can be trusted with CUI.

- HSAR 3052.204-73 *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents* requires contractors and/or subcontractors to provide, when applicable and directed by the Contracting Officer, notification, call center and credit monitoring services, in the event of an incident impacting personally identifiable information.

- **Note:** There are no new impacts to small entities from the changes HSAR 3052.204-71 *Contractor Employee Access*.

Resources to Support Compliance Among Small Entities

The Contracting Officer and Contracting Officer's Representative are great resources to ensure proper understanding of contract terms and conditions. Other resources include:

- DHS Security Requirements for Contractors at: https://www.dhs.gov/dhs-security-and-training-requirements-contractors

- Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules at: https://csrc.nist.gov/pubs/fips/140-2/upd2/final

- FIPS 140-3 Security Requirements for Cryptographic Modules at: https://csrc.nist.gov/pubs/fips/140-3/final

- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems at: https://csrc.nist.gov/pubs/fips/199/final

- NIST Special Publication (SP) 800-53 Security and Privacy Controls for Information Systems and Organizations at: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

- NIST SSP 800-88 Guidelines for Media Sanitization at: SP 800-88 Rev. 1, Guidelines for Media Sanitization | CSRC (nist.gov)

- Final Rule at: https://www.federalregister.gov/documents/2023/06/21/2023-11270/homeland-security-acquisition-regulation-safeguarding-of-controlled-unclassified-information