Strategic Perspectives | Cybersecurity Policy Report

Two New Cybersecurity Proposed Rules Mean Big Changes For Federal Contractors

By Townsend Bourne and Lillia Damalouji of Sheppard Mullin Richter & Hampton

Listen to this post

On October 3, 2023, the FAR Council released two long-awaited proposed rules for federal contractor cybersecurity stemming from the Biden Administration's Cybersecurity Executive Order from May 2021 (Executive Order 14028). The proposed rules relate to **Cyber Threat and Incident Reporting and Information Sharing** (FAR Case 2021-017) and **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems** (FAR Case 2021-019). The comment period for both rules is currently open and is scheduled to close on December 4, 2023.

There is a lot to unpack in the proposed rules. We summarize and highlight key points below.

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

This proposed rule is meant to apply to contracts where information and communications technology (ICT) 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.

Updates to relevant terms and definitions – The proposed rule includes new definitions for "IoT devices," "Operational Technology," "Telecommunication s Equipment," "Telecommunications Services," and "Security incident" to be included in FAR 2.101. Items to note:

- **"Information and communications technology" –** This updated definition includes additional examples of ICT including telecommunications services, electronic media, IoT devices, and operational technology.
- **"Telecommunications equipment"** and **"Telecommunications services"** – These new definitions may help inform contractor compliance with FAR requirements relating to Section 889, which implement prohibitions on supply and use of covered telecommunications equipment and services. Notably absent from those FAR provisions is a definition for these terms.
- **"Security incident" –** This definition mirrors a similar provision in FISMA, but also includes as an "incident" the "transfer of classified or controlled unclassified information [CUI]" 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 CUI in non-federal systems or clear accreditation or authorization rules for such systems.

New Requirements for Federal Contractors – The proposed rule prescribes new requirements, including:

- **Software Bills of Materials (SBOM):** Federal contractors will be required to develop and maintain a Software Bill of Materials ("SBOM") for ***any*** software used in contract performance. Other "preparation and maintenance activities" include subscribing to automated indicator sharing (AIS) capability and sharing cyber threat indicators using AIS during performance.
- **IPv6 Implementation:** Federal contractors will be required to complete Internet Protocol version 6 (IPv6) implementation activities in accordance with OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6* (November 19, 2020).
- **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.
- **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 ("FBI") and the contracting agency with full access to applicable contractor information, information systems, and personnel.

- **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. The proposed rule seeks specific feedback on barriers for companies that operate outside the United States.
- **Security Incident Reporting Harmonization:** Federal contractors will be required to report security incidents through the CISA incident reporting portal ***within eight (8) hours*** of discovery and to provide updates every 72 hours thereafter until the incident is eradicated or remediated.

New contract clauses – The proposed rule includes new additions to FAR Part 39, Acquisition of Information Technology, as well as two new FAR clauses to be included in solicitations and contracts (final numbering to be determined):

- **FAR 52.239-ZZ, *Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology*** – includes requirements as discussed above relating to (1) security incident investigation, response, and reporting; (2) SBOMs; (3) sharing cyber threat indicators and defensive measures; and (4) IPv6. The clause is a required flow-down in all subcontracts where ICT is used or provided.
- **FAR 52.239-AA, *Security Incident Reporting Representation* –** will require 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 (i) notify the company within 8 hours of discovery of a security incident and (ii) flow down requirements for reporting security incidents.

The new FAR provisions are to be included in ***all*** solicitations and contracts. There is no exception for contracts below the simplified acquisition threshold, for commercial products and services, or for commercially available off-the-shelf (COTS) products. Note, however, the rule is only meant to impact contracts where ICT 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 "75 percent of all entities are awarded contracts that include some ICT."

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

This proposed rule provides standardized requirements for contractors that develop, implement, operate, or maintain a Federal Information System ("FIS"). It provides a new definition for FIS 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." This proposed rule includes the following changes to the FAR.

Updates to Relevant Definitions – The proposed rule includes several new definitions, the most notable being the definition for Federal Information System:

- **"Federal Information System"** (FIS) –

  (1) Means an information system (44 U.S.C. 3502(8)) used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency;
  (2) *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 (32 CFR part 2002).

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." This is likely to be an area of focus for public comments.

New Requirements for Federal Information System (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, FIS services. These requirements include:

- **For Federal Information Systems using *non-cloud computing services:***
  - Agencies must (1) use FIPS 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.
  - 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 (this includes 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, and comply with continuous monitoring and supply chain risk management requirements.

- **For Federal Information Systems using *cloud computing services*** agencies will require Federal Risk and Authorization Management Program (FedRAMP) 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.

  – For systems designated as "high," all Government data must be maintained within the United States 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 "Federal Information Systems" and two new FAR clauses to be included in solicitations and contracts as prescribed in FAR 39.X04 (final numbering to be determined)

- **FAR Clause 52.239-YY, *Federal Information Systems Using Non-Cloud Computing Services*** – 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 a FIS using other than cloud computing services.
- **FAR Clause 52.239-XX, *Federal Information Systems Using Cloud Computing Services*** – 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 a FIS using cloud computing services.

Both 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.

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 COTS procurements, it is limited 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 (both non-cloud FIS contractors and cloud FIS contractors), 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 as set forth in OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022). There is a separate open FAR case (No. 2023-002) and CISA rulemaking to establish a common attestation form for this effort.

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 to tie compliance to potential False Claims Act liability.

These proposed rules were published in the Federal Register on October 3, 2023 and will be open for public comment for a period of 60 days, until December 4, 2023. Contractors and industry should submit written comments through the Federal eRulemaking portal at *https://www.regulations.gov* by searching for "FAR Case 2021-017" or "FAR Case 2021-019."

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Ms. Townsend Bourne
Sheppard Mullin Richter & Hampton
1300 I Street NW
11th Floor East
Washington, DC
UNITED STATES
Fax: 2136201398
E-mail: mbennett@sheppardmullin.com
URL: www.sheppardmullin.com

(c) Mondaq Ltd, 2023 - Tel. +44 (0)20 8544 8300 - http://www.mondaq.com