THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

OCTOBER 18, 2023 | VOLUME 65 | ISSUE 38

¶ 280 FEATURE COMMENT: Cyber Security Slasher: What's Lurking In FAR Case 2021-017, Cyber Threat And Incident Reporting And Information Sharing Proposed Rule

Alexander Major[*]

Cue the eerie music. It may be Halloween season, but there are no tricks or treats here. It's a quiet night, perhaps on a barren street, or at a placid lake, or at an abandoned amusement park, and there's tension in the air. Reports of sightings. Long-heard rumors of escapes. There's a menace looming. Floorboards are creaking. [Fire]doors are slamming. Is that a shimmer of a sharpened knife hiding in the *Federal Register*? Red, glowing regulatory eyes peering out from under previously innocuous Federal Acquisition Regulation Clauses? Is it Michael? Jason? Freddie? Cozy Bear? … is cyber risk calling … ***from inside the house?!***

In a flurry of brutal activity, on Oct. 3, 2023 the Federal Acquisition Regulatory Council issued ***two*** proposed rules intended to partially implement President Biden's Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," and the Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (P.L. 116–207). Both are robust, and thus treated separately by this blog (as to will a critique of the proposed rules). The first Proposed Rule, FAR Case 2021-017, and discussed in detail below, will impact all federal contractors in innumerable ways by imposing ardent and expressly material cybersecurity incident reporting requirements. The second, FAR Case 2021-019, will have an equally significant impact but on a smaller swath of federal contractors. It is focused on those who develop, implement, operate, or maintain an on-premises or cloud-based information system "used or operated by an agency, by a contractor of an agency, or by another organization, on behalf of an agency," (now identified as a "Federal Information System"). The comment period for both of these proposed rules closes on Dec. 4, 2023, and it would be well-worth contractors' time to examine the looming risk in the proposed rules so you not only can sleep tight … but so that you can make it through the night.

The False Claims Act Specter—Before we stab deeper into the Proposed Rule, it is worth noting that its preamble uses a phrase that should send chills down the spine of every contractor and emphasizes the gravity of the Government's concerns: "This proposed rule underscores that the compliance with information-sharing and

[*] *This Feature Comment was written for* THE GOVERNMENT CONTRACTOR *by* Alexander Major. *Mr. Major is a partner and co-leader of the Government Contracts & Global Trade Practice Group at McCarter & English, LLP.*

incident-reporting requirements are material to eligibility and payment under Government contracts." Eeek! As the Navy did just a few short years ago in Navy Marine Corps Acquisition Regulations Supplement subpt. 5204.7303, the FAR Council is emphasizing that the provisions related to incident-reporting and information-sharing are "material" to contract payment. This is critical for understanding the underlying risk posed by these clauses and the ease by which non-compliance may lead to FCA risk. In order to successfully bring an FCA claim under 18 USCA § 3729(a)(1)(A), the Government or a qui tam relator must establish the following elements:

1. A false claim has been submitted;
2. The false claim was made with the requisite scienter (or knowledge that it was false);
3. The false claim caused the Government to pay money; and
4. The false claim is material to payment.

As the Proposed Rule preamble makes clear, materiality is stated up front and is no longer able to play the "final girl" role in your FCA-defense slasher story. Materiality is presumed, right up front. (For those unfamiliar, "final girl" is a horror movie trope referring to the surviving female protagonist positioned to outwit and confront the killer at the end of the movie. See Carol J. Clover, Men, Women, and Chain Saws: Gender in the Modern Horror Film (1992)).

The Cabin, in the Woods, by the Lake—"Information and Communications Technology"—It should come as no surprise that the Federal Government is keen to ensure that certain data and material provided to its contractors need to remain secure. However, as industry is becoming increasingly aware, due to the nature of electronic commerce and technology, cyber incidents, such as breach, email compromise, ransomware, etc., will happen. And while the Proposed Rule for FAR Case 2021-017 doesn't provide discrete requirements contractors must meet to secure or safeguard their information systems holding sensitive federal data (i.e. as in Defense FAR Supplement 252.204-7012), the Proposed Rule does attempt to address past security gaps (such as with operational technology, or "OT"), the adoption of new technology (such as internet protocol version 6, "IPv6," Software Bills of Materials, and the Internet of Things, "IoT") while harmonizing and clarifying cyber threat and incident information sharing requirements between industry and the Government should/when that eventuality does occur and something goes sideways.

The key to FAR Case 2021-017 is understanding the newly defined term "information and communications technology," or "ICT." It is an extremely broad definition intended to refer to:

> 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.

Recognizing whether a contract addresses ICT is paramount to understanding the impact on contractor systems, procedures, and contractual requirements. FAR Case 2021-17 appears to be focused on ICT providers and, presumably, would apply security incident reporting requirements only to contractors (i) awarded contracts that include ICT and who (ii) experience a reportable security incident. However, it is worth noting that the present iteration of the Proposed Rule, at proposed FAR provision 39.108, would have the incident and threat reporting and incident response requirements resident in "all solicitations and contracts," not just contracts for ICT. Barring a change in the final rule, this could mean significant impact/risk/confusion for contractors who may not be 100 percent clear on whether they provide ICT per their contract or know 100 percent that they do not.

Torture Chamber—The Definition of "Security Incident"—While ICT is broad (and getting broader), a more challenging aspect for federal contractors may

be addressing and responding to the Proposed Rule's definition of "security incident":

> (1) Any event or series of events, which pose(s) actual or imminent jeopardy, without lawful authority, to the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;
>
> (2) Any malicious computer software discovered on an information system; or
>
> (3) Transfer of classified or controlled unclassified information onto an information system not accredited (*i.e*., authorized) for the appropriate security level.

There is a LOT to unpack in this incredibly broad definition. Contractors would be wise to understand all of the implications, but most notably the fact that security incidents can occur not only when you operate counter to law and regulation, but also if you fail to meet the company's own policies and procedures.

The Proposed Rule, of course, also adds additional contractual and subcontract flowdown clauses that will require offerors to represent that they have submitted all security incident reports in a current, accurate and complete manner; and represent whether they have properly flowed down requirements (FAR 52.239-AA) and establishes new definitions and coverage for: requests for security incident reporting; supporting incident response; cyber threat indicators and defensive measures reporting; and IPv6 (FAR 52.239-ZZ). Both clauses are explored in greater detail below.

The Jump Scare of New Technology—It's dark as pitch. Breathing is all that's heard. Is there something out there? Who could it be? What could it **…** ***IoT***!

It's worth remembering that EO 14028 was issued in the wake of significant cyber incidents involving SolarWinds and the Colonial Pipeline. Accordingly, the EO took it upon itself to discuss the terrors of software supply chain compromise, the vulnerability of OT, and the menaces posed by the internet of things (which, in and of itself, has a bit of a creepy name), before providing executive agencies with what appeared to be a strict timeline to address these very real concerns. While few agencies, with the exception of the National Institute of Standards and Technology, appeared to have taken those deadlines to heart (all efforts were to be complete by May 12, 2022; ***spoilers*** They weren't), the Proposed Rule attempts to course correct by addressing some of these issues in catch-all fashion.

Internet of Things: The Proposed Rule addresses IoT by first defining it as technology that may:

1. Have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional information technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and

2. Can function on their own and are not only able to function when acting as a component of another device, such as a processor.

That defined IoT is now included as ICT, the breach of which will be addressed in the same manner as other IT technology. By contrast, the manner by which IoT can be procured by the Federal Government, as directed by The IoT Cybersecurity Improvement Act of 2020, is properly laid out in the Proposed Rule for FAR Case 2021-019.

Internet Protocol version 6 (IPv6): Adjacent to IoT issues is the next-generation internet protocol (IP) requirements, version six, or IPv6, which, as the next generation of Internet protocol, is needed to address the exponential demand for IP addresses. The purpose of these provisions is to assist in the transition of all federal information systems and services to IPv6 by 2025, as mandated in the Office of Management and Budget, Nov. 19, 2020 memorandum, M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)." For those unfamiliar with IPv6, it relates generally to the upgrade of agency servers and web and email services and intended to enhance trusted internet connectivity by providing better support for end-to-end encryption.

Operational Technology: Like IoT, Operational Technology, or "OT," is defined in the Proposed Rule and brought under the protective umbrella of ICT. In

line with NIST SP 800-160 vol 2, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, OT means:

> Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples of operational technology include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

While acquisition and management of OT systems are addressed in the Proposed Rule for FAR Case 2021-019, cyber incidents related to OT would be reportable under this Proposed Rule.

Software Bills of Materials (SBOM): Following the SolarWinds security incident EO 14028 took direct focus on the need to address the software supply chain. An SBOM, as simply defined in the Proposed Rule, is "a formal record containing the details and supply chain relationships of various components used in building software."

The Proposed Rule would require contractors to develop and maintain an SBOM "for any software used in the performance of the contract regardless of whether there is any security incident." Access to that SBOM is to be provided to the contracting officer upon initial use and then again upon any "new build or major release" in a manner commensurate with the then-current version of § IV of the Department of Commerce's *The Minimum Elements for a Software Bill of Materials*. As the presence and presentation of an SBOM is a fundamentally new task for COs and contractors alike, the FAR Council is seeking specific comments from contractors on:

- How should SBOMs be collected from contractors? What specific protections are necessary for the information contained within an SBOM?
- How should the Government think about the appropriate scope of the requirement on contractors to provide SBOMs to ensure appropriate security?
- What challenges will contractors face in the development of SBOMs? What challenges are unique to software resellers? What challenges exist regarding legacy software?
- What are the appropriate means of evaluating when an SBOM must be updated based on changes in a new build or major release?
- What is the appropriate balance between the Government and the contractor, when monitoring SBOMs for embedded software vulnerabilities as they are discovered?

Out from Behind the Mask—New Roles for the FBI and CISA—A significant factor to the Proposed Rule is the enhanced role played by both the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation. Specifically, the Proposed Rule opens the door to direct/encourage contractors to cooperate with CISA by allowing the agency access, when needed for threat hunting and incident response, in order to give CISA "visibility into systems to observe adversary activity." While such actions that would be taken by CISA are "expected … [to] only be taken after consultation between the contractor and the contracting agency," it remains to be seen how or if that "consultation" takes form.

Similarly, in response to a security incident, the Proposed Rule would require contractors to provide timely and "full access" to applicable contractor information, information systems, and personnel to CISA, the FBI, and the impacted contracting agency. This could expressly include submitting malicious code samples or artifacts to CISA and providing access to additional information or equipment necessary for forensic analysis. Hereto, the FAR Council is seeking input as to the impact these access and production directives would have on contractors by welcoming input on the following questions:

- Do you have any specific concerns with providing CISA, the FBI, or the contracting agency full access (see definition at 52.239–ZZ(a)) information, equipment, and to contractor personnel? Please provide specific details regarding any concerns associated with providing such access.

- For any specific concerns identified, are there any specific safeguards, including safeguards that would address the scope of full access or how full access would be provided or that would address your concerns while still providing the Government with appropriate access to conduct necessary forensic analysis regarding security incidents?

- Are there any specific safeguards that should be considered to ensure that protections for privacy and civil liberties are effectively accomplished?

It Came from … Overseas—Addressing Global Contractors and Supply Chains—An inescapable reality of federal contracting today is the presence and need for foreign contractors and supply chains. Case in point is the Aug. 18, 2023, Department of Defense report identifying that $15.1 billion, or roughly 3.7 percent, of the total fiscal year 2022 DOD obligations were expended on purchases from foreign entities. A crucial symptom of this, as the Proposed Rule appears to recognize, is that such foreign companies undoubtedly have their own laws and regulations on how that company, as a corporate citizen of a particular country, must approach/deal with a security incident. Beyond the question over access to the specific content of the data, systems and personnel of that foreign entity contemplated by FAR Case 2021-017, there will be inevitable domestic notification provisions that may prove paramount to U.S. Government laws and the terms of the contract. Moreover, as mandatory flowdowns plunge deeper into the subcontract chain, additional challenges and, perhaps, waivers, may be required to access sources not sufficiently available or economical to obtain from U.S. domestic sources.

Recognizing and addressing these issues, the FAR Council is seeking input to the following questions:

- Are there any specific situations you anticipate where your organization would be prevented from complying with the incident reporting or incident response requirements of FAR 52.239–ZZ due to country laws and regulations imposed by a foreign government? If so, provide specific examples that identify which requirements would be impacted and the reason that compliance would be prevented by the laws of a foreign government or operating environment within a foreign country.

- Do you anticipate situations where compliance with requirements in FAR 52.239–ZZ or alternative compliance methods (if added) would be prevented due to country laws and regulations imposed by a foreign government. If so, provide specific examples of when you expect such situations to occur, citing the authoritative source from the foreign government.

Knife, Axe or Chainsaw—The Proposed Clauses—Although not nearly as sharp or as loud as many slashers' tools of the trade, the clauses introduced by the Proposed Rule can be equally perilous to a contractor if not approached with caution. Some of that risk is found in the fact that the Proposed Rule would require the new incident reporting clause at FAR 52.239-ZZ to be included in all FAR-based contracts involving ICT, including contracts and solicitations for items below the simplified acquisition threshold and those for commercially available off-the-shelf items—segments expressly excluded under the DFARS clause.

There's no running away from these clauses, so let's see what they've got:

FAR 52.239-AA, Security Incident Reporting Representation: This straightforward clause requires an offering contractor to represent two distinct issues:

1. That it has submitted all security incident reports in a current, accurate and complete manner; and

2. That it has required each lower-tier subcontractor to include the "substance" of FAR clause 52.239–ZZ in their respective subcontracts.

If finalized, the Proposed Clause at FAR 52.239-AA would not only require contractors to address existing cybersecurity policies and procedures, including incident response plans, but also subcontracting playbooks and policies to ensure that the required certification can be properly provided and documented.

FAR 52.239-ZZ, Incident and Threat Reporting and

Incident Response Requirements for Products or Services Containing Information and Communications Technology:

You made it! After all of this, it's time to confront the "big bad," the monster under the bed/in the closet/banging around in the basement—the actual reporting requirements with which contractors will be expected to comply if the Proposed Rule goes final. Notably, the proposed changes to the implementing clause at FAR 39.108(b) do not limit the type of contract into which this clause is to be inserted. Instead, it states the CO "shall insert the clause at 52.239-ZZ … in all solicitations and contracts." Meaning, as presently drafted, it would be applicable and included in contracts when ICT is expressly not expected or contemplated to be present.

As the definitions in this Proposed Clause are legion, it's best to not limit your expectations; think broadly (because the Government surely did!) when addressing these requirements after a cyber security incident (defined above) occurs. Under the Proposed Rule, in summary fashion, a security incident will trigger a contractor requirement to:

1. Immediately and thoroughly investigate all security incident indicators that may have occurred and use the CISA Incident Reporting System to submit a CISA Incident Reporting Form on all security incidents involving a product or service provided to the Government that includes information and communications technology, or the information system used in developing or providing the product or service, within eight hours;

2. Notify the CO of any agency which placed an affected order under the contract, that an incident reporting portal has been submitted to CISA, within eight hours;

3. Update the CISA and CO submission every 72 hours thereafter until the contractor, the agency, and/or any investigating agencies have completed all eradication or remediation activities, exclusive of security incidents (i.e. controlled unclassified information/classified breaches) where additional, separate reporting may be required;

4. Use sound judgment as to using potentially compromised communications or messaging platforms to provide notification(s) or otherwise communicate information about the security incident and associated response activities and employ contractually described validating procedures before responding to any CISA or FBI access or information requests;

5. Collect and properly preserve as directed in the clause, for at least 18 months, available images, monitoring/packet capture data, and information relevant to security incident prevention, detection, response and investigation within information systems used in developing or providing ICT products or services to the Government and be prepared, upon request by the CO, to promptly provide this data and information to the Government;

6. Promptly provide to the Government, and any independent third party specifically authorized by the Government, all information identified above to conduct an incident or damage assessment regarding a security incident;

7. Upon discovering and isolating malicious computer software in connection with a security incident, submit malicious code samples or artifacts to CISA using the appropriate form within eight hours of that discovery and isolation;

8. Respond to any contracting agency, CISA, and/or FBI requests for system or personnel access or additional requested information related to the security incident within 96 hours and notify the CO of the same;

9. Subscribe to the CISA Automated Indicator Sharing (AIS) capability or successor technology during the performance of the contract and share cyber threat indicators and recommended defensive measures when such indicators or measures are observed on information and com-

munications technology used in performance of the contract or provided to the Government, in an automated fashion using this medium during the performance of the contract; and

10. Participate in an information sharing and analysis organization or information sharing and analysis center with the capability to share indicators with AIS or successor technology and that further shares cyber threat indicators and recommended defensive measures submitted to it with AIS, during the performance of the contract.

In addition to new requirements for managing and reporting security incidents, the clause at FAR 52.239-ZZ also directs unique data retention requirements, such as the requirement to:

1. Develop, store, and maintain throughout the life of the contract and at least one year thereafter an up-to-date collection of "customizations" (an undefined term in the Proposed Rule) that differ from manufacturer defaults on devices, computer software, applications, and services;

2. Be prepared, at the request of the CO, to provide the cognizant program office/requiring activity, CISA and/or the FBI, with a copy of the current and historical customization files, and advise the CO that such information has been shared and with whom it has been shared; and

3. Maintain, and upon the initial use (and/or later update with a new build or major release) of such software in the performance of the contract, or provide access to the CO a current or updated SBOM for each piece of computer software used in performance of the contract in an industry-standard format that complies with Department of Commerce requirements.

Don't Scream … They'll Hear You—Suffice it to say that the significant changes promised by this one FAR Case contains a lot of "scary." But there's a reason why people turn the lights on when they're scared. Fear is a product of the unknown. While the Proposed Rule behind FAR Case 2021-017 is daunting, any concern can be combatted by showing it the light of day—reviewing it, taking it in, applying it against present cybersecurity policies and incident response plans and, hopefully, seeing those areas where the new requirements gel with existing practices. This Halloween, keep the horror confined to the screen-bound maniacs, not the cyber-security boogeymen and regulators.