Updates

The Federal Acquisition Regulatory (FAR) Council published two proposed rules on October 3, 2023, that would impose significant new cybersecurity obligations on government contractors.

Including requiring them to share information with the government about actual and imminent cyber incidents, provide software bills of materials (SBOMs) to government customers, and make representations about compliance that will create new False Claims Act (FCA) risks.

The proposed rules (FAR Case 2021-017 [Cyber Threat and Incident Reporting and Information Sharing] and FAR Case 2021-019 [Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems]) represent a substantial expansion of contract requirements related to cybersecurity and will affect large numbers of contractors, including commercial companies. They also present new risks of FCA enforcement activity

related to cybersecurity—a priority of the U.S. Department of Justice (DOJ) under its Civil Cyber-Fraud Initiative launched in October 2021. The proposed rules are open to public comment through December 4, 2023.

In this Update, we summarize the FAR Council's proposed rules and their significance.

Background: Executive Order 14028

By way of background, both proposed rules were issued pursuant to President Biden's May 12, 2021, Executive Order 14028 (EO 14028), *Improving the Nation's Cybersecurity*, which initiated a series of agency actions in response to the SolarWinds and other high-profile cybersecurity incidents affecting government networks and critical infrastructure. Following EO 14028, the FAR Council began rulemaking efforts to carry out recommendations in EO 14028.

Neither of the proposed rules is binding on contractors as of yet; a final rule would need to be published based on public comments before the rules would have the force of law.

Nevertheless, contractors should not delay in making preparations for new clauses in their contracts.

Cyber Incident Reporting and Information Sharing

The first proposed rule (Cyber Incident Rule) is a sweeping rule with broad application to any contract that "may include" information and communications technology (ICT) in support of the product or service being offered to the government. ICT would be defined in the FAR to include items like computers and peripheral equipment, as well as software and applications—a vast category. Indeed, according to the proposed rule, the FAR Council assumes that 75% of all contractors are awarded contracts that include some form of ICT.

Among other things, the Cyber Incident Rule contains the following:

Security Incident Reporting and Data Preservation. The Cyber Incident Rule would adopt a new FAR clause at FAR 52.239 requiring that contractors "immediately and thoroughly" investigate "all indicators that a security incident **may have occurred**" and submit information to the Cybersecurity and Infrastructure Security Agency (CISA) within eight hours of discovery (emphasis added). Contractors would then provide updates to CISA every 72 hours until all eradication or remediation activities are complete.

Significantly, the definition of "security incident" includes an "actual **or potential**" occurrence of certain cyber-related events, including those that pose "actual or **imminent** jeopardy" to information or information systems, as well as those resulting in the discovery of malicious code discovered on an information system or the unauthorized transfer of classified or controlled unclassified information (CUI).

The proposed new contract clause would also mandate that contractors collect and preserve data for at least 12 months following a security incident and provide it to the government if requested. If the government elects to conduct an incident or damage assessment, contractors would be required to provide various information to the government and any third-party authorized accessor.

Although for many years defense contracts have included a 72-hour reporting requirement for cyber incidents in DFARS 242.204-7012, until now, there has not been a corresponding incident reporting requirement in the FAR. Acknowledging that various reporting timeframes for cyber incidents exist, the rule invites public comments about "harmonization" of such requirements.

The proposed rule also would require offerors seeking government contracts to represent (1) that they have submitted all security incident reports in a current, accurate, and complete manner; and (2) whether they have required the clause to be included in lower-tier subcontracts.

Requirement for an SBOM. The proposed rule also includes a long-awaited requirement: the SBOM.

An SBOM is a list of a software's components, similar to a list of ingredients on a food product. It is intended to provide a formal record of the details and supply chain relationships of components used in building software. President Biden's EO 14028 specifically called for SBOMs as part of a series of actions meant to enhance software supply chain security.

Under the proposed rule, contractors would be required to maintain—and provide to the government—an SBOM for software "used in the performance of the contract," regardless of whether a security incident has occurred. According to the rule, an SBOM is "critical in incident response, as they allow for prompt identification of any sources of a known vulnerability."

Under the proposed rule, each SBOM "shall be produced in a machine-readable, industry-standard format and shall comply" with certain minimum elements of an SBOM in guidance issued by the U.S. Department of Commerce's National Telecommunications and Information Administration.

The rule invites "input" on various issues regarding the SBOM.

Information Sharing. The rule also would require contractors to provide access to and cooperate with CISA in relation to threat hunting and incident response. In response to a security incident, CISA, the Federal Bureau of Investigation (FBI), the U.S. Department of Justice, and the contracting agency would have "full access" to a contractor's information or equipment "necessary for forensic analysis." However, such "full access" must be "consistent with applicable laws, regulations, and Governmentwide policies that limit or prohibit access to data[.]" This latter caveat will raise interpretive questions about whether and when information may be properly withheld.

Contractors would also be required to complete certain activities to implement Internet Protocol V6 (IPV6), a next-generation internet protocol.

Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems (FIS)

The second proposed rule (FIS Rule) provides standardized cybersecurity policies, procedures, and requirements for contractors that develop, implement, operate, or maintain a FIS, which the rule defines as "an information system used or operated by an executive agency, by a contractor of an agency, or by another organization, on behalf of an agency." According to the FAR Council, by standardizing a set of minimum cybersecurity standards to be applied consistently to FISs across federal agencies, the proposed rule would ensure that such systems are better positioned to protect against cyber threats.

The proposed rule would adopt two clauses: one for cloud-based services and one for on-premises computing services. For cloud-based services involving an FIS, the proposed clause would require contractors to: (1) implement and maintain safeguards and controls in accordance with the Federal Risk and Authorization Management Program (FedRAMP) level specified by the agency, (2) engage in continuous monitoring activities, and (3) provide continuous monitoring deliverables as required by FedRAMP. The proposed rule also imposes obligations on contractors related to disposal of government data.

For on-premises computing services involving an FIS, the proposed rule would require agencies to specify security and privacy controls necessary for contract performance based on enumerated National Institute of Standards and Technology (NIST) Special Publications. It would also require awarding agencies to specify the necessary security and privacy controls for a contract based on an impact analysis using Federal Information Processing Standard (FIPS) Publication 199. Contractors would have to undergo annual cyber threat and vulnerability assessments, as well as perform an annual, independent assessment of the security of each FIS.

Takeaways

The proposed rules reflect the administration's efforts to obtain more information in the possession of contractors about cybersecurity incidents and vulnerabilities. It also underscores the Biden administration's focus on "harmonization" of cybersecurity-related regulations, which is an objective highlighted in the White House's March 1, 2023, National Cybersecurity Strategy.

The proposed rules raise significant new issues and considerations for government contractors.

- Contractors should review the proposed rules and assess their potential impact on their businesses. The Cyber Incident Rule, in particular, will affect significant numbers of contractors—including those serving only civilian agencies—with new requirements.
- Among other things, contractors should examine the definitions of terms such as "information and communications technology" and "security incident" in the Cyber Incident Rule. For many contractors, further investments and resources will be necessary to comply with the proposed rules. Contractors will also need to make preparations to flow down clauses to their subcontractors (and lower-tiered subcontractors).
- The Cyber Incident Rule will raise numerous implementation issues. Contractors will have to be prepared to make incident reports almost immediately, often with incomplete information about the incident and its impact. The rule also raises questions about the extent to which companies can disclose to the government the information required by the rule while protecting their own confidences and trade secrets. The definition of "full access" in the rule will likely be among the provisions to generate close scrutiny.
- The SBOM requirement raises major considerations for contractors that sell software to the government, as well as those that incorporate software into their products. Contractors will want to familiarize themselves with the essential elements of an SBOM and evaluate steps necessary to obtain SBOMs from software producers in their supply chains.
- Both rules highlight new risks of FCA investigations and qui tam litigation related to cybersecurity. Inaccurate representations to the government required under the rules related to cyber incidents and other matters will create significant exposure to risks of liability under the FCA, which carries treble damages and penalties. Implicitly referring to the FCA, the Cyber Incident Rule notes that it is intended, in part, to ensure that entities and individuals that "knowingly put U.S. information or systems at risk, by violating [the rule's] cybersecurity requirements, are held accountable."
- As noted above, the rules are subject to change. Contractors and other stakeholders may wish to consider submitting comments on the rules by the December 4, 2023, deadline.

Authors

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Julia M. Fox

Counsel
JuliaFox@perkinscoie.com

Explore more in

Government Contracts Privacy & Security

Related insights

Update

Cybersecurity Implementation Plan Offers a Roadmap for Cyber Priorities

Update

US Supreme Court Clarifies Knowledge Requirement in False Claims Act Cases—Raising New Interpretive Issues