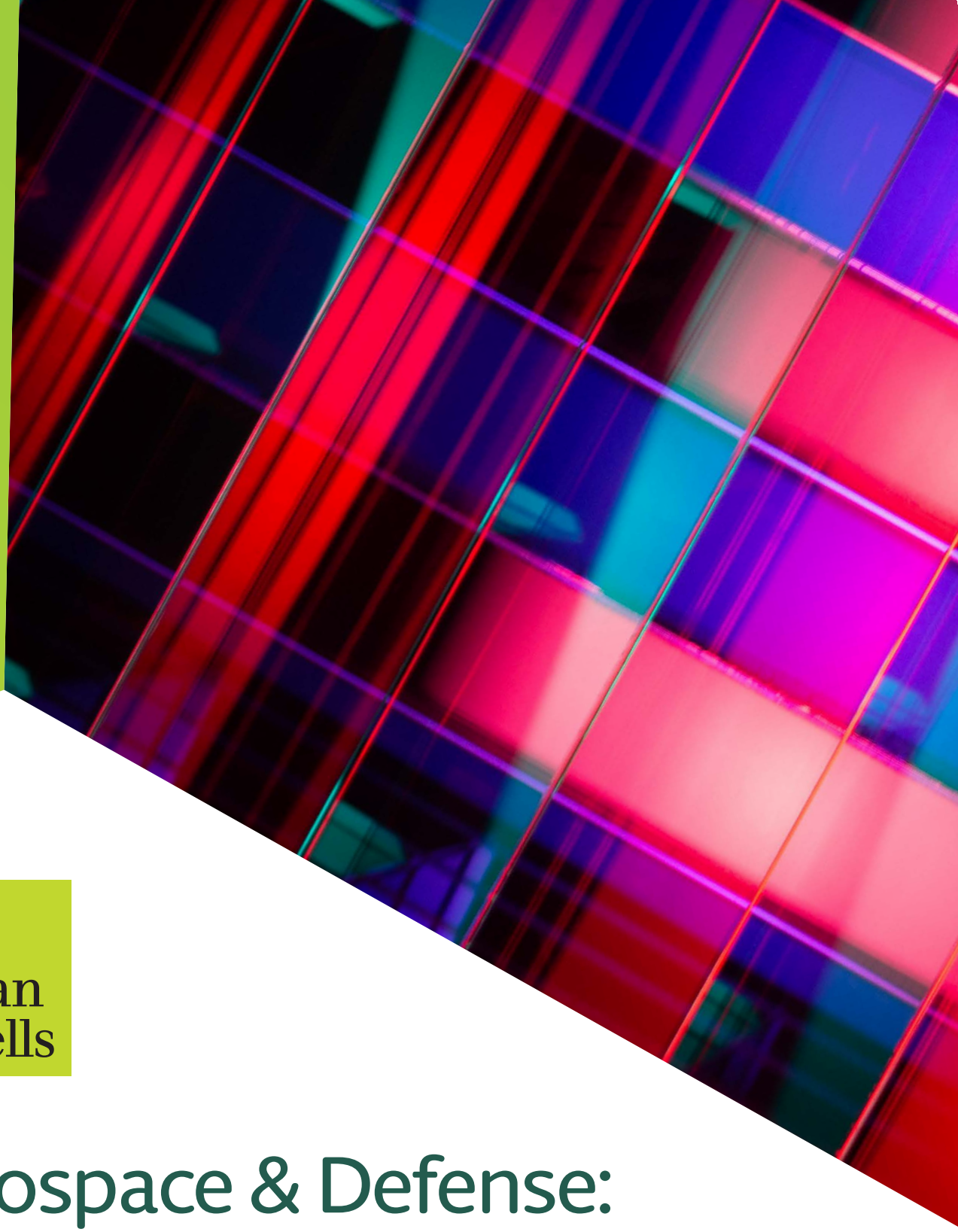


Hogan Lovells

Aerospace & Defense:

Proposed FAR Rules Implement Cybersecurity Standardization and Incident Reporting Requirements for Government Contractors

Stacy Hadeka, Mike Scheimer, and Mike Mason

Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

Proposed FAR Rules Implement Cybersecurity Standardization and Incident Reporting Requirements for Government Contractors

This publication presents Part 2 of our A&D Insights series covering the two recently proposed Federal Acquisition Regulation (FAR) Council rules addressing (1) **the standardization of cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems** (FAR Case 2021-019), and (2) **cyber threats and incident reporting and information sharing requirements for government contractors** FAR Case 2021-017). In Part 1 of our series, we addressed the proposed standardization of cybersecurity contractual requirements (addressed **here**). This Part 2 focuses on the proposed rule to impose new requirements concerning cyber threat and incident reporting and information sharing. As discussed in more detail below, the rule will impact a significant number of government contractors and impose more expansive requirements than what we have seen in the acquisition regulations to date.

Part 2: Cyber Threat and Incident Reporting and Information Sharing

The FAR Council published a proposed rule requiring government contractors to share information about cyber threats and report cyber incidents. *See* **88 Fed. Reg. 68,402 (Oct. 3, 2023)**.[1] The proposed rule expressly states that compliance with these information-sharing and incident-reporting requirements are material to eligibility and payment under Government contracts. Citing to the SolarWinds, Microsoft Exchange, and the Colonial Pipeline cyber incidents, the rule also underscores the need to modernize cybersecurity defenses by protecting federal networks, improving information sharing between the U.S. Government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. The rule proposes to achieve these goals through changes to the FAR, including:

- Changes to FAR Part 2.101 and FAR Part 39 to update and add relevant definitions.[2]
- Addition of a new section at FAR 39.107, "Response to incident reports and requests for information or access."
- Addition of ***two*** new FAR clauses for use in solicitations and contracts below the simplified acquisition threshold, and for commercial products, including commercially-available off-the-shelf (COTS) items, and for commercial services:
    1. FAR 52.239-AA, *Security Incident Reporting Representation*; and
    2. FAR 52.239-ZZ, *Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology*.
- Addition of FAR 52.239-AA to FAR 52.239-1, *Privacy or Security Safeguards*.
- Addition of FAR 52.239-ZZ to (i) 52.212-3, *Offeror Representations and Certifications— Commercial Products and Commercial Services; (ii) 52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders— Commercial Products and Commercial Services; and (iii) 52.213-4, Terms and Conditions— Simplified Acquisitions (Other Than Commercial Products and Commercial Services)*.

These updates will impact the majority of government contractors, including COTS contractors. This is a significant change from the DoD's Defense FAR Supplement (DFARS) 252.204 7012, which includes a COTS exception. Indeed, the FAR Council estimates that at least 75 percent of all organizations awarded contracts will be subject to the rule. This proposed rule would also flow down to subcontracts where information and communications technology (ICT) is used or provided in the performance of the subcontract, including subcontracts for the acquisition of commercial products or services. As drafted, this rule would have a far greater impact than DoD's requirements already in effect given the rule's broad applicability and its coverage extending beyond incident reporting to also reach threat sharing.

1 This rule is separate and apart from the still pending CUI FAR rule (Open FAR Case No. 2017-16) to implement regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of Controlled Unclassified Information (CUI) and to implement OMB Memorandum M-17-12 guidance on Personally Identifiable Information (PII) breaches

2 This includes (i) updating the definition in FAR 2.101 to information and communications technology (ICT) to provide additional examples not primarily aimed at Section 508: telecommunications services, electronic media, Internet of Things (IoT) devices, and operational technology, and (ii) proposed new definitions to be added for IoT devices (derived from Section 2 of Pub. L. 116-207), operational technology (derived from NIST SP 800-160 vol. 2), telecommunications equipment (derived from DFARS subpart 239.74), and telecommunications services (derived from DFARS subpart 239.74)

I. Background

The proposed FAR rule adds to the already existing universe of cyber incident reporting obligations impacting government contractors:

- DoD's DFARS 252.204 7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, requiring reporting of cybersecurity incidents impacting DoD CUI within 72 hours of discovery to the DoD Cyber Crime Center (DC3) through the DIBNet.
- DHS's new Homeland Security Acquisition Regulation (HSAR) clause 3052.204-72, *Safeguarding of Controlled Unclassified Information*, requiring contractors to report any cybersecurity incident that could affect CUI within eight hours (or one hour if it involves personally identifiable information) to the DHS Component Security Operations Center (SOC).
- The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (not yet finalized through regulation), requiring a covered entity that experiences a covered cyber incident shall report the covered cyber incident to CISA not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.
- The National Industrial Security Program Operating Manual (NISPOM) (32 C.F.R. Part 117), requiring contractors with security clearances to "promptly" report cyber incidents involving classified information.
- The new SEC rule (17 C.F.R § 229.106; Form 8-K Item 1.05), requiring public companies to report a cybersecurity incident on Form 8-K within four business days after the company determines the incident is material.

Government contractors that offer products and services to the federal Government may be subject to these and other incident reporting requirements, including state, local, and foreign government reporting requirements. The new FAR cyber threat sharing and incident reporting rule will layer on another reporting obligation for contractors.

II. FAR 52.239-ZZ, *Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology*

This newly proposed clause at FAR 52.239-ZZ implements cybersecurity incident and threat reporting and incident response requirements. As mentioned above, the clause would apply to all types of contracts, including contracts for commercial products, including COTS items, and for commercial services.

FAR 52.239-ZZ includes requirements addressing the following topics:

1. Security Incident Reporting - Paragraph (b)

Clause: The proposed rule would require contractors that experience a reportable security incident (i) involving a product or service provided to the Government that includes ICT, or (ii) the information system used in developing or providing the product or service to report security incidents that may have occurred within 8 hours of discovery to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at https:// www.cisa.gov/report and to affected agencies (e.g., the Contracting Officer), to include providing any updates every 72 hours thereafter until eradication or remediation activities are completed.

Once reported, the proposed FAR clause notes that CISA will share the information with (i) any contracting agency potentially affected by the incident or by a vulnerability revealed by the incident, and (ii) other executive agencies responsible for investigating or remediating cyber incidents, such as the Federal Bureau of Investigation (FBI), and other elements of the intelligence community.

Takeaway: The scope of the proposed reporting requirement in FAR 52.239-ZZ is quite broad. The incident reporting threshold as drafted in Section (b)(1) requires reporting "on all security incidents involving a product or service provided to the Government that includes [ICT], or the information system used in developing or providing the product or service." The expansive scope of this requirement could lead to varying interpretations amongst contractors, resulting in inconsistent and possibly the over-reporting of incidents.

The proposed rule's definition of a "security incident" is also broad, meaning an actual or potential occurrence of (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 CUI onto an information system not accredited (*i.e.*, authorized) for the appropriate security level. This new and expansive definition will likely lead to questions as what must be reported—*e.g.*, a mere vulnerability or policy violation—and how often. The FAR council chose not to use definitions of incidents already seen in the procurement space, such as "cyber incident" in DFARS 252.204-7012 and "incident" in HSAR 3052.204-72. These differing definitions and thresholds could create difficulties amongst contractors, complicating even further the reporting regimes they already find themselves subject to.

Regarding the definition of "information system," the proposed rule defines the term as a discrete set of information resources (including ICT) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)), which mirrors the definition in the DFARS[3]. However, the clause does not differentiate between a federal information system or contractor information system and whether the information system should have a direct tie to the contract containing the FAR clause[4]. As drafted, the definition could encompass any information system located anywhere.

In adding to the patchwork of incident reporting requirements across the federal Government, the 8 hour reporting timeline differs than those reporting requirements that contractors may already find themselves subject to[5]—the 72 hour reporting requirement in the DFARS[6] or CIRCIA;[7] 1 hour reporting requirement in the HSAR;[8] and 4-day reporting requirement for SEC.[9] Moreover, unlike the other reporting requirements, this rule would require continual information sharing obligations every 72 hours until eradicated or remediated. Many of these differences were addressed in a recent DHS report on "**Harmonization of Cyber Incident Reporting to the Federal Government**," stressing the need to address duplicative reporting. Introduction by the FAR Council of a divergent timeline of 8 hours for reporting cyber incidents could present significant challenges to contractors and for the harmonization of reporting requirements.

3 *See* DFARS 252.204-7012

4 In addition to defining "information system," DFARS 252.204-7012 uses "covered contractor information system" to delineate the type of system subject to the cybersecurity safeguarding and incident reporting requirements

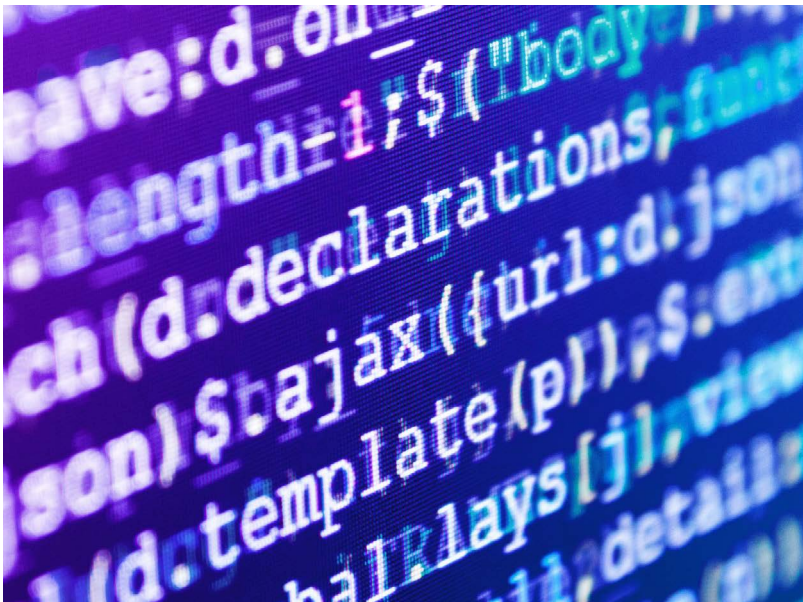
5 *See* proposed FAR clause 52.239-ZZ(b)(3) ("Security incidents involving specific types of information (e.g., controlled unclassified information, classified information) may require additional reporting that is separate from the requirements of this clause"))

6 DFARS 252.204-7012(c)

7 6 U.S.C. § 681b(a)(1)(A)

8 HSAR 3052.204-72(c)(2)

9 17 C.F.R § 229.106; Form 8-K Item 1.05



FAR Council Questions for Industry:

- *Timeline for reporting:* Are there specific situations you anticipate where your organization will be required to report on different timelines in order to comply with the incident reporting requirements outlined in 52.239-ZZ, other Federal contract requirements, or other regulations promulgated under Federal law? How would your organization handle disparate cyber incident reporting timelines in other Federal Government contracting requirements or from other regulatory agencies?
- *Potential effect on incident response*: Incident response and associated reporting are often iterative processes, with system owners updating reports as a situation evolves and more data becomes available. What implications are there for your organization, including with respect to incident response, to meet disparate timelines for incident reporting?
- *Cost of providing ICT products and services*: How much, if at all, would you estimate that the initial reporting requirement described in this proposed rule could increase the price of the products or services your organization provides to the Federal Government?
- *Scope of the contract clause*: The proposed rule would require the new incident reporting clause to be included in all contracts involving ICT that are subject to the FAR, including those for commercially available off-the-shelf (COTS) items. This is broader in scope than, for instance, the DFARS clause. How would differences in scope between reporting requirements affect your organization's implementation of this clause?
- *Definition of incident*: The definition of "security incident" in the proposed rule incorporates the substantive provisions of the definition in 44 U.S.C. 3552, which has minor differences from with the definition of "incident" in Section 2209 of the Homeland Security Act of 2002 (as amended) and from the modified definition of "covered incident" used in CIRCIA, which is currently the subject of a separate rulemaking process, see 6 U.S.C. 681b(b). What, if any, additional implementation issues would your entity face complying with different definitions of an incident? How would your entity make the distinction between "imminent jeopardy" and "actual jeopardy," and what effect could that have on the number of reported incidents that did not end up actually affecting confidentiality, integrity, and availability of information or an information system?
- *Operating in a Foreign Country:*
  - 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.

2. Supporting Incident Response - Paragraph (c)

Paragraph (c) of the proposed rule would require contractors to support cyber incident reporting through the following means:

i. Data Preservation and Protection - (c)(1)

Clause: The rule would require contractors to collect and preserve for at least 12 months in active storage followed by 6 months in active or cold storage, available 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. This data includes, but is not limited to, network traffic data, full network flow, full packet capture, perimeter defense logs (firewall, intrusion detection systems, intrusion prevention systems), telemetry, and system logs including, but not limited to, system event logs, authentication logs, and audit logs. Upon request by its Contracting Officer, a contractor would also be required to promptly provide this data and information to the Government.

Moreover, contractors would be required to immediately preserve and protect images of all known affected information systems and all available monitoring/packet capture data if an incident were to occur or if requested by the government. The images and data must be retained for the longer of (a) 180 days from the submission of the report or receipt of the request; (b) for a period from 12 to 18 months; or (c) if instructed to retain such images and data beyond 180 days by the Contracting Officer, until the contractor is notified by the Contracting Officer that retention is no longer required.

Takeaway: Paragraph (c)(1) of the clause would impose either a 180 day, 12 month, or 18 month data preservation and protection timeline. This differs from DFARS 252.204-7012(e), which requires contractors to preserve and protect only images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report. The FAR Council has lengthened this preservation and protection timeline and added additional data and information that contractors would be required to preserve.

ii. Customization Files - (c)(2)

Clause: As proposed, this paragraph would require a contractor to develop, store, and maintain throughout the life of the contract and for at least 1 year thereafter an up-to-date collection of customizations that differ from manufacturer defaults on devices, computer software, applications, and services, which includes but is not limited to configuration files, logic files and settings on web and cloud applications for all information systems used in developing or providing an ICT product or service to the Government. The contractor would also be required to provide the cognizant program office/requiring activity, CISA and/or the FBI if requested by the contracting officer, with a copy of the current and historical customization files, and notice to the contracting officer that such information has been shared and with whom it has been shared.

Takeaway: This would serve as a new contractual requirement, directing contractors to develop customization files so that the Government could plausibly understand what changes a contractor would have made to impacted software or hardware when sold. The rule does not prescribe the format for such customization file and could be viewed as quite expansive, possibly covering any information system located throughout the world and any minor change to software or hardware. Contractors may also find themselves facing pushback from lower-

tier suppliers for sharing their own proprietary customization information to be include in a prime contractor's customization file. The FAR Council estimates that developing and maintaining a customization file will take approximately 5 hours per year, but this may require more time and could add to the increased burden and cost already facing contractors as a result of this clause.

iii. Software Bill of Materials (SBOM) - (c)(3)

Clause: Paragraph (c)(3) would impose a new requirement for contractors to develop and maintain an SBOM for any software used in the performance of the contract. The proposed rule would require contractors to maintain, and upon the initial use of software in the performance of its contract, provide (or provide access to) the contracting officer a current SBOM for each piece of computer software used in performance of the contract.[10] This section of the clause requires that each SBOM be produced in a machine-readable, industry-standard format and must comply with "all of the minimum elements [(except for frequency)] identified in Section IV of The Minimum Elements for a Software Bill of Materials (the current version at the time of solicitation) published by the Department of Commerce at https://www.ntia.doc.gov/report/2021/minimum-elements-software-bill-materials-sbom."

Contractors would also be required to update the computer SBOM and provide it to the contracting officer if a piece of computer software used in the performance of the contract is updated with a new build or major release, including computer software builds to integrate an updated component or dependency.

Takeaway: According to the FAR Council, SBOMs can be "critical in incident response, as they allow for prompt identification of any sources of a known vulnerability." However, the rule does not appear to account for the other Government efforts to address SBOMs, including under Section 4 of the Biden Cyber EO. Pursuant to the EO, The Department of Commerce and NTIA jointly published **minimum elements for a SBOM** on July 12, 2021, and the Office of Management and Budget's (OMB) followed with a Memorandum on "**Enhancing the Security of the Software Supply Chain through Secure Software Development Practices**" in September 2022, addressing agency's ability to include SBOMs in their solicitation requirements and the prescribed SBOM formats.[11] These efforts have coincided with the Government's software attestation efforts, including the open FAR Case No. 2023-002 for Supply Chain Software Security, requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements.

If required to develop and maintain an SBOM as a result of this clause, contractors will want to ensure that the requirement is adequately considered in the pricing of the contract.[12]

FAR Council Questions for Industry:

- 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?

iv. Incident and Damage Assessment Activities - (c)(4)

Clause: Paragraph (c)(4) of the clause indicates that if the Government elects to conduct an incident or damage assessment regarding a security incident, and that the contractor must promptly

10 If an SBOM has been provided to the contracting officer at the basic contract level, the SBOM does not need to be provided to the contracting officer for each order

11 *See also* CISA's SBOM resources at https://www.cisa.gov/sbom

12 The FAR Council estimates it will take 80 hours for a contractor to develop and maintain an SBOM

provide preserved security incident data ((c)(1)), customization files ((c)(2)), and SBOMs ((c)(3)).

Takeaway: This proposed requirement would allow the Government and any 3rd party authorized assessor access to all incident and damage assessment information if the Government elected to conduct such assessment. Contractors will want to ensure they properly mark information provided to the Government, including the customization files and SBOMs, as proprietary and confidential trade secrets to protect from release under the Freedom of Information Act (FOIA).

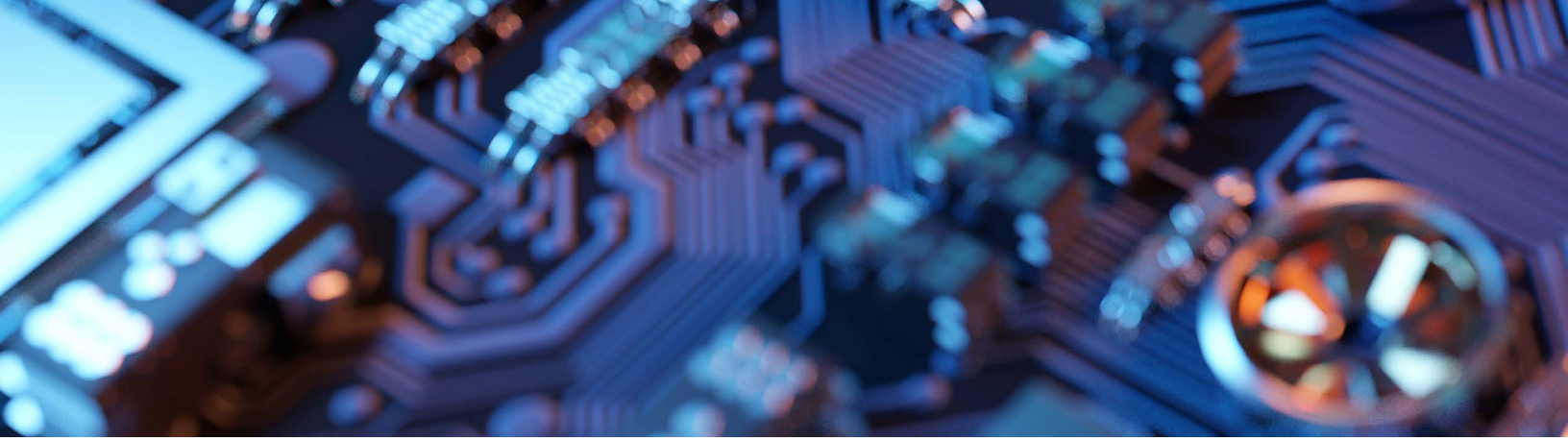
v. Malicious Computer Software - (c)(5)

Clause: Paragraph (c)(5) would require a contractor to submit malicious code samples or artifacts if it discovers and isolates malicious computer software in connection with a security incident to CISA using the form at https://www.malware.us-cert.gov within 8 hours of discovery and isolation of the malicious computer software, in addition to the required incident reporting captured elsewhere in the clause.

Takeaway: This portion of the clause imposes another timed reporting requirement, adding another layer onto the initial 8 hour and 72 hour continual reporting requirements. It is plausible this could coincide with the clause's initial 8 hour security incident reporting obligation, but it is also plausible that this report could be triggered at a differing time, which would require contractors to track another reporting obligation to ensure it does not get missed.

vi. Access, Including Access to Additional Information or Equipment Necessary for Forensic Analysis - (c)(6)

Clause: Paragraph (c)(6) would provide CISA, FBI, and the contracting agency full access to applicable contractor information and information systems, and to contractor personnel, in response to a security incident reported by the contractor or a security incident identified by the Government. According to the clause, contractors would need to provide full access and cooperation for all activities determined by the contracting agency, CISA, and the FBI to: (1) Ensure an effective incident response, investigation of potential incidents, and threat



hunting activity, including supporting cloud and virtual infrastructure; and (2) Coordinate with CISA, the FBI, and the contracting agency to develop and implement corrections, fixes or other mitigations for discovered vulnerabilities and exploits.

In response to a security incident report to or access request from the Government, contractors would be required to first validate any CISA or FBI access request[13] and respond to any requests for access from the contracting agency, CISA, and the FBI within 96 hours with available information identified in paragraphs (c)(1), (c)(2), and (c)(3), as well as access to additional information or equipment that is necessary to conduct a forensic analysis.

Takeaway: The FAR Council explained that the purpose of this paragraph is for contractors to support incident response by providing access to additional information or equipment necessary for forensic analysis and time to cooperate with the Government on ensuring effective incident response, corrections, or fixes. The clause as worded would give a broad grant of access to contractor information and information systems. "Full access" has an expansive definition in the clause, meaning all contractor information systems used in performance or in support of performance of a contract to include:

1. Physical and electronic access to—

— (i) Contractor networks,

— (ii) Systems,

— (iii) Accounts dedicated to Government systems,

— (iv) Other infrastructure housed on the same computer network,

— (v) Other infrastructure with a shared identity boundary or interconnection to the Government system; and

2. Provision of all requested Government data or Government-related data, including—

— (i) Images,

— (ii) Log files,

— (iii) Event information, and

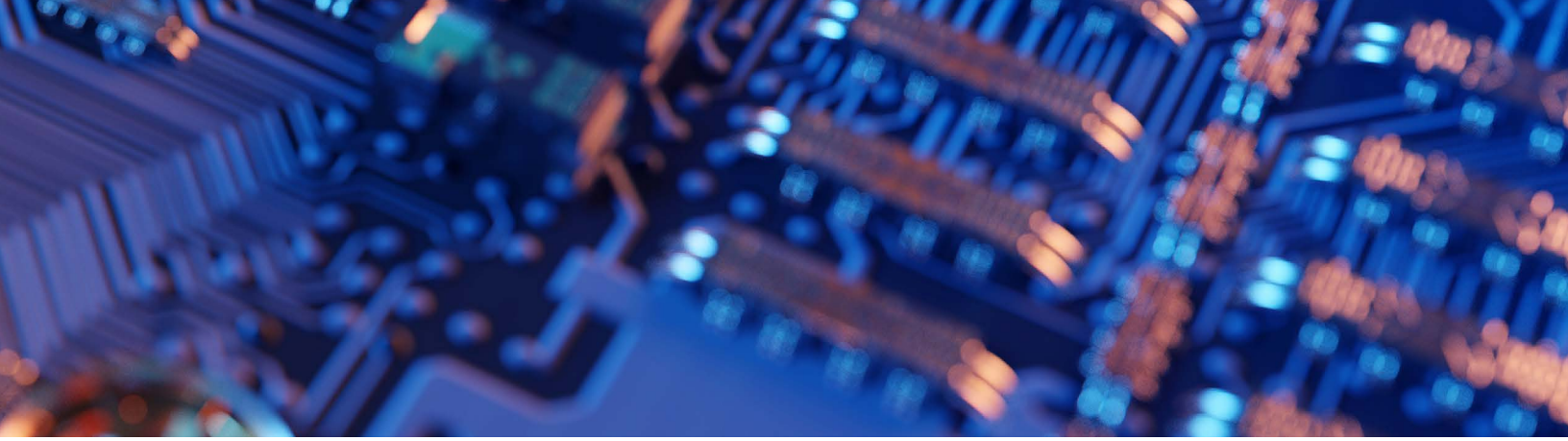
— (iv) Statements, written or audio, of contractor employees describing what they witnessed or experienced in connection with the contractor's performance of the contract.

This requirement would, for example, raise concerns related to the Government's access to and handling of trade secrets, legally privileged data, or third-party privacy or proprietary information that may be subject to confidentiality or use restrictions. Moreover, there is a risk that Government access could negatively impact a contractor's information system or lead to issues with the Government's protection of such data.

FAR Council Questions for Industry:

- Do you have any specific concerns with providing CISA, the FBI, or the contacting 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, that would address your

13 This would occur by contacting CISA Central at report@cisa.gov or (888) 282–0870, the FBI field office identified by the requestor using contact information from https:// www.fbi.gov/contact-us/field-offices, and immediately notifying the contracting officer and any other agency official designated in the contract in writing of receipt of the request



concerns while still providing the Government with appropriate access to conduct necessary forensic analysis regarding security incidents?

- Subparagraph (g)(i)(C) of section 2 of E.O. 14028 recognizes the need to identify appropriate and effective protections for privacy and civil liberties. Are there any specific safeguards that should be considered to ensure that these protections are effectively accomplished?

3. Cyber Threat Indicators and Defensive Measures Reporting - Paragraph (d)

Clause: The clause as proposed would also require contractors to either (i) subscribe to CIS Automated Indicator Sharing (AIS) (https://www.cisa.gov/ais) capability or successor technology during the performance of a contract, or (ii) during performance of a contract, participate in an information sharing and analysis organization (ISAO) or information sharing and analysis center (ISAC) with the capability to share indicators with AIS or successor technology. In utilizing one of these options for information sharing, the contractor would be required to share cyber threat indicators and recommended defensive measures, including associated tactics, techniques, and procedures, if available, when such indicators or measures are observed on ICT used in performance of the contract or provided to the Government.

As noted by the proposed clause, contractors submitting cyber threat indicators and defensive measures through AIS or an ISAC or ISAC will receive applicable legal protections (*see* 6 U.S.C. § 1505) in accordance with the Cybersecurity Information Sharing Act of 2015, Procedures and Guidance.

Takeaway: The sharing of threat indicators has largely been governed by voluntary arrangements, where contractors voluntarily sign an agreement with the Government to share threat information.[14] This clause would now mandate threat indicator and defensive measures sharing, potentially with respect to any threat indicator on ICT "used in performance of the contract or provided to the Government." As we have seen with other FAR clauses, the scope of "used in the performance of a contract" can be quite broad—potentially capturing any ICT used by a lawyer supporting a contract or any ancillary ICT used by a product development team. Having to report on every single threat indicator and associated defensive measures could over-extend contractors and those bodies receiving such reports.

4. Internet Protocol version 6 (IPv6) - Paragraph (e)

Clause: Paragraph (e) of the clause would apply to any ICT using internet protocol provided to the Government, and any interfaces exposed to the Government from a contractor information system using internet protocol, and would require the contractor to comply with all applicable mandatory capabilities specified in the current version of the USGv6 Profile (*see* NIST SP 500-267B) and provide to the Contracting Officer a copy of or access to the corresponding supplier's declaration of conformity in accordance with the USGv6 Test Program (*see* NIST SP 500-281A). If a wavier for IPv6 is granted, it will be identified elsewhere in the contract along with any conditions (*see* FAR 39.106-2).[15]

---

14 *See* 88 Fed. Reg. 27832 (May 3, 2023) (describing the Defense Industrial Base (DIB) Cybersecurity (CS) Program where contractors voluntarily sign a Framework Agreement)

15 If the agency Chief Information Officer (CIO) grants a waiver, contractors must develop and provide a product/service-specific IPv6 implementation plan that details how the contractor plans to incorporate applicable required capabilities recommended in the current version of NIST SP 500-267B into products and services provided to the Government. *See* FAR 39.106-2(c)

Takeaway: This paragraph captures the Government's transition efforts to deliver its information services, operate its networks, and access the services of others using only IPv6 (*see* OMB Memorandum M-21-07, **Completing the Transition to internet Protocol Version 6 (IPv6)**, dated November 19, 2020). IPv6 is the next-generation internet protocol, designed to replace version 4 (IPv4) that has been in use since 1983. Contractors awarded contracts that include ICT products and services that use internet protocols will be required to implement IPv6 and are expected to support incident response by implementing delta capabilities required for moving to IPv6.

5. Subcontracts - Paragraph (f)

Clause: Paragraph (f) would require a contractor to include the substance of this clause in all subcontracts where ICT is used or provided in the performance of the subcontract, including subcontracts for the acquisition of commercial products or services. As proposed, the contractor would also need to require subcontractors to notify the prime contractor and next higher tier subcontractor within 8 hours of discovery of a security incident.

Takeaway: Given the proposed rule would make FAR 52.239-ZZ a mandatory flow down for subcontractors using or providing ICT, both prime contractors and subcontractors will need to ensure this is incorporated into their lower-tier subcontractor agreements. Moreover, the flow down of this clause would not only impose a requirement for subcontractors to inform the prime or higher-tier subcontractor of an incident, but a subcontractor must also notify CISA as prescribed in the other sections of the clause.

III. FAR 52.239-AA, *Security Incident Reporting Representation*

In addition to FAR 52.239-ZZ, the FAR Council added a new clause that would require prime contractors to make an affirmative representation.

Clause: FAR 52.239-AA, *Security Incident Reporting Representation*, is required to appear in all solicitations. The clause would require offerors to represent that they have submitted all security incident reports in a current, accurate and complete manner. The clause would also require the offeror to represent whether it has required (i) each first tier subcontractor to notify the offeror within 8 hours of discovery of a security incident, as required by paragraph (f) of FAR clause 52.239-ZZ; and (ii) each lower-tier subcontractor to include the requirements of paragraph (f) of FAR clause 52.239-ZZ in their subcontract.

Takeaway: A new representation for incident reporting will up the ante for enforcement risk under the False Claims Act (FCA). Similar to the requirements for certified cost and pricing data,[16] this representation calls for current, accurate, and complete incident reports. As DOJ has leveraged a current, accurate, and complete certification requirement for targeting companies for defective cost and pricing data,[17] they have a road map for doing so when a contractor provides untimely, inaccurate, or incomplete security incident reports. Moreover, failure to flow down incident reporting obligations—both to CISA and the prime or higher-tier contractor—could not only cause a breach of contract, but could also lead a contractor to become subject to FCA liability.

IV. Conclusion

If adopted as currently written, the proposed rule would require contractors to comply with two new FAR clauses with wide-reaching implications on contractor cybersecurity compliance, impacting contractors with contracts below the simplified acquisition threshold or for commercial products (including COTS items) and services where ICT is used or provided in the performance of the contract. The new security incident reporting and threat sharing obligations highlight the importance of understanding the applicable cybersecurity requirements contained in the FAR and one's contract. Failure to comply with such requirements could pose significant liability in terms of breach damages, and, in some instances, liability for fraud under the FCA.

---

16 *See* FAR 15.406-2

17 *See, e.g.*, PowerSecure, Inc.'s $8.4 million settlement in November 2022 related to its failure to disclose cost or pricing data; Insitu Inc.'s $25 million settlement in January 2021 to resolve allegations that it knowingly submitted materially false cost and pricing data for contracts with the U.S. Special Operations Command and the Department of the Navy to supply and operate Unmanned Aerial Vehicles

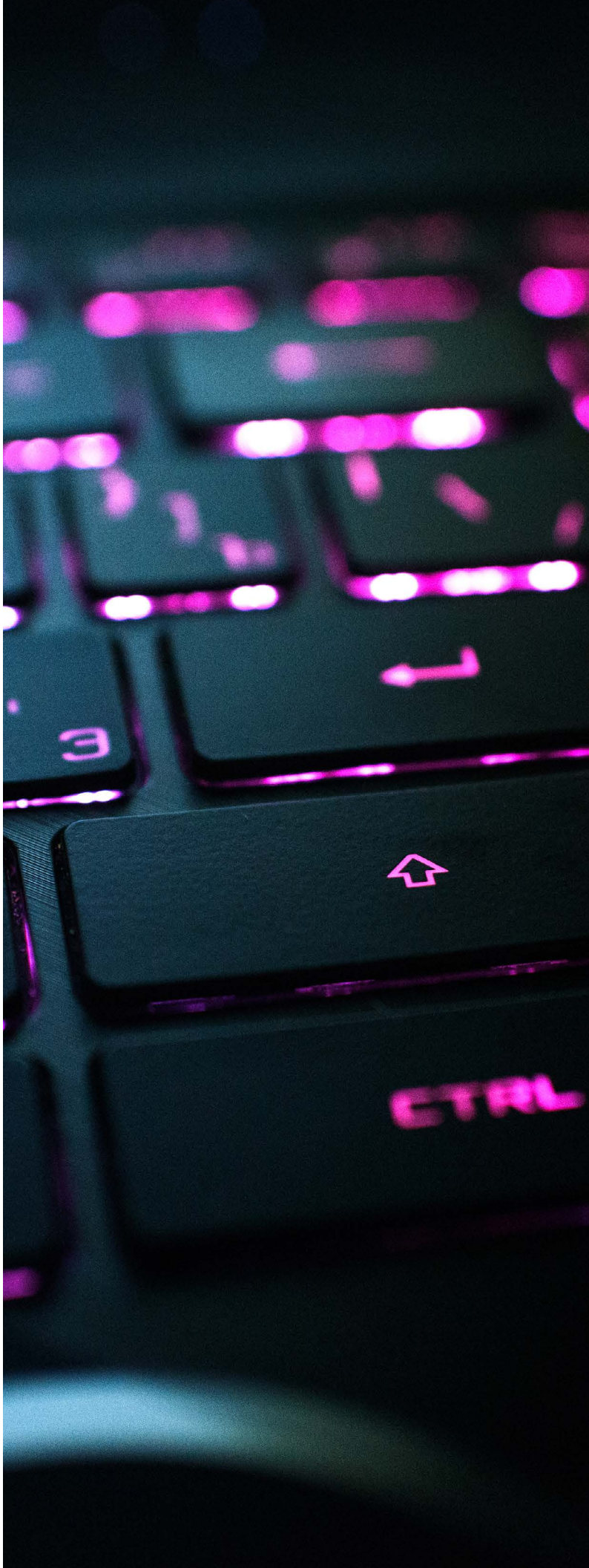
As emphasized by DOJ in its **Civil-Cyber Fraud Initiative**, this area is ripe for enforcement.[18]

Contractors are well advised to monitor the proposed rule, assess its impact, and consider submitting comments as part of the rulemaking process.

Hogan Lovells has deep experience advising businesses on the compliance obligations and challenges of the federal Government's cybersecurity requirements. Please feel free to reach out to the authors if you would like additional information about the proposed rule or other assistance concerning the complex and evolving area of government contractor cybersecurity requirements.

---

18 Stating that the initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly violating obligations to monitor and report cybersecurity incidents and breaches



Stacy Hadeka
Counsel | Washington, D.C.
T: +1 202 637 3678
E: stacy.hadeka@hoganlovells.com

Michael Scheimer
Partner | Washington, D.C.
T: + 1 202 637 6584
E: michael.scheimer@hoganlovells.com

Michael Mason
Partner | Washington, D.C.
T: +1 202 637 5499
E: mike.mason@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Centre: Berlin

www.hoganlovells.com