PAUL HASTINGS

Stay Current

October 2023

Follow @Paul_Hastings

"FAR" Reaching Consequences: Proposed FAR Cybersecurity Requirements Will Add New Obligations for Contractors

By Aaron Charfoos, John Michels & Marisa Polowitz

Earlier this month the Federal Acquisition Regulatory ("FAR") Council released two draft rules which would impose new cybersecurity requirements for federal contractors. The proposed rules, **Cyber Threat and Incident Reporting and Information Sharing** and **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems**, target new requirements for sharing of information related to cyber threats, compliance representations, provision of software bills of materials ("SBOMs"), and cybersecurity requirements for Federal Information Systems ("FIS").

These changes stem from the May 2021 Cybersecurity Executive Order, "Improving the Nation's Cybersecurity" (Executive Order 14028), focused on improving the nation's cybersecurity, including enhancing protection of Government networks. If finalized in current form, the new requirements will require contractors to make substantial adjustments to satisfy these significant changes. Both proposed rules provide that compliance is "material to eligibility and payment under Government contracts."

The comment period for each of these proposed rules closes December 4, 2023.

Below, we provide an overview of the key requirements of each of the proposed rules, and provide some high-level advice on what contractors should do to prepare.

I. Cyber Threat and Incident Reporting and Information Sharing (FAR Case 2021-017)

The proposed Cyber Threat and Incident Reporting and Information Sharing rule would apply to contractors that provide or require the use of information and communications technology ("ICT"). It aims to revise and increase information sharing and cybersecurity policies for federal contractors, and additionally includes new requirements for subcontractor compliance as well. Changes center on the sharing of threat and incident-related information between the federal government and information technology and operational technology service providers, as well as outlining requirements for "preparation and maintenance activities" pertaining to incident preparedness and response. The FAR Council estimates that approximately 75% of all government contractors are awarded contracts which include ICT.

Included in the proposed amendment are updated definitions and terminology. Amongst others, notable updates to key terms include:

- **ICT:** The proposed rule specifically expands the existing enumerated scope of ICT by including the elements of telecommunications services, electronic media, Internet of Things ("IoT") devices, and operational technology.

- **Security Incident:** The proposed rule broadly defines an incident to include an actual or potential occurrence of "any event that may pose an actual or imminent threat to the integrity, confidentiality, or availability of information or an information system," the discovery of malicious software, and the transfer of classified or controlled unclassified information to an unaccredited information system. It also includes any actual or potential occurrence of any event or series of events which "constitutes a violation or imminent threat of violation of law, security policies or procedures, or acceptable use policies." The definition encompasses a broad range of potential indicators and circumstances, implicating a wide range of possible events contractors will need to be prepared to address. This definition of "security incident" will be utilized to determine whether certain requirements of the proposed rules have been triggered.

The proposed changes include, but are not limited to, the following requirements:

- **Security Incident Reporting and Data Preservation:** Contractors will be required to "immediately and thoroughly" investigate "all indicators that a security incident may have occurred." The broad scope of the proposed rule's expanded definition of what constitutes a security incident means that contractors will need to be prepared to rapidly respond to a broad range of indicators. Contractors must also collect and preserve data related to security incident prevention, detection, investigating, and response for a minimum of 12 months following an incident and to provide it upon request.

- **Security Incident Harmonization:** The proposed rule would require mandatory reporting of security incidents through the CISA incident reporting portal within 8 hours of discovering that an incident may have occurred. Subsequent mandatory updates will need to be provided every 72 hours thereafter until "the Contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities."

- **Subcontractor Requirement:** Subcontractors of the next lower tier would be required to notify the prime contractor and next tier higher subcontractor within 8 hours of discovery of the threat. This will require more and generally faster reporting of threat indicators by and to contractors on varying levels.

- **CISA Engagement Services:** Contractors would be required to provide access to, and cooperate with, Cybersecurity and Infrastructure Security Agency ("CISA") engagement services in relation to threat hunting and incident response.

- **"Full access" to Contractor Information and Information Systems:** Upon request from CISA, the FBI, or the contracting agency, a contracting officer will be required to provide "full access" to the relevant contractor information, information system(s), and personnel in response to security incidents. Full access includes "physical and electronic access to contractor networks, systems, accounts dedicated to Government systems, other infrastructure housed on the same computer network, other infrastructure with a shared identity boundary or interconnection with the Government system, and provision of all requested Government or government-related data." The scope of access is defined broadly, but specifically excludes data such as the contractor's business records that do not incorporate Government data, and

data such as operating procedures, software coding or algorithms, that are "not uniquely applied to the Government data." Contractors will be required to respond to access requests within 96 hours of receiving the request.

- **Software Bills of Materials ("SBOM"):** Contractors would be required to develop and maintain a "software bill of materials," a list of software's components, for any and all software used in the performance of the contract, whether or not a security incident has occurred. Contractors will be required to update the SBOM upon any major update to, or new or major release of computer software used in performance of the contract.

- **Compliance When Operating in a Foreign Country:** The proposed rule requires both contractors and subcontractors to report security incidents and take enhanced action to support incident response. Feedback is specifically requested for this amendment in regard to obstacles to incident reporting and response companies anticipate while operating in foreign countries.

II. Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems (FAR Case 2021-019)

This proposed rule, Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems, is somewhat narrower in terms of its scope, but nonetheless may have far-reaching impacts on covered contractors. The rule aims to standardize cybersecurity requirements for contractors that develop, implement, operate or maintain a FIS, which is defined 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." Whether a given system constitutes a FIS is determined on a case-by-case basis, but in general is a set of information resources that are either owned or controlled by, or operated on behalf of, a federal agency. Some examples include computers, office machines, websites, software, and telecommunications systems.

The proposed rule adopts two new clauses to be included in contracts for services to develop, implement, operate, or maintain a FIS. The clauses differentiate between cloud-based and on-premises computing services that constitute or form a part of a FIS.

For cloud-based services, contractors would be required to:

- Implement and maintain safeguards at the requisite level in accordance with the Federal Risk and Authorization Management Program ("FedRAMP");

- Engage in continuous monitoring activities;

- Provide the required continuous monitoring deliverables required by FedRAMP; and

- Adhere to government data disposal obligations as articulated within the FAR.

For on-premises/non-cloud services, the rule would require:

- Agencies to (1) perform an impact analysis using Federal Information Processing Standard ("FIPS") Publication 199 to categorize the information processed, stored, or transmitted by the FIS, and (2) apply the requisite privacy and security controls based on the categorization of the FIS. These measures include, but are not limited to, multifactor authentication, administrative accounts, and IoT device controls.

- Contractors to adhere to annual cyber threat and vulnerability assessments and independent annual security assessments of FIS security.

What Should Contractors Do to Prepare?

While these proposed rules are subject to change prior to finalization, contractors should take steps now to prepare.

1. **Consider submitting a comment**. As noted above, the comment period on the two proposed rules expires on December 4, 2023. Contractors should consider whether the proposed rules as drafted may lead to significant compliance issues as applied to their organization, and, where warranted, consider submitting a comment prior to the close-out date.

2. **Determine whether and the extent to which the proposed rules apply to your organization**. The two proposed rules have different standards of applicability, and in some cases distinguish between cloud-based and on-premises computing services. Contractors should review their current and prospective government engagements and determine what which rules would apply to their product and services offerings.

3. **Benchmark organizational policies and procedures against the requirements of the proposed rules**. Contractors should pressure-test existing policies and procedures, and evaluate any gaps that the proposed rules would create if they are enacted as presently drafted. While the proposed rules may change in some ways prior to being finalized, this preparatory step can help avoid being caught flat-footed when the rules are ultimately finalized.

4. **Tabletop potential practical, technical, and legal issues**. The proposed rules raise a number of practical, technical, and legal compliance questions. Contractors should examine how the proposed rules might apply in practice, and assess potential issues with some of the more wide-sweeping changes, such as the "full access" requirement discussed above.

Conclusion

These proposed rules introduce new and heightened cybersecurity obligations for contractors. If finalized in this current form, contractors will be required to respond rapidly to threat indicators and to report those threats with an often incomplete picture of the full circumstances. Additionally, contractors will need to develop policies and procedures reflecting the new demands enabling information sharing and access to the relevant agencies in instances of a security incident.

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises on compliance with cybersecurity requirements at the federal, state, and international levels. If you have any questions concerning how to better prepare for these proposed rules or other cybersecurity requirements, please do not hesitate to contact a member of our team.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Chicago lawyers:

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

John J. Michels
1.312.499.6017
johnmichels@paulhastings.com

Marisa Polowitz
1.312.499.6093
marisapolowitz@paulhastings.com