PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 9 **NUMBER 11** **November 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
LexisNexis® Support Center . . . . . https://supportcenter.lexisnexis.com/app/home/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3385

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)
ISSN: 2688-7290

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt).
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

Pratt's Government Contracting Law Report is published 12 times a year by Matthew Bender & Company, Inc. For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

DHS Updates CUI Safeguarding and Incident Reporting Requirements for Contractors

By Megan L. Brown, Tracye Winfrey Howard and Teresita Regelbrugge*

The authors of this article discuss revisions to the Homeland Security Acquisition Regulation (HSAR) to implement security and privacy measures for contractors to safeguard controlled unclassified information and to revise contractor incident reporting requirements. The authors describe three HSAR clauses that contracting officers have begun incorporating into new Department of Homeland Security solicitations and contracts and key takeaways.

The U.S. Department of Homeland Security (DHS) issued a final rule[1] that revises the Homeland Security Acquisition Regulation (HSAR) to implement security and privacy measures for contractors to safeguard controlled unclassified information (CUI) and to revise contractor incident reporting requirements. The final rule follows a proposed rule DHS issued in 2017. The final rule is intended to ensure that federal CUI is adequately protected in situations when: CUI is accessed by contractor or subcontractor employees; CUI is collected or maintained on behalf of the agency; or federal information systems, including contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. To achieve this protection, the rule describes three HSAR clauses that contracting officers will immediately begin incorporating into new DHS solicitations and contracts.

With this rule, DHS is layering on additional obligations and expanding the application of current requirements that are different and in addition to the existing obligations facing contractors for other agencies. Companies that contract with DHS and possess CUI should heed these new obligations and adjust incident response plans accordingly.

BACKGROUND

DHS issued the final rule to address what it describes as "the urgent need to protect CUI and respond appropriately when DHS contractors experience incidents with DHS information." CUI is defined as "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,

---

* Megan L. Brown, Tracye Winfrey Howard and Teresita Regelbrugge are attorneys at Wiley Rein LLP. They may be reached at mbrown@wiley.law, twhoward@wiley.law and rregelbrugge@wiley.law, respectively.

[1] https://www.federalregister.gov/documents/2023/06/21/2023-11270/homeland-security-acquisition-regulation-safeguarding-of-controlled-unclassified-information.

regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls." This is the same definition that appears in the National Archives and Records Administration's (NARA) regulations at 32 C.F.R. § 2002.4(h) and similar to the definition of CUI in the U.S. Department of Defense (DOD) FAR Supplement (DFARS) clause at 252.204-7012.

DHS notes that pervasive, high-profile breaches of federal information demonstrate the need to ensure that information security protections are clearly, effectively, and consistently addressed in DHS contracts. DHS has determined that the measures included in the final rule will enable DHS to identify, remediate, mitigate, and resolve incidents that actually or imminently jeopardize the integrity, confidentiality, or availability of information or an information system, or constitute a violation or of violation of law or security policies.

SUMMARY OF THE RULE

Among other requirements, the rule updates incident reporting and response requirements, measures for handling CUI, and notification requirements for incidents involving Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII).

Incident Reporting and Response Requirements

Safeguarding of Controlled Unclassified Information, HSAR 3052.204-72, requires contractors to report any cybersecurity incident that could affect CUI within eight hours of discovery. If the incident involved PII, the rule requires contractors to report the incident within one hour of discovery. Subcontractors are also required to notify the prime contractor that they have reported a known or suspected incident to DHS. Lower-tier subcontractors are likewise required to notify the next higher-tier subcontractor until the prime contractor is reached.

The clause also identifies several requirements that contractors must follow after discovery of an incident. For example, the clause requires that contractors provide full access and cooperation for activities required by the government to ensure an effective incident response, including providing all requested images, log files, and event information. Contractors must also immediately preserve and protect images of all known affected information systems and monitoring/packet capture data.

Measures for Handling CUI

Contractor Employee Access, HSAR 3052.204-71, requires that contractors provide employees authorized to handle CUI with initial and refresher training concerning the protection and disclosure of CUI at prescribed intervals (initial

training within 60 days of contract award, with refresher training every 2 years thereafter). The Alternate I version of the clause, which will be used when the contractor has access to government information resources, imposes additional requirements, such as additional security briefing, training for specific CUI categories, and completion of a nondisclosure agreement. The additional briefing and training will be arranged by the Contracting Officer's Representative (COR). The Alternate I clause also prohibits non-U.S. citizens from assisting in the development, operation, management, or maintenance of DHS IT systems under the contract unless a waiver has been granted. The Alternate I clause also requires that contractors identify the names and citizenship of any non-U.S. citizens included in their proposals.

The revised Safeguarding clause (-72) also specifies CUI handling requirements and security processes and procedures applicable to federal information systems. Notably, the clause requires that contractors and subcontractors provide adequate security to protect CUI from unauthorized access and disclosure, meaning that the contractor must provide security protections commensurate with the risk resulting from the unauthorized access or use of information, including information hosted on behalf of an agency. At the conclusion of a contract, the clause also requires contractors to return or destroy all CUI, and to certify the sanitization of all government files and information.

The Safeguarding clause Alternate II—which applies when the contractor will use government information systems or contractor systems operated on behalf of the government to collect, process, store, or transmit CUI—includes additional requirements, which include obtaining an Authority to Operate (ATO) before using a federal information system; obtaining an independent assessment from a third party to validate the security and privacy controls in place for the information system(s); and complying with continuous monitoring requirements.

Notification Requirements for Incidents Involving PII and SPII

The final rule also adds HSAR 3052.204-73, Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents. This clause requires contractors to create procedures for and maintain the capability to notify and provide credit monitoring services to any individual whose PII or SPII was under the control of the contractor or resided in the information system at the time of an incident. 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. SPII is a subset of PII that, if lost or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked to the individual. The rule cautions that information can become PII when additional information "becomes available, in any medium or from any source, that would make it possible to identify an individual." The rule provides several examples of information that is PII (e.g., Social Security numbers), and SPII (e.g., an individual's name along with a date of birth, citizenship status, or ethnic or religious affiliation).

KEY TAKEAWAYS

Contractors should generally take note of DHS's updated requirements and consider how they will interact with existing and upcoming requirements for safeguarding CUI and reporting security incidents.

Another Set of Compliance Standards for Safeguarding CUI

Many contractors currently must comply with existing standards for handling CUI and safeguarding information systems, such as FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, and DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Practically, the DHS rule requires certain measures be taken that exceed existing requirements in other regulations. For example, the DHS rule requires that contractors report incidents within eight hours of discovery (one hour for incidents involving PII), while the DOD safeguarding clause requires that contractors report incidents within 72 hours of discovery.

Interaction with NIST Special Publication (SP) 800-53

DHS drafted the rule to impose requirements on federal information systems, to include contractor information systems being operated on the government's behalf. DHS recognized that its requirements are separate from, and in addition to, other requirements for federal information systems, such as the minimum set of requirements selected from NIST SP 800-53, Rev. 5, to protect federal information and information systems in accordance with the Office of Management and Budget (OMB) Circular A-130 and provisions of the Federal Information Security Modernization Act (FISMA).[2]

Interaction with NIST SP 800-171

In contrast, DHS stated that the rule is intentionally silent regarding requirements for protecting the confidentiality of CUI for nonfederal information systems published in NIST SP 800-171, Protecting CUI in Nonfederal Systems and Organizations. DHS specified that the rule is intended to apply to

[2] 44 U.S.C. § 3551, et seq.

federal information systems—to include contractor information systems operated on behalf of the agency—and determined that the requirements in NIST SP 800-171 are inapposite. DHS's conclusion is not fully explained, and there remains some uncertainty about how DHS will interpret when a contractor's work under a contract results in the contractor's information system being "operated on behalf of the agency."