LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Unpacking The FAR Council's Cybersecurity Rules Proposal

By **Townsend Bourne and Lillia Damalouji** (October 25, 2023, 5:51 PM EDT)

Townsend Bourne

Lillia Damalouji

On Oct. 3, the Federal Acquisition Regulatory Council **released** two long-awaited proposed rules for federal contractor cybersecurity, stemming from the Biden administration's May 2021 Cybersecurity Executive Order No. 14028.

The proposed rules relate to cyber threat and incident reporting and information sharing,[1] and standardizing cybersecurity requirements for unclassified federal information systems[2]. The comment period for both rules is currently open and is scheduled to close on Dec. 4.

While there is a lot to unpack in the proposed rules, it is critical for companies to begin working to understand the new requirements, assess their cybersecurity posture, systems, contracts, and processes, and ensure they are on track to comply, as they may become enforceable as soon as next year.

As indicated by the proposed rules, these requirements will be material to eligibility and payment under government contracts, which certainly indicates that this is an area ripe for False Claims Act enforceability, and likely will be another area of focus for the U.S. Department of Justice's Civil Cyber Fraud Initiative.

We expect to see robust feedback throughout the comment period and anticipate that the FAR Council may re-assess some of these requirements as potential compliance challenges are identified. We summarize and highlight key points below.

Cyber Threat and Incident Reporting and Information Sharing

The proposed rule relating to Federal Acquisition Regulation Case No. 2021-017 is meant to apply to contracts where information and communications technology is used or provided in the performance of the contract. It includes numerous updated definitions, requirements and representations relating to contractor cybersecurity.

The representations and requirements are not limited to incident reporting and information sharing — they also include preparation and maintenance activities, enhanced collaboration with agencies and subcontractor compliance.

The scope of the rule represents a shift in how contractors will need to think about cybersecurity compliance — from a focus in the current FAR and Defense Federal Acquisition Regulation Supplement rules on protecting certain types of sensitive government information within information systems, to scoping based on technology that is provided to the government and information and systems related to that technology.

Updates to Relevant Terms and Definitions

The proposed rule includes new definitions for "IoT devices," "Operational Technology," "Telecommunications Equipment," "Telecommunications Services" and "Security incident" to be

included in FAR 2.101.

While we have seen the National Institute of Standards and Technology provide guidance on cybersecurity for smart devices connected to the Internet of Things, this is the first time that several of these terms have been defined in the FAR and will be incorporated into federal contracts. Accordingly, organizations will have to assess these new definitions as they apply to this proposed rule.

Information and Communications Technology

This definition provides:

> [information and communications technology] means information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include but are not limited to the following: Computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; telecommunications services; customer premises equipment; multifunction office machines; computer software; applications; websites; electronic media; electronic documents; Internet of Things (IoT) devices; and operational technology."

The definition updates an earlier version with additional examples of information and communications technology, including telecommunications services, electronic media, IoT devices and operational technology. This brings additional devices and technology within the scope of contractors' cybersecurity compliance obligations.

Telecommunications Equipment and Telecommunications Services

These are new definitions in the FAR. In addition to informing the scope of the new proposed rules, these definitions may help inform contractor compliance with FAR requirements relating to Section 889 implementing prohibitions on supply and use of covered telecommunications equipment and services. Notably absent from the FAR provisions implementing Section 889 is a definition for these terms.

Security Incident

This definition mirrors a similar provision in the Federal Information Security Management Act, but also includes as an "incident" discovery of malicious computer software and the "transfer of classified or controlled unclassified information" onto a system that is not accredited or authorized at the appropriate security level.

This is likely to cause headaches for contractors and agency personnel as there is not yet a FAR rule specifying requirements for protection of controlled unclassified information in nonfederal systems, or clear accreditation or authorization rules for such systems.

Further, this could bring potential spillage of classified information within the scope of the rules, which may ultimately be determined to be inappropriate where protection of classified information is governed by a different set of laws and regulations.

New Requirements for Federal Contractors

The proposed rule prescribes new requirements, including:

Software Bill of Materials

Federal contractors will be required to develop and maintain a software bill of materials for any software used in contract performance.

There is a separate rulemaking effort relating to supply chain software security (open FAR Case No. 2023-002), for which a proposed rule has not yet been released, and parallel efforts by the U.S. Cybersecurity and Infrastructure Security Agency, or CISA, to establish a common attestation form for software producers.

It is unclear why the software-bill-of-materials requirement was included in the new proposed rule and, as a result of comments, the FAR Council may determine this requirement should be removed and addressed in the rulemaking specific to software security.

Sharing Cyber Threat Indicators

Other "preparation and maintenance activities" in the proposed rule include subscribing to automated indicator sharing capability and sharing cyber threat indicators using AIS during performance.

Historically, cyber threat and information sharing has been facilitated through voluntary programs with contractors. Where the proposed rule would mandate such sharing, contractors likely will want to seek guidance through comments on the relevant definitions and make appropriate determinations on what is to be shared.

IPv6 Implementation

Federal contractors will be required to complete Internet Protocol version 6 implementation activities in accordance with the Office of Management and Budget's Nov. 19, 2020, Memorandum M-21-07 on completing the transition to IPv6.

In recent years, the government has attempted to introduce IPv6 into federal contracts via agency-specific policies and guidance documents. Accordingly, this implementation of the OMB's 2020 memorandum does not necessarily come as a surprise, and is on-trend with recent agency shifts. However, where it does not directly relate to cyber threat and incident reporting, comments may question its inclusion in the proposed rule.

CISA Engagement Services

Federal contractors will be required to allow access and cooperate with CISA for purposes of "threat hunting and incident response." The rule notes that recommendations from CISA are to be implemented only after consultation between the contractor and the agency.

While the primary purpose of this requirement is to help CISA reduce cybersecurity risks by observing potential adversary activity on contractor systems, open questions remain concerning the extent of CISA's visibility into these systems.

For example, it is not clear whether CISA is limited to viewing an organization's metadata or if analysts could have access to all content in an organization's system. We anticipate extensive feedback on this requirement.

Access to Contractor Information and Systems

In the event of a security incident, federal contractors will be required to provide CISA, the Federal Bureau of Investigation and the contracting agency with full access to applicable contractor information, information systems and personnel. The proposed rule includes a definition of "full access" that is incredibly broad.

As with the previous requirement, concerns arise with regard to the broad scope of access, whether the government will be able to share contractor information, with whom and whether this information could be attributable to a specific organization.

Operations in a Foreign Country

The FAR Council recognizes that contractors operating in a foreign country may be subject to multiple requirements and added complexity. In certain countries, the requirements in the new proposed rule may conflict with existing reporting requirements and obligations. The proposed rule seeks specific feedback on barriers for companies that operate outside the U.S.

Security Incident Reporting Timelines

Federal contractors will be required to report security incidents through the CISA incident-reporting portal within eight hours of discovery and to provide updates every 72 hours thereafter until the incident is eradicated or remediated.

While establishing timed requirements for reporting security incidents is certainly a commendable goal, meeting such a deadline will likely prove to be difficult for federal contractors. Contractors must first determine whether a cybersecurity issue is a "security incident" as defined by the rule, and if so, must begin the reporting process with CISA — all within eight hours of discovery.

Further, required updates every 72 hours may cause contractors to divert resources that otherwise would be focused on incident response and remediation, in order to make updates.

In addition to these timing concerns, the security incident reporting timelines are inconsistent with existing incident reporting timelines contained in other federal government contracting requirements and from other regulatory agencies, and may make compliance more rather than less cumbersome.

For example, the current reporting time period in the DFARS is 72 hours. Contractors likely already have incident response plans that must build in different deadlines from various laws and regulations. One of the stated goals of recent federal efforts is to harmonize requirements, which this does not seem to do.

New Contract Clauses

The proposed rule includes new additions to FAR Part 39 on acquisition of information technology, as well as two new FAR clauses to be included in solicitations and contracts with final numbering to be determined.

FAR 52.239-ZZ, Reporting and Incident Response Requirements

FAR 52.239-ZZ on incident and threat reporting, and incident response requirements for products and services containing information and communications technology is a new clause that includes requirements discussed above relating to (1) security incident investigation, response and reporting; (2) software bill of materials; (3) sharing cyber threat indicators and defensive measures; and (4) IPv6. The clause is to be a required flow-down in all subcontracts where information and communications technology is used or provided.

FAR 52.239-AA, Security Incident Reporting Representation

FAR 52.239-AA on security incident reporting is a new clause that requires offerors to represent they have (1) submitted in a current, accurate and complete manner all security incident reports required by existing contracts; (2) flowed down to each first-tier subcontractor requirements to notify the company of security incidents within eight hours of discovery, and for reporting security incidents.

Applicability

The new FAR provisions are to be included in all solicitations and contracts. There are no exceptions for contracts below the simplified acquisition threshold, for commercial products and services or for commercially available off-the-shelf products. This differs from current FAR and DFARS cybersecurity requirements, which include carveouts for commercially available off-the-shelf procurements.

Note, however, the rule is only meant to affect contracts where information and communications technology is used or provided in the performance of the contract. The proposed rule asserts agencies do "not have a way to track awards that may include ICT" so the provisions will be included in all solicitations and contracts.

The government estimates that 75% "of all entities are awarded contracts that include some ICT." Contractors will need to assess their contracts and inventory and the products and services they provide to the federal government in order to be able to articulate clearly when they believe the new clauses do not apply.

Determining applicability is sure to be an area heavily covered in comments.

Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

The proposed rule relating to FAR Case 2021-019 provides standardized requirements for contractors that develop, implement, operate or maintain a federal information system.

It provides a new definition for federal information systems and creates a new FAR subpart that will require agencies to conduct extensive acquisition planning and assessments to determine the appropriate security requirements for each FIS. Of note, the new proposed FAR clauses distinguish between FIS requirements for "cloud computing services" and "non-cloud computing services."

Updates to Relevant Definitions

The proposed rule includes several new definitions, the most notable being the definition for an FIS:

> *"Federal Information System" (FIS)*
>
> Means an information system[3] used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency;
>
> On behalf of an agency as used in this definition, means when a contractor uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Government data, and those activities are not incidental to providing a service or product to the Government.[4]

While still not crystal clear, this is a welcome definition in the FAR where industry has struggled in some cases to determine whether certain systems should be characterized as operated "on behalf of" the government and thus subject to one set of cybersecurity requirements or are more appropriately defined as "non-federal systems."

Historically, in the cybersecurity context, a "federal information system" operated by a contractor on behalf of an agency has been understood to mean a system for which the contractor "steps into the shoes" of the agency to maintain an information system for the purpose of housing government data, and applies to systems requiring security controls from NIST Special Publication 800-53 — the prior version of this was titled security controls for "Federal Information Systems."

This is to be distinguished from internal contractor information systems that house information relating to a federal contract, incidental to providing a product or service to the government, and require security controls from NIST SP 800-171, which will be most contractor-operated systems.

However, it is possible individual agencies and contracting officers may have different interpretations, and ensuring a consistent understanding is key. This is likely to be an area of focus for public comments.

New Requirements for FIS Contracts

The new FAR provisions include policies and procedures for agencies as well as requirements for contractors relating to the acquisition of, and contracts for, the following FIS services.

FIS Using Noncloud-Computing Services

For an FIS using noncloud-computing services, agencies must (1) use Federal Information Processing Standard 199 to perform an impact analysis relating to information within the system; and (2) address multifactor authentication, administrative accounts, consent banners, IoT device controls and assessment requirements for each contract.

This hopefully means it will be clear from the agency perspective, and communicated clearly to contractors, when the new requirements will apply to a particular solicitation or contract.

Contractors will have obligations with respect to records management and agency access to government data, government-related data and contractor personnel involved in contract performance, including access by CISA.

In addition, for certain systems, contractors will be required to develop a system security plan, implement and maintain extensive security controls, conduct annual security assessments, and cyber threat hunting and vulnerability assessments, as well as comply with continuous monitoring and supply chain risk management requirements.

FIS Using Cloud-Computing Services

For an FIS using cloud-computing services, agencies will require Federal Risk and Authorization Management Program authorization at the level determined by the agency. FedRAMP authorization requires a third-party assessment and continuous monitoring in accordance with guidance published by the FedRAMP Program Management Office.

This is an important addition to the FAR. While FedRAMP has been a government program run through the General Services Administration since 2011, it was only recently codified via statute as part of the fiscal-year 2023 National Defense Authorization Act.

The recent codification and inclusion in the FAR means we are likely to see more activity from the FedRAMP Program Management Office, further refining the program. Efforts already are underway to review and improve the program through the Federal Secure Cloud Advisory Committee.

For systems designated as "high," all government data must be maintained within the U.S. or its outlying areas, unless otherwise specified in the contract. This is similar to the existing DFARS requirement for cloud service providers at DFARS 252.239-7010.

New Contract Clauses

The proposed rule includes a new FAR subpart 39.X relating to FIS, and two new FAR clauses to be included in solicitations and contracts as prescribed in FAR 39.X04 (final numbering to be determined)

FAR 52.239-YY, FIS Using Noncloud-Computing Services

FAR 52.239-YY will require contractors to comply with multiple requirements, as discussed above, to include conducting annual assessments, developing and maintaining controls consistent with NIST guidelines, managing access to government data and government-related data, and complying with CISA directives.

The clause is to be flowed down in all subcontracts for services to develop, implement, operate or maintain an FIS using services other than cloud-computing services.

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

FAR 52.239-XX will require contractors to achieve and maintain FedRAMP authorization at a specified level, institute proper controls and access limitations for government data and government-related data, adhere to applicable security guidelines, allow access to authorized government representatives, and maintain certain high-impact data within the U.S.

The clause is to be flowed down in all subcontracts for services involving an FIS using cloud-computing services.

Both of these new FAR clauses include indemnification provisions that will require contractors to indemnify the government against potential or actual loss or damage of government data, and to waive the government contractor defense.

This represents the government's attempt to build in an indemnification clause similar to what we see in the commercial context for contractors housing its data.

While the proposed rule states it will be applicable to contracts at or below the simplified acquisition threshold, and to contracts for commercial products and commercial services, including commercially available off-the-shelf procurements, the proposal limits its applicability to "contracts for services to develop, implement, operate, or maintain a FIS."

The FAR Council estimates that the rule will apply to 84 contractors annually — 28 noncloud FIS contractors and 56 cloud FIS contractors — and approximately 168 offerors. This suggests the proposed rule will have limited applicability, although hundreds of contractors that bid on these contracts will need to familiarize themselves with the new regulations.

Additional Considerations

The FAR Council is soliciting comments on the above areas, as well as its time estimates associated with contractor compliance and collection of information. Detailed questions and time estimates from the FAR Council are included in the proposed rules.

These rules are separate from and do not implement requirements for secure software development, set forth in the Sept. 14, 2022, OMB Memorandum M-22-18, on enhancing the security of the software supply chain through secure software development practices. There is a separate open FAR case and CISA rulemaking to establish a common attestation form for this effort.[5]

Finally, it is notable that both proposed rules state that compliance with the requirements is "material to eligibility and payment under Government contracts." This appears to provide strong support for tying compliance to potential False Claims Act liability.

The proposed rules were published in the Federal Register on Oct. 3, and will be open for public comment until Dec. 4. Contractors and industry participants should submit written comments through the Federal eRulemaking portal by searching for "FAR Case 202/1-/217" or "FAR Case 202/1-/219." [6]

Townsend L. Bourne is a partner and the leader of the government business group at Sheppard Mullin Richter & Hampton LLP.

Lillia J. Damalouji is an associate at the firm.

[1] FAR Case 2021-017, https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing.

[2] FAR Case 2021-019, https://www.federalregister.gov/documents/2023/10/03/2023-21327/federal-acquisition-regulation-standardizing-cybersecurity-requirements-for-unclassified-federal.

[3] 44 U.S.C. 3502(8).

[4] 32 CFR Part 2002.

[5] No. 2023-002, Supply Chain Software Security.

[6] https://www.regulations.gov.
