wiley

ALERT

Update: FAR Council Proposes Pair of Major Cybersecurity Rules for Government Contracts

October 11, 2023

WHAT: As we previously reported here, on October 3, 2023, the Federal Acquisition Regulatory Council (FAR Council) proposed a pair of major cybersecurity rules intended to implement key parts of President Biden's May 2021 Executive Order No. 14028 on Improving the Nation's Cybersecurity. The proposed rule in FAR Case No. 2021-0017 primarily addresses incident reporting and applies broadly to all contractors that use information and communications technology (ICT) systems in the performance of a government contract. The proposed rule in FAR Case No. 2021-0019 is intended to standardize security requirements for federal information systems (FIS) that contractors provide or maintain under a federal contract. This alert provides further analysis of these significant proposed rules.

WHEN: The FAR Council issued both proposed rules on October 3, 2023, with a request for comments within 60 days (by December 4, 2023).

WHAT DOES IT MEAN FOR INDUSTRY: As our prior alert summarized, the FAR Council's proposed rule on incident reporting (FAR Case No. 2021-0017) would have the broadest reach and would affect, according to the FAR Council, approximately 75% of contractors—those awarded contracts that "include some ICT." The proposed rule in FAR Case No. 2021-0019 is intended to standardize the requirements for FIS provided or maintained as part of a contractual requirement. Continue reading for a deeper dive into the key issues in these two proposed rules.

FAR Case No. 2021-0017, Cyber Threat and Incident Reporting

Authors

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance
Telecom, Media & Technology

The proposed rule introduces two additions to FAR Subpart 52.239:

- A new contract clause at FAR 52.239-zz entitled *Incident and Threat Reporting and Incident Response Requirements for Products and Services Containing Information and Communications Technology*; and
- A new representation at FAR 52.239-AA entitled *Security Incident Reporting Representation*.

Both additions will be mandatory for all contracts above the micro-purchase threshold. This includes contracts for commercial products and services, commercially available off-the-shelf (COTS) items, contracts below the simplified acquisition threshold, and contracts held by small businesses.

Preliminary Scope Questions

Although the proposed rule will require Contracting Officers (COs) to include the proposed contract clauses in virtually every contract, it is not obvious that each requirement in the proposed Incident and Threat Reporting clause applies to all contractors. The flowchart included with this alert provides a high-level reference for evaluating when each of the paragraphs could apply.

As currently written, several of the key requirements should apply only when a contractor is ***developing*** for or ***providing*** to the Government—*as part of the contract*—a product or service that includes ICT. This includes the requirement to investigate and report security incidents, data preservation requirements, and requirements to support any incident response activities. We stress "should" here because paragraph (b) of the Incident and Threat Reporting clause does not expressly limit itself to incidents affecting ***the*** product or service that the contractor is providing under the contract. Instead, it refers generally to "a product or service provided to the Government." And because many aspects of the data preservation and incident response are tied to security incidents, some could argue that these also apply more broadly.

Several other important requirements also have a potentially broader reach under different criteria. For example, the Software Bill of Materials (SBOM) provision requires contractors to maintain an SBOM "for each piece of computer software ***used*** in the performance of the contract." The Government has included similarly broad triggers in several recent policies and rules, but there is still room for significant disagreement on what constitutes use "in the performance of the contract."

Key Aspects of Clause

FAR 52.239-zz, *Incident and Threat Reporting and Incident Response Requirements for Products and Services Containing Information and Communications Technology*, includes several new requirements for contractors. We highlight a few of the most significant requirements below:

Broad Range of "Security Incidents": The proposed contract clause would require contractors to report any security incidents that "may have occurred" as long as the incident "involve[es] [1] a product or service provided to the Government that includes [ICT], or [2] the information system used in developing or providing the product or service." This is a different approach than the existing DFARS 252.204-7012 framework because this rule applies based on an information system's use or connection to a product or service, rather than the

sensitivity of the information (e.g., Controlled Unclassified Information [CUI]) residing on the information system. The term "security incident" is also not limited to traditional cybersecurity incidents; it could include imminent or actual violations of law, security policies, security procedures, or acceptable use policies. The term also covers the transfer of classified information or CUI to an information system below the authorized security level.

8-Hour Incident Reporting Deadline with Periodic Updates: The proposed contract clause would require contractors to report all security incidents to the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency's (CISA) incident reporting portal within eight hours of discovery that a security incident may have occurred and update that submission every 72 hours thereafter until all eradication or remediation activities have been completed.

Software Bill of Materials: The proposed contract clause would require contractors to maintain, and potentially provide to the CO, an SBOM for each piece of computer software used in performance of the contract. The clause would also require contractors to update the SBOM whenever the software is updated with a new build or major release. Finally, the clause would require SBOMs to include minimum elements identified in the U.S. Department of Commerce's Minimum Elements for a Software Bill of Materials, Section IV (the version current at the time of the relevant solicitation). This provision is likely a surprise to many in industry. The Executive Order (EO) that led to this proposed rule specifically mentioned SBOMs but in a different context: the EO contemplated SBOMs for software that the Government procures. It is not clear why the FAR Council chose to insert a potentially broader SBOM requirement—one that applies to all software that contractors use in performance of a contract—as part of a rule implementing a different part of the Executive Order that says nothing about SBOMs. As discussed further below, the substance of this SBOM requirement—a link to the Department of Commerce's website—is an example of a questionable "dynamic incorporation."

Activities to Support Incident Response: The proposed contract clause would impose several other requirements on contractors to cooperate with the Government's requests during an incident response. This would include:

- Preserving data and information related to the incident prevention, detection, response, and investigation within the information systems used in developing or providing ICT products or services to the Government for at least 18 months;
- Developing customization files identifying customizations that differ from manufacturer defaults on devices, computer software, applications, and services; and, upon request, providing current and historical customization files to the program office, CISA, or Federal Bureau of Investigation (FBI); and
- Providing the contracting agency, FBI, and/or CISA "full access and cooperation" to contractor personnel and systems after a reported security incident to ensure effective incident response, investigation, and threat hunting activities.

Reporting Cyber Threat Indicators and Defense Measures: The proposed contract clause would also require contractors to subscribe to CISA's Automated Indicator Sharing (AIS) capability, and to share (i) cyber threat indicators observed on ICT used in contract performance and (ii) recommended defensive measures.

Contractors that submit cyber threat indicators and defensive measures through AIS will receive legal protections under the Cybersecurity and Information Sharing Act of 2015 (6 U.S.C § 1505).

Subcontractor Flow Down Required: The proposed clause would require prime contractors to flow down the clause to subcontractors when ICT is used or provided in performing the subcontract. Subcontractors also have further obligations to flow the clause down to their affected subcontractors. Following on from the prime's reporting obligations, the prime must require that subcontractors notify the prime and the next higher-tier subcontractor within eight hours of discovering a security incident.

FAR 52.239-AA, *Security Incident Reporting Representation*

The proposed Reporting Representation clause would be mandatory for all solicitations. Paragraph (b) of the clause would require offerors to represent that they have submitted all security incident reports on existing contracts "in a current, accurate, and complete manner," and that they have required each subcontractor to include the requirements of paragraph (f) of the Incident Reporting and Response clause in their lower-tier subcontracts. The representation, however, would be limited to security incident reports required under the proposed contract clause FAR 52.239-zz; it would not encompass any reports that might have been required under other contract clauses such as DFARS 252.204-7012.

Representations like these heighten the risk contractors face from enforcement actions under the False Claims Act. In fact, the preamble to the proposed rule states: "This proposed rule underscores that the compliance with information-sharing and incident-reporting requirements are material to eligibility and payment under Government contracts," and that its mechanisms "ensure that entities or individuals that knowingly put U.S. information or systems at risk, by violating these cybersecurity requirements, are held accountable."

FAR Case No. 2021-0019, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

Many aspects of the second proposed rule may bring more welcome news for contractors because it strives for standardization. It also emphasizes that "[a]gencies are responsible for determining what information systems are FIS" and that agencies need to define the security requirements early in the acquisition process. This should, hopefully, bring an end to contracts that instruct contractors to "comply with FISMA, FIPS 199, FIPS 200, and NIST 800-53," without identifying what portions of those frameworks or what controls within these catalogs might be applicable. Under the proposed rule, the Government would use two standard contract clauses depending on whether the FIS is, or would be, cloud-based:

- FAR 52.239-XX, *Federal Information Systems Using Cloud Computing Services*
- FAR 52.239-YY, *Federal Information Systems Using Non-Cloud Computing Services*

COs will be required to include at least one of these clauses in all contracts to develop, implement, operate, or maintain an FIS. This includes contracts for COTS items and contracts below the simplified acquisition threshold.

Cloud-Based Systems: For procurements to acquire services to develop, operate, or maintain an FIS using cloud computing services, the proposed clause would task agencies with identifying the FIPS-199 impact level and corresponding FedRAMP authorization level. Contractors would then be required to implement and maintain the safeguards and controls associated with that FedRAMP authorization level. The proposed clause also would include an expansive indemnification requirement, discussed in more depth below.

Non-Cloud Systems: The proposed clause for non-cloud systems would also require agencies to identify the appropriate FIPS-199 impact level and security controls for procurements of services for non-cloud computing services. Rather than applying a single FedRAMP security baseline, agencies will have to determine which specific controls to require for each acquisition and FIS and address issues such as multifactor authentication, administrative accounts, consent banners, Internet of Things (IoT) device controls, and assessment requirements. The proposed clause would require the CO to select applicable security controls from several existing sources, including NIST publications: SP 800-53, "Security and Privacy Controls for Information Systems and Organizations"; SP 800–213, "IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements"; SP 800–161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations"; and SP 800–82, "Guide to Industrial Control Systems Security."

The proposed clause also contemplates several additional requirements, such as:

- Government access. Contractors would be required to provide CISA and other specified Government representatives with full access to Government and Government-related data and contractor personnel for inspections, audits, and investigations.
- Periodic assessments. For FIS designated at the moderate or high FIPS-199 level, contractors must conduct periodic assessments as described in the proposed rule.

Indemnification Obligations: Both proposed clauses (for cloud-based and non-cloud systems) contain an expansive indemnification provision. The indemnification provisions would obligate contractors to indemnify the Government from ***any liability*** arising out of performance, due to either (a) the contractor's introduction of certain information or matter into Government data, or (b) the contractor's unauthorized disclosure of information or material. The preamble explains that the FAR Council intended this clause to operate as a waiver provision "to change the analysis from negligence, which is the defense, to strict liability, which doesn't allow for a defense." The proposed rule does not provide any other basis for including this indemnification provision, other than a brief note that the language "was taken from industry terms of service agreements for cloud services providers."

Subcontractor Flow Down: The proposed clauses both require that prime contractors flow down the substance of the clause in any subcontracts for services to develop, implement, operate, or maintain the FIS.

For Both Rules: A Looming Test for Dynamic Incorporation?

Throughout both proposed rules, the Government has included URLs or referenced other existing publications —the contents of which will likely change over time and, at least theoretically, immediately become binding in the FAR as they evolve. For example, the FAR Council has acknowledged that the version of the SBOM minimum elements referenced, the Department of Commerce's Minimum Elements for a Software Bill of Materials, Section IV, will change over time, and has asked contractors to use the version that is current as of the issuance of the solicitation. Although incorporated reference to external, living documents is becoming an increasingly common practice in the FAR, its lawfulness is questionable. Arguably, this is the same type of "dynamic incorporation" that the Office of the Federal Register's rules prohibit by providing that any incorporation is limited to a specific "edition of the publication"; and that "[f]uture amendments or revisions of the publications are not included." 1 C.F.R. § 51.1(f). Courts have also rejected "dynamic incorporation" in other contexts. Thus, it is unclear whether this approach will survive in any final rule.

***

Wiley's Government Contracts and cross-disciplinary teams will continue to monitor these and similar regulations issued by federal agencies to establish cybersecurity and incident response obligations for contractors.