Westlaw Today
powered by Reuters

FAR Council proposes cybersecurity rule for reporting, info sharing

By Bob Huffman, Esq., Susan B. Cassidy, Esq., Ryan Burnette, Esq., and Darby Rourick, Esq., Covington & Burling LLP*

NOVEMBER 6, 2023

On October 3, 2023, the Federal Acquisition Regulation (FAR) Council released two new proposed cybersecurity rules. The first of the two, titled "Cyber Threat and Incident Reporting and Information Sharing," adds new requirements to the cybersecurity incident reporting obligations of federal contractors.

The second rule, which we will cover in a separate blog post, is titled "Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems" and covers cybersecurity contractual requirements for unclassified Federal information systems.

The rule applies to contracts below the simplified acquisition threshold, and to commercial products, including commercial off the shelf items, and commercial services.

Both rules arise from Executive Order 14028,[1] "Improving the Nation's Cybersecurity," issued by President Biden on May 12, 2021 (the "Cyber EO"). We have covered developments under this Executive Order as part of a series of monthly posts.

The first blog summarized the Cyber EO's key provisions and timelines, and subsequent blogs described the actions taken by various government agencies to implement the Cyber EO from June 2021[2] through September 2023.[3] This blog describes key requirements imposed by the proposed "Cyber Threat and Incident Reporting and Information Sharing" rule.

New incident reporting and information sharing requirements

As directed by the Cyber EO, the rule proposed by FAR case 2021-017 implements recommendations made by OMB and CISA concerning the cybersecurity incident reporting obligations of federal contractors. The rule amends provisions of several existing FAR Subparts and introduces new FAR clauses for contracting officers to incorporate into future solicitations and contract actions. The rule also adds new FAR definitions and expands others.

For example, the proposed rule broadly expands the definition of "Information and Communications Technology (ICT)" by specifying that operational technology, such as industrial control systems, building management systems and physical access control mechanisms, are covered by the rule.

Under the new rule, contracting officers will include the primary incident reporting clause, FAR 52.239-ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology, in all new solicitations and contracts. The rule applies to contracts below the simplified acquisition threshold, and to commercial products, including commercial off the shelf (COTS) items, and commercial services.

The rule imposes a number of requirements, the most notable of which concern: (1) Security Incident Reporting; (2) Government Access to Contractor Information and Information Systems; (3) Security Incident Reporting Representations; and (4) Software Bills of Materials (SBOMs).

Security incident reporting obligations

The proposed rule imposes new and aggressive reporting obligations on contractors that discover indicators that a "security incident" may have occurred, a term broadly defined to include the "actual or potential occurrence [of] any event or series of events … which pose(s) actual or imminent jeopardy to the integrity, confidentiality, or availability of information or an information system" OR which constitutes a "violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

These incident reporting obligations are applicable to all security incidents involving a product or service provided to the Government that includes Information and Communication Technology (ICT) or the information system used in developing or providing the product or service to the Government.

The rule requires contractors to "'immediately and thoroughly investigate all indicators that a security incident may have occurred

and submit information using the CISA incident reporting portal ... within eight hours of discovery ... [and to] update the submission every 72 hours thereafter until the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities."

This reporting timeline is much shorter than the 72-hour reporting timeline imposed by the Department of Defense in DFARS 252.204-7012(c)(1)(ii). Further, the proposed rule does not relieve applicable contractors of their DoD-reporting obligations under DFARS, but instead notes that "[t]he products and systems that contractors offer to the Federal Government may be subject to ... other incident reporting requirements."

The proposed rule imposes new and aggressive reporting obligations on contractors that discover indicators that a "security incident" may have occurred.

In addition to the CISA reporting requirement, contractors must notify: (1) the applicable contracting officer for the contract; and (2) any contracting officers or ordering officers of any agency which placed an affected order under a contract for which an incident report has been submitted to CISA.

The rule does not specify a timeline for reporting the potential incident to the affected contracting officers, but under the Rule, CISA is required to share the information reported "with any contracting agency potentially affected by the incident or by a vulnerability revealed by the incident," as well as law enforcement. From a practical standpoint, there may be an advantage to contractors notifying their customers before government regulators reach out to them based on a report to CISA.

Granting access to contractor information and information systems

The proposed rule grants CISA, the FBI, and the contracting agency "full access" to applicable contractor information, information systems, and personnel, in response to a security incident reported by the contractor or a security incident identified by the Government. Under the proposed FAR clause, "full access" means: (1) physical and electronic access to networks, systems, accounts and other infrastructure; and (2) contractor "provision of all requested Government data or Government-related data," including images, log files, event information, and contractor employee statements.

The proposed rule does not meaningfully address the implications of granting the government "full access" to contractor information and systems. For example, the proposed rule does not mention safeguards for third-party privacy rights or civil liberties, except to invite industry comment on these topics.

The proposed rule also fails to address how such access could impact trade secrets, other proprietary data of the contractor or the contractor's suppliers/subcontractors and teaming partners, or materials subject to legal privilege. In addition, the proposed rule provides no guidance for how easily or often a contractor obligation to grant "full access" might be triggered.

Under the proposed rule, CISA, the FBI, and the contracting agency are entitled to "full access" to contractor information and systems "upon request" and "in response to a [reported or identified] security incident." But the definition of "security incident" under the proposed clause is very broad. In certain ways, the language is broader than the Department of Defense's definition of an incident.

For example, even a *potential* violation of the contractor's *internal* acceptable-use policies is an act that could constitute a security incident and trigger the contractor's "full-access" obligations.

Security incident reporting representations

The proposed rule requires contractors to represent that they have "submitted in a current, accurate, and complete manner, all security incident reports required by current existing contracts between the Offeror and the Government," as part of each new contract bid.

The proposed rule grants CISA, the FBI, and the contracting agency "full access" to applicable contractor information, information systems, and personnel, in response to a security incident.

Under the new representation clause, contractors must also assert that they have required each first tier subcontractor to: (1) notify the prime within eight hours of discovery of a security incident; and (2) flow the same requirement down to lower-tier subcontractors.

Software bill of materials (SBOM)

The proposed rule requires "contractors to develop and maintain a software bill of materials (SBOM) for any software used in the performance of the contract." The proposed rule does not further explain what constitutes use in the performance of a contract. An SBOM is a formal record of the various components used in building software.

According to the rule, and E.O. 14028, the government envisions a central repository for SBOMs that can be queried by other applications and systems. The rule will require contractors to produce SBOMs in a "machine-readable, industry-standard format and ... comply with all of the minimum elements" established by the U.S. Department of Commerce, National Telecommunications and Information Administration.

The proposed rule requires contractors to provide the contracting officer a copy of or access to a current SBOM for "each piece of computer software" upon the initial use of that software in performance of the contract.

Further, under the proposed rule, if any software receives a significant update, new build, or major release, the contractor must update its contract SBOM and file the new version with the contracting officer. Finally, it is likely that these SBOMs will be among the files subject to the data preservation and protection requirements imposed by other sections of the proposed rule.

It is unclear how these requirements may be harmonized, if at all, with forthcoming self-attestation requirements outlined in the Office of Management and Budget (OMB) Memorandum M-22-18 (previously covered here[4]), which requires an SBOM only where an agency makes a determination that an SBOM is necessary and/or that software is sufficiently critical to warrant creation and submission of an SBOM.

Notes

[1] https://bit.ly/3QCViZI

[2] https://bit.ly/40nBNHF

[3] https://bit.ly/46062pb

[4] https://bit.ly/477Yy4y

About the authors




(L-R) **Bob Huffman**, a senior of counsel at **Covington & Burling LLP**, focuses on False Claims Act qui tam investigations and litigation, cybersecurity and supply chain security counseling and compliance, and intellectual property matters related to U.S. government contracts. He can be reached at rhuffman@cov.com. **Susan B. Cassidy**, a partner at the firm, previously served as in-house counsel for two defense contractors and now advises clients on compliance with supply chain and cybersecurity requirements under the Federal Acquisition Regulation and Defense Federal Acquisition Regulation. She can be reached at scassidy@cov.com. **Ryan Burnette**, a special counsel in the firm, advises clients on federal cybersecurity and supply chain security, defense and intelligence community issues, and government cost accounting. He can be reached at rburnette@cov.com. **Darby Rourick**, an associate in the firm, focuses on government contracting, federal cybersecurity and information technology supply chain issues. She can be reached at drourick@cov.com. The authors are based in Washington, D.C. They would like to thank firm partners Ashden Fein and Michael Wagner for their contributions to this article, which was originally published Oct. 10, 2023, on the firm's website. Republished with permission.

This article was published on Westlaw Today on November 6, 2023.