THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

THOMSON REUTERS®

Vol. 65, No. 29 August 9, 2023

Focus

¶ 211

FEATURE COMMENT: Setting The Table: The Department Of Homeland Security's Rules On Safeguarding Controlled Unclassified Information

Every home has a silverware drawer. Perhaps not recognized for its importance, but critical for daily nourishment. Home to the knives, the forks, and the spoons, the silverware drawer holds unique tools meant for the same purpose—eating. Although the silverware share the same aim of helping one enjoy a meal, each possesses a distinctive function that defies grouping beyond the term "silverware."

Like the U.S.'s own silverware drawer, the U.S. Department of Homeland Security (DHS) is an amalgamation of entities pulled together for the same purpose: "to secure the nation from the many threats we face." To accomplish this, the components of DHS have diverse functions and capabilities that make any singular "solution" beyond challenging. For example, the needs of the Transportation Security Administration (TSA) to protect the nation's transportation systems to ensure freedom of movement for people and commerce will vary significantly from those of the Federal Emergency Management Agency (FEMA) to help people through disasters. Accordingly, any policy crafted to address the needs of the entire DHS must reflect, address, and qualify the broad scope of DHS's mandate. As reflected in DHS's cybersecurity acquisition requirements, that is no easy or clean task.

After six long years, on June 21, 2023, DHS finally took formative steps to safeguard Controlled Unclassified Information (CUI) by issuing a Final Rule titled "Safeguarding of Controlled Unclassified Information" (Final Rule). This Final Rule, published in the Federal Register (88 Fed. Reg. 40560), amends the Homeland Security Acquisition Regulation (HSAR) and introduces three new HSAR contract clauses at 48 CFR §§ 3052.204-71, 3052.204-72, and 3052.204-73 for use by DHS contracting officers in securing CUI within DHS contracts and handling incidents involving DHS information. As a result, effective July 21, 2023, the newly added HSAR clauses address security and privacy measures aimed at fortifying the protection of CUI and obligating contractors to enhance incident reporting to DHS in ways unique to DHS's varied mission.

The DHS Rule stands out among Government cybersecurity directives as distinct from Defense Federal Acquisition Regulation Supplement clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," the long-pending Federal Acquisition Regulatory Council's proposed CUI rule, and even the existing CUI security requirements outlined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." This Final Rule sets its own course by, in broad strokes, strengthening and expanding "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." 88 Fed. Reg. 40561. This wide

application of protections to a broad range of data, missions, and contractors is more confusing than clarifying and is likely to cause much consternation among Government purchasers and contractors alike. So, like with any good silverware drawer, it's best to get organized.

Fork: The Many Tines of DHS—DHS was established in response to the Sept. 11, 2001 attack, the rise in terrorist attacks on the U.S., and an identified need for a coordinated and centralized approach to national security against several differing threats. As a result, on Nov. 25, 2002, the Homeland Security Act of 2002 (the "Act") was signed into law by President George W. Bush. This act formed DHS by bringing together 22 federal agencies and departments each with specific national security and emergency management responsibilities. Most notably, these agencies included:

1. U.S. Citizenship and Immigration Services (USCIS): Oversees immigration services and enforcement, including border control and the issuance of visas.
2. U.S. Coast Guard: In charge of maritime security, search and rescue operations, and protecting U.S. ports and waterways.
3. FEMA: Handles disaster preparedness, response, recovery, and mitigation efforts for natural and man-made disasters.
4. TSA: Responsible for security measures for all transportation systems, primarily focusing on aviation security.
5. Secret Service: Originally under the Department of the Treasury, the Secret Service protects high-ranking officials, including the president, and investigates financial and electronic crimes.
6. Cybersecurity and Infrastructure Security Agency: Focuses on protecting the nation's critical infrastructure and cyberspace from cyber threats.
7. Federal Protective Service: Ensures the security of federal buildings and properties.
8. U.S. Customs and Border Protection: Manages border security and customs enforcement, including inspection and entry processes at ports of entry.
9. U.S. Immigration and Customs Enforcement: Focuses on immigration enforcement and investigates customs violations and certain transnational crimes.

Few agencies have as broad or wide-reaching mission as DHS: safeguard the American people, territory, and interests from a wide range of threats while ensuring the flow of lawful trade and travel. To meet that mission, DHS is responsible for evolving while ensuring that data is adequately protected from national security threats.

Spoon: The Scoop Behind the Final Rule—The effort of DHS to protect CUI started six years ago when, in January 2017, it issued a notice of proposed rulemaking aimed at implementing robust security and privacy measures to safeguard CUI while enhancing incident reporting capabilities to DHS. 82 Fed. Reg. 6429 (Jan. 19, 2017).

Despite the feedback received, the Final Rule remains essentially unchanged from the initial proposal, incorporating only minor adjustments, resulting in:

1. *A Broader Definition of CUI (HSAR 3052.204-71(a) and 3052.204-72(a))*: Across the clauses created by the Rule, DHS takes a broad approach to defining CUI. The definition encompasses all information created or possessed by the Government or an entity for or on behalf of the Government, carrying with it necessary safeguarding and dissemination controls. The Final Rule meticulously outlines eleven categories and various subcategories of CUI, even surpassing the confines of the National Archives and Records Administration's (NARA's) prescribed boundaries to include newly defined types, such as Information Systems Vulnerability Information, International Agreement Information, Homeland Security Enforcement Information, and others.
2. *Contractor Employee Access Restrictions (HSAR 3052.204-71)*: Perhaps one of the most significant distinctions between the DHS Rule and other federal analogs is DHS's imposition of rigorous security screening and training obligations upon contractor or subcontractor employees who are granted access to CUI or Government facilities.
3. *Security and Incident Reporting Requirements (HSAR 3052.204-72)*: The Rule lays down stringent security prerequisites for contractor employees accessing CUI, aiming higher for secure data handling. It expedites the timeline for reporting security incidents,

particularly in cases involving Personally Identifiable Information (PII) or Sensitive PII (SPII), mandating reporting within ***one hour***. Notably, due to the flowdown requirement of this Rule, subcontractors facing incidents now bear the responsibility of reporting to both DHS and the prime contractor, ensuring a comprehensive and coordinated approach to incident management. Yet a lack of certainty on who should be notified further complicates the notification provision.

4. *Notification and Credit Monitoring for PII Incidents (HSAR 3052.204-73)*: Contractors or subcontractors entrusted with PII or SPII are required to provide prompt notification to affected individuals within five business days following any security incident. COs may exercise discretion to require credit monitoring and additional services, further safeguarding those affected.

The upside is that the Final Rule appears to be generally limited. The Final Rule applies to federal information systems that collect, process, store, or transmit CUI. The Final Rule clarifies that this applicability extends to "contractor information systems operated on behalf" of DHS and that such systems, under the eyes of the Final Rule, amount to a federal information system. What is imprecise is whether and to what extent the Final Rule applies to contractor information systems of contractors who do ***not*** directly operate information systems for or on behalf of DHS. This clarified scope would address many DHS contractors and may help limit the application of the Final Rule to only a subset of DHS contractors. Further emphasizing that limitation, HSAR 3004.470-4(a) expressly states that, in terms of the application of the HSAR 3052.204–71 clause, "[n]either the basic clause nor its alternates shall be used unless contractor and/or subcontractor employees will require recurring access to government facilities or access to CUI." Moreover, in a nod to the plight of universities that receive federal grants or contracts, the Final Rule also notes that "[n]either the [HSAR 3052.204–71] basic clause nor its alternates should ordinarily be used in contracts with educational institutions."

It is clear that in crafting its own cybersecurity acquisitions rule in a manner distinct from NIST SP 800-171, DHS intended to tailor its directives to their specific protection needs. A comprehensive updating of policies, particularly in training, handling, transmission, marking requirements, and incident reporting, is promised. But, until that update is complete, the Rule directs contractors to review, use, and rely on dated cybersecurity policies and forms (found at www.dhs.gov/dhs-security-and-training-requirements-contractors) that may deviate from NIST SP 800-171 requirements and even the tenets of the Rule itself.

Knife: A Sharper Look at the New Clauses—*HSAR 3052.204-71, Contractor Employee Access*: This clause is included in solicitations and contracts when contractor and/or subcontractor employees seek recurring access to Government facilities or access to CUI. An integral aspect of the clause is employee training on safeguarding and disclosing CUI. According to this requirement, contractors are responsible for ensuring that initial training is promptly completed within 60 days of contract award, while subsequent "refresher training" sessions are mandated biennially. Such recurrent training aims to reinforce employees' comprehension of their roles in handling CUI. This clause effectively enforces the imperative that contractor employees fulfill essential security-related requirements, including background investigations, while circumscribing their access to CUI solely to provide direct advisory or assistance support to the Government's activities.

HSAR 3052.204-71, Contractor Employee Access (Alternate I): In instances where acquisitions require contractor access to Government information resources, defined as "information and related resources, such as personnel, equipment, funds, and information technology," COs must include the Alternate I clause and its additional requirements on top of those in the primary clause (adding paragraphs (g)-(k)). This clause entails mandatory security briefings for contractor employees before they gain access to information resources, along with the possibility of additional training requirements for specified categories of CUI. Moreover, with some notable exceptions (like for educational institutions), the Alternate I clause explicitly prohibits non-U.S. citizens from accessing or contributing to the "development, operation, management, or maintenance of Department IT systems under the contract" without the requisite waiver.

HSAR 3052.204-71, Contractor Employee Access (Alternate II): Adds two paragraphs (paragraphs (g)–(h)) to address when contract employees might have access to "sensitive information or Government facilities" but not IT resources. The addition allows access to U.S. citizens and lawful permanent residents.

HSAR 3052.204–72, Safeguarding of Controlled Unclassified Information: This clause is intended to protect CUI from unauthorized use, access, or disclosure. It is to be applied in two distinct scenarios. First, the Safeguarding clause is obligatory in solicitations and contracts where contractor and/or subcontractor employees are granted access to CUI or where CUI is collected or maintained on behalf of the agency. Or second, the basic clause and its Alternate I additions must be incorporated when federal information systems, including contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI. The clause also contains instructions reflecting a stringent prohibition barring contractors from retaining SPII within their invoicing, billing, or other recordkeeping systems and identifying that CUI transmission via email is only permissible through encrypted means or within secure communications systems.

Finally, the clause identifies the incident reporting requirements, including timelines, obligatory data elements, inspection provisions, and post-incident engagements. A crucial provision mandates that all "known or suspected incidents" be promptly communicated to DHS's Component Security Operations Center within a strict timeframe of eight hours from their discovery. Furthermore, a heightened sense of urgency is enshrined in the clause, compelling contractors to report all incidents involving PII or SPII within a mere one hour of their discovery.

Like its Department of Defense corollary, the HSAR 3052.204-72 clause also insists that contractors employ "adequate security." But unlike the DOD clause, the "adequate security" required by the Final Rule is far more … fuzzy. Under DFARS 252.204-7012(a), "Adequate security" is defined as the "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."

At one point, in 3052.204-72(a), "adequate security" is defined as

> security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

But in the very next section of the clause, at 3052.204-72(b)(1), "adequate security" is redefined as "compliance with DHS policies and procedures in effect at the time of contract award" before whisking contractors off to review those "policies and procedures" at www.dhs.gov/dhs-security-and-training-requirements-contractors. This is neither helpful nor easy because, as conveyed above, not only are many of these policies and procedures circa 2015 extremely outdated, but it also leaves too much room for error by contractors who are left to their own devices to figure out what may apply.

Perhaps most noteworthy about the clause is its reluctance to commit. HSAR 3052.204-72 addresses the obligations of contractor employees who access CUI; however, it hesitates in specifying security safeguards on nonfederal information systems that process, store, or transmit CUI. Instead, it acknowledges ongoing collaborative efforts between NARA, DHS, and the FAR Councils to develop a FAR CUI rule that addresses the security requirements for nonfederal information systems.

HSAR 3052.204-72, Safeguarding of Controlled Unclassified Information (Alternate I): This clause is used when federal information systems, encompassing contractor information systems operated on behalf of the agency, undertake the task of collecting, processing, storing, or transmitting CUI. This Alternate I requires contractors to obtain a DHS Authority to Operate (ATO), valid for three years (unless otherwise specified and requires renewal at the end of this term), before engaging in the collection, processing, storage, or transmission of CUI within a federal information system. It is noteworthy that the ATO process, in essence, bears resemblances to the authorization protocols employed in the FedRAMP framework, which, in

turn, is dedicated to cloud services operated for or on behalf of federal agencies.

HSAR 3052.204-73, Notification and Credit Monitoring Requirements for Personally Identifiable Information (PII) Incidents: This clause is relevant to solicitations and contracts involving contractor and/or subcontractor employees with access to PII. This clause imposes upon contractors the obligation to establish robust procedures and capabilities for notifying and providing credit monitoring services to individuals whose PII or SPII was within the contractor's control or housed within their information system during a cyber incident.

It is essential to recognize that the decision to furnish notification and credit monitoring services is singular to each incident. The Rule thus highlights that the CO will let contractors know their specific requirements based on the nature and gravity of the incident with the ultimate determination on whether to provide notification and credit monitoring services depending on the severity of the cyber incident.

Of final note, it is worth recognizing that, in relation to these clauses, an "incident" is defined as:

> an occurrence that—(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

The breadth of the definition of "incident" requires particular attention when coordinating the need to apply this clause with existing policies. That an incident can occur when/if "security procedures" are violated may make for a "hair trigger" when making the requisite notifications.

Organizing the Drawer: Challenges for Contractors—That it took DHS seven years to finalize its "standard" CUI handling requirements is no surprise. The various needs of agencies within DHS make such an undertaking nearly impossible. It helps that the Final Rule is limited in scope to a subset of contractors; this will aid the majority of contractors with no intent or inclination to obtain access to CUI or operate information systems on behalf of the agency. But for those that the Final Rule will impact, and there will be many, a plethora of questions must be asked. Failing to understand the implications of the Final Rule's clauses—and whether those clauses should even be there in the first instance—is a new but necessary evil for DHS contractors moving forward. DHS has a lot of work left to do, especially regarding updating the aging IT policies and procedures the Final Rule directs contractors to review and follow. In the meantime, contractors must be comfortable asking questions to vet just what it is—exactly—they must do to meet DHS's specific contractual requirements. Failure to do so would be the equivalent of eating soup with a steak knife—sloppy and bloody.

♦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Alexander Major. *Mr. Major is a partner and co-leader of the Government Contracts & Global Trade Practice Group at McCarter & English, LLP. The author would like to thank Deborah Alexander for assistance in drafting this article. Ms. Alexander is a May 2022 graduate from Georgetown University Walsh School of Foreign Service with a B.S. in International Politics and a Minor in Spanish.

