



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.

Part 1 of this A&D Insights covers one of two proposed Federal Acquisition Regulation (FAR) council rules on cybersecurity—Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems.

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

On October 3, 2023, the FAR Council issued two proposed FAR 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). These rules implement portions of President Biden’s May 2021 Executive Order (EO) No. 14,028, *Improving the Nation’s Cybersecurity* (previously discussed [here](#)). Industry has until December 4, 2023, to comment on these rules.

These proposed rules come during Cybersecurity Awareness month and at a time of increased cybersecurity rulemaking—*see, e.g.*, the Department of Homeland Security’s (DHS) final rule on safeguarding Controlled Unclassified Information (CUI) (**88 Fed. Reg. 40,560 (June 21, 2023)**); DHS’s request for information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (**87 Fed. Reg. 55,833 (Sept. 12, 2022)** (discussed [here](#))); and the Security and Exchange Commission’s final rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (**88 Fed. Reg. 51,896 (Sept. 5, 2023)** (discussed [here](#)). We expect to see continued cybersecurity developments across the federal Government in the coming months—*see, e.g.*, **FAR Case No. 2017-016**, Controlled Unclassified Information; **FAR Case No. 2023-002**, Supply Chain Software Security;

and the Department of Defense’s (DoD’s) **expected rulemaking** implementing the Cybersecurity Maturity Model Certification (CMMC) program.

Organizations subject to these new rules, including the one discussed in more detail below, will want to monitor and prepare for these developments, understand one’s current cybersecurity posture, and consider preparing comments if impacted.

Part 1: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems

The FAR Council published a proposed rule on October 3, 2023, to standardize cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems (FIS).¹ **See 88 Fed. Reg. 68,402 (Oct. 3, 2023)**. Recognizing the importance of securing FIS, whether cloud-based, on-premises, or a hybrid of the two, the proposed rule sets out in great detail cybersecurity policies, procedures, and requirements applicable to contractors that develop, implement, operate, or maintain a FIS. Consistent with the Government’s focus on scrutinizing cybersecurity noncompliance in terms of fraud²—the rule states that compliance with these cybersecurity requirements “is material to eligibility and payment under Government contracts.”

The Government often contracts with information technology (IT) and operational technology (OT) providers to conduct day-to-day functions on FIS.³ Historically, the contracts for such services have imposed cybersecurity requirements that lack consistency and clarity, add costs, and frequently restrict competition. Moreover, agencies have taken inconsistent approaches as to determining whether a system is a FIS versus a contractor information system, resulting sometimes in unnecessary and

burdensome requirements on contractors.

The proposed FAR rule is intended to provide a more consistent and streamlined implementation of cybersecurity standards—including those included in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and the Federal Risk and Authorization Management Program (FedRAMP). The proposal seeks to achieve these goals through changes to FAR, including:

- Adding a new FAR subpart 39.X, “Federal Information Systems,” to prescribe definitions, policies, and procedures for agencies when acquiring services to develop, implement, operate, or maintain a FIS; and
- Adding **two** new FAR clauses for use when acquiring services to develop, implement, operate, or maintain a FIS:
 1. FAR 52.239-YY, *Federal Information Systems Using Non-Cloud Computing Services*, for inclusion in solicitations and contracts that use or may use non-cloud computing services in performance of the contract; and
 2. FAR 52.239-XX, *Federal Information Systems Using Cloud Computing Services*, for inclusion in solicitations and contracts that use or may use cloud computing services in performance of the contract.

The specific FAR clauses applicable to a contract will depend on whether the FIS utilizes cloud computing services, services other than cloud computing services (*e.g.*, on-premises computing services), or a hybrid of both approaches when providing services to develop, implement, operate, or maintain the FIS. The proposed rule would require compliance with the policies, procedures, and requirements applicable to each respective service approach.

1 This proposed rule is separate and apart from the anticipated FAR rule addressing contractor information system cybersecurity requirements. See Open FAR Case No. 2017-016.

2 See our previous discussion of the Department of Justice’s Civil Cyber Fraud Initiative [here](#).

3 See proposed updates to FAR 2.101 and FAR 52.239-YY(a) for definitions of IT and OT.

I. Background

All FIS are governed by the Federal Information Security Management Act, originally implemented as Title III of the e-Government Act of 2002 (Pub. L. No. 107-347), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283) (collectively, “FISMA”). FISMA requires agencies to protect FIS, but the statute itself does **not** include any technical security requirements—it mandates that agencies create an information security program commensurate with an agency’s level of risk.⁴ The actual security requirements are then documented in agency-specific security policies, which can be extended to industry partners (*e.g.*, contractors), via clauses in contracts or other agreements.

Under FISMA, every FIS must go through a security authorization process and receive a final “Authorization to Operate” (ATO) from an agency.⁵ No FISMA-covered FIS can operate in the federal government without a security authorization. This is accomplished using the NIST Risk Management Framework (RMF) process described in NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, which provides that:

- An agency will first determine the security category of their information system (based on the “impact level”) in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;⁶
- Based on that final security category, the agency selects minimum security

requirements in accordance with FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;

- The agency then applies the appropriately tailored set of baseline security controls from the catalog in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.⁷
- This information is then documented in a security authorization package⁸ for the AO to conduct an assessment and issue an authorization decision (*i.e.*, the ATO).

According to the proposed rule, a FIS is an information system—to include Internet of Things (IoT) devices and OT—used or operated by an agency, a contractor of an agency, or another organization, on behalf of an agency. The proposed rule notes that agencies are responsible for determining what information systems are FIS in accordance with the following definition:

- (1) Means an information system (44 U.S.C. 3502(8))⁹ 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).¹⁰

Thus, this proposed rule impacts those contractors that develop, implement, operate, or maintain a FIS.

4 Under FISMA, each agency is responsible for “providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of...information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency[.]” 44 U.S.C. § 3544(a)(1)(A)(i)(ii) (emphasis added).

5 See *e.g.*, OMB Circular A-130, Managing Information as a Strategic Resource; NIST 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy; NIST 800-53, Security and Privacy Controls for Information Systems and Organizations.

6 FIPS 199 establishes three potential levels of impact (Low, Moderate, or High) relevant to securing federal information and information systems for each of three stated security objectives (Confidentiality, Integrity, and Availability).

7 Under the RMF process, the level of effort required for a security authorization depends on the impact level of the information contained on each system (the security authorization of a system with a FISMA impact level of “Low” will be less rigorous and costly than a system with a higher impact level).

8 In accordance with NIST SP 800-37 and SP 800-53, the security authorization package should include the System Security Plan (SSP), the Security Assessment Report (SAR), and a Plan of Action and Milestones (POAM).

9 “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)). Information resources as used in this definition, includes any ICT.

10 See 32 C.F.R. § 2002.4(hh).

II. FAR 52.239-YY, Federal Information Systems Using Non-Cloud Computing Services

This newly proposed clause at FAR 52.239-YY implements cybersecurity requirements for contractors that develop, implement, operate, or maintain a FIS using **non-cloud computing** systems.

FAR 52.239-YY includes requirements addressing the following topics:

1. Records Management and Government Access - Paragraph (c)

Clause: The clause includes a section requiring contractors to provide and dispose of Government data and Government-related data in the manner and format specified in the contract. Contractors must also provide confirmation to the contracting officer that such data has been disposed of in accordance with contract closeout procedures. This section also outlines the requirements for contractors to assist the Government: (1) in carrying out a program of inspection to safeguard against threats and hazards to the security and privacy of Government data, and (2) conduct audits, investigations, inspections or similar activities. Specifically, the clause would require contractors to provide the Government, which can include Cybersecurity and Infrastructure Security Agency (CISA) (for civilian agencies) or other agencies specified by the contracting officer (*e.g.*, Federal Bureau of Investigation (FBI)), with timely and full access to Government data and Government-related data, contractor personnel, and facilities.

Takeaway: This clause, like other clauses providing for audit rights (including Paragraph (f) of FAR 52.239-XX), gives the Government a broad latitude to access contractor records and information. For instance, the definitions of “Government data” and “Government-related data” could be viewed to include information that is created or obtained by the Government, or by a contractor on behalf of the Government, in the course of official Government business and information that is created or obtained by a contractor through the storage, processing,



or communication of Government data.¹¹ Based on these broad definitions, contractor information discussing Government data might be considered a type of Government-related data. This clause also provides a process for confirming the validity of requests from CISA for access, imposing additional affirmative actions on the contractor. Contractors will want to ensure they have proper recordkeeping, documentation handling, and information safeguarding policies and procedures in place.

2. Annual Assessments - Paragraph (d)

Clause: When a FIS is designated by an agency as a “Moderate” or “High” impact level in accordance with FIPS Publication 199, the clause would require the contractor to conduct at least annually (1) a cyber threat hunting and vulnerability assessment to search for vulnerabilities, risks, and indicators of compromise; and (2) an independent assessment of the security of each FIS.

The contractor would also be required to submit assessment results, including any recommended improvements or risk mitigations, to the contracting officer. The agency would review the results and may require the contractor to implement any recommended improvement(s) or mitigation. If the agency does not require the contractor to implement a recommendation or mitigation, the contractor would document the agency’s rationale in its System Security Plan (SSP) (*see* Paragraph (e) for more details).

Takeaway: This assessment requirement is not new, but makes it a clear contractual requirement for contractors to complete and document. The clause would also allow for the use of a third-party assessment organization to perform the required assessments, but requires the parties to enter into a confidentiality agreement to protect federal data under the contract and notify the contracting officer of any existing business relationships the contractor may have with the assessment organization. These are similar concerns with third-party assessors we already see with FedRAMP¹² and we expect to see addressed in DoD’s CMMC program.¹³ Contractors will want to ensure that the assessment requirement and the potential for mitigation measures are adequately considered in the pricing of the contract.¹⁴

3. Security and Privacy Controls - Paragraph (e)

Clause: This section notes that controls ***specified by the agency*** will be based on the “current version” of the following documents at the time of contract award:

- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*;
- NIST SP 800-213, *IOT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*;

11 Government-related data does not include—(1) A contractor’s business records (e.g., financial records, legal records) that do not incorporate Government data; or (2) Data such as operating procedures, software coding or algorithms that are not primarily applied to the Government data.

12 See 3PAO Obligations and Performance Standards, Version 3.3 (Apr. 6, 2023), available at https://demo.fedramp.gov/assets/resources/documents/3PAO_Obligations_and_Performance_Guide.pdf.

13 See, e.g., Cyber AB CMMC Assessment Process (CAP), Version 1.0 (Draft) (July 2022), available at <https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf>.

14 The FAR Council estimates it will annually cost contractors approximately \$132,000 to obtain an independent assessment of the security of a FIS and approximately \$112,000 for a contractor to conduct a cyber threat hunting and vulnerability assessment of a FIS.



- NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*; and
- NIST SP 800-82, *Guide to Industrial Control Systems Security*.

For FIS designated as a high value asset,¹⁵ contractors will also be subject to additional security and privacy controls, that could include the implementation of a high value asset overlay, immediate failover and/or recover plans, and complying with requisite cybersecurity assessments.¹⁶

This section of the clause also requires contractors to: (1) develop, review, and update, if appropriate, an SSP to support authorization of all applicable FIS, and (2) maintain contingency plans for all information technology systems aligned to NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*.

Takeaway: Although this clause identifies relevant NIST SP guidance for contractors, this section still contemplates agency-level discretion as to the applicability for certain controls captured within the NIST publications. The agencies are charged with identifying which controls will apply to the contractor. This provision also puts the onus on the contractor to follow the current versions of each NIST SP. Although the rule does not require a specific format for the SSP, it notes that NIST SP 80034 provides information on a template that contractors may choose to use. The rule also contemplates that contractors will be expected to provide a copy of the SSP and contingency plans

to an agency upon request. Contractors will want to ensure they adequately document their SSPs.

4. Additional Considerations - Paragraph (f)

This Section requires contractors to apply NIST SP guidance on various topics when performing or managing certain activities related to the FIS, including:

- managing information system risk when supporting agency risk management activities (e.g., NIST SP 800-39);
- developing risk management processes (NIST SP 800-37);
- conducting and communicating the results of risk assessments (e.g., NIST SP 800-30);
- designing zero trust architecture approaches; considering security when executing within the context of systems engineering (e.g., NIST SP 800-207);
- selecting, adapting, and using cyber resiliency constructs for new systems, system upgrades, or repurposed systems; implementing continuous monitoring strategies for FISs (e.g., NIST SP 800-160);
- implementing digital identity services and requirements (e.g., NIST SP 800-63-3); and
- providing continuous monitoring (e.g., NIST SP 800-137).

Takeaway: In addition to the NIST SP guidance required by paragraph (e), contractors will

¹⁵ "High value asset" means Government data or a FIS that is designated as a high value asset pursuant to OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program.

¹⁶ See, e.g., CISA's High Value Asset Overlay, Version 2 (Jan. 2021), available at https://www.cisa.gov/sites/default/files/publications/HVA%20Control%20Overlay%20v2.0_0.pdf.



be required to implement additional controls and processes as captured in the nine NIST SPs identified in this section of clause. This listed guidance documents impose significant requirements, so contractors will want explicit confirmation from the agency as to which controls and processes it should implement based on the ultimate impact level of the FIS.

5. Supply Chain Risk Management - Paragraph (g)

Clause: This section of the clause advises that contractors may implement alternative, additional, or compensating cyber supply chain risk¹⁷ management security controls when authorized in writing to do so by the contracting officer.

Takeaway: The clause requires contractors to implement the controls in NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*. See FAR 52.239-YY(e). However, this clause also provides the contractor with an opportunity to substitute or add cyber supply chain risk management security controls with permission of the contracting officer.

6. Incident Reporting - Paragraph (h)

Clause: This section refers to FAR 52.239-ZZ, *Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology*, which would require contractors to comply with the security incident and cyber threat reporting requirements outlined in the newly proposed clause.

Takeaway: See our further analysis of FAR 52.239-ZZ in Part 2 of this A&D Insights.

7. Limitations on Access to, Use, and Disclosure of Data - Paragraph (i)

Clause: This section specifies the limitations on contractor access to, use, and disclosure of Government data, Government-related data, and metadata under the contract, including ensuring that its employees are subject to all such access, use, and

disclosure prohibitions and obligations of the clause. This section also states that a contractor can only use Government metadata to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the contracting officer.

This section also requires contractors to notify the contracting officer of any requests from an entity other than the contracting activity (including warrants, seizures, or subpoenas the contractor receives from another Federal, State, or local agency) for access to Government data, Government-related data, or any associated metadata. The clause notifies contractors that they must also comply with applicable clauses, regulations, and laws regarding unauthorized disclosure.

Takeaway: As noted above, the definition of “Government data” and “Government-related data” is quite broad (and includes the OT equipment list required by paragraph (k)), so contractors will need to ensure they safeguard and properly handle such data. If not, the clause imposes significant consequences whereby the contractor must indemnify the Government from liability that arises out of the contractor’s unauthorized disclosure. See FAR 52.239-YY(m). Thus, if the rule is implemented as currently drafted, contractors will want to implement or supplement recordkeeping, documentation handling, and information safeguarding policies and procedures.

8. Cryptographic Key Services - Paragraph (j)

Clause: Through this section, the Government reserves the right to implement and operate its own cryptographic key management, key revocation, and key escrow services; otherwise, the contractor will need to provide the agency with applicable key material and services.

Takeaway: When providing cryptographic key services under the contract, the proposed clause would require contractors to provide the agency with applicable key material and services; however, the Government reserves the right to implement

17 “Cyber supply chain risk” means the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. This includes risks that arise from threats exploiting vulnerabilities or exposures within products and services traversing the supply chain as well as threats or exposures within the supply chain itself. The level of risk depends on the likelihood that relevant threats may exploit applicable vulnerabilities and the consequential potential impacts.

and operate its own cryptographic key services under the contract. Contractors would want to review their contract to determine whether the Government has exercised this option.

9. List of OT equipment – Paragraph (k)

Clause: Unless the contract states otherwise, this section requires contractors to develop and maintain a list of the physical location of all OT equipment included within the boundary for the non-cloud FIS (which will be considered “Government data”) and provide a copy of current and/or historical list(s) to the Government, upon request.

Takeaway: As noted above, this proposed clause addresses the contractor’s rights to access, use, and disclose Government data, which can also have implications for indemnification. Moreover, the proposed rule does **not** specify a format for the OT equipment list, but it must include at a minimum five categories of information about the equipment to positively locate and track any movement of the equipment during contract performance, including details on password protection and the ability for remote access to the equipment. Thus, if the rule is implemented as currently drafted, contractors will want to ensure it properly compile their OT equipment lists and ensure their safeguarding.

10. Binding Operational Directives and Emergency Directives – Paragraph (l)

Clause: This portion of the clause advises that contractors must comply with Binding Operational Directives (BODs) and Emergency Directives (EDs) issued by CISA that have specific applicability to a FIS used or operated by a contractor. Those BODs and EDs not applicable to the contract will be listed in the clause. Relevant BODs and EDs issued after the date of the contract award will be applied to this contract, at the contracting officer’s discretion, through appropriate modification of the contract.

Takeaway: A list of BODs and EDs can be found at <https://www.cisa.gov/directives>. Contractors will be responsible for accessing and understanding the applicable BODs and EDs, adding additional obligations for contractors to affirmatively identify and implement additional cybersecurity requirements at the time of contract award. Contractors will also





want to ensure they track contract modifications that add newly issued BODs and/or EDs and consider submitting requests for equitable adjustments to account for any increased costs of performance.¹⁸

11. Indemnification - Paragraph (m)

Clause: The proposed clause would require the contractor to indemnify the Government from any liability that arises out of the performance of the contract and is incurred because of a contractor's introduction of certain information¹⁹ or matter into Government data or the contractor's unauthorized disclosure of certain information or material.²⁰ According to the rule, this section serves as a waiver of any defenses—including negligence and the "Government Contractor Defense"—in essence turning a contractor's liability into strict liability. This section of the clause also provides terms and requirements in the event of a claim or suit against the Government for such an unauthorized disclosure or introduction of data or information, including notice by the Government of any claim or suit and a contractor's furnishing of information pertaining to a claim or suit.

The indemnity provision does not apply to—(1) A disclosure or inclusion of data or information upon specific written instructions of the contracting officer directing the disclosure or inclusion of such information or data; or (2) A third-party claim that is unreasonably settled without the consent of a contractor, unless required by final decree of a court of competent jurisdiction.

Takeaway: According to the proposed rule, the indemnification text was taken from industry terms of service agreements for cloud services providers, despite this clause relating to **non-cloud** computing services. Moreover, this indemnification provision imposes strict liability for a contractor, removing all potential defenses. Given the broad scope of information referred to in this provision—*e.g.*, CUI, personally identifiable information (PII), and records maintained on individuals—the proposed clause would pose for contractors a heightened risk of liability.

12. Subcontracts – Paragraph (n)


Clause: This section requires the substance of FAR 52.236-YY to be included in any subcontracts issued under the contract that are for services to develop, implement, operate, or maintain a FIS using non-cloud computing services.

Takeaway: Given FAR 52.239-YY is a mandatory flow down for subcontractors providing services to develop, implement, operate, or maintain a FIS using non-cloud computing services, prime contractors and subcontractors will need to ensure this is incorporated into their lower-tier subcontractor agreements.

18 The FAR Council estimates it will cost contractors approximately \$130,000 to implement existing CISA BODs and EDs in year one and approximately \$30,000 to implement new BODs or EDs issued each following year.

19 This includes copyrighted material to which a contractor has no rights or license that may infringe on the copyright interest of others, information subject to a right of privacy, and any libelous or other unlawful matter.

20 This includes a contractor's potential or actual unauthorized disclosure of trade secrets, copyrighted materials, contractor bid or proposal information, source selection information, classified information, material marked as "Controlled Unclassified Information," information subject to a right of privacy or publicity, personally identifiable information as defined by OMB Circular A-130 (2016) or successor thereof, or any record maintained on individuals as defined in 5 U.S.C. § 552a.



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

FAR 52.239-XX only applies to aspects of a FIS that involve **cloud computing services**, which includes service models such as software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.²¹

FAR 52.239-XX includes requirements addressing the following topics:

1. Cloud Computing Security Requirements - Paragraph (c)

Clause: This section of the clause outlines the cloud-specific requirements for contractors developing, implementing, operating, or maintaining a FIS using cloud computing services. Agencies will be required to identify the FIPS Publication 199 impact level and the corresponding Federal Risk and Authorization Management Program (FedRAMP) authorization level for all applicable cloud computing services in the contract. Contractors subject to the clause will also need to engage in continuous monitoring activities and provide continuous monitoring deliverables as required for FedRAMP approved capabilities.²² This section also provides the Government with the right to implement and operate its own cryptographic key management, key revocation, and key escrow services. Lastly, this section specifies that, when a system is categorized as having FIPS Publication 199 “High” impact, contractors must maintain within the United States or its outlying areas (*see* FAR 2.101) all Government data that is not physically located on U.S. Government premises, unless otherwise specified in the contract.

Takeaway: FedRAMP has been a long-established program since 2011, and was finally codified with the passage of the FedRAMP Authorization Act (44 U.S.C. § 3608), which was enacted as part of the Fiscal Year 2023 National Defense Authorization Act (Pub. L. No. 117-263). It also establishes a “presumption of adequacy” for cloud computing services that have received a FedRAMP authorization. In particular, the Act requires Government agencies to confirm whether a cloud computing product or service has already received authorization prior to beginning the authorization process and, to the extent practicable, reuse existing assessments of security controls and materials. *See* 44 U.S.C. § 3613. The legislation caveats, however, that agencies may still impose their own security requirements where necessary. As currently written, the proposed rule does not address the presumption of adequacy.

2. Limitation on Access to, Use, and Disclosure of Data - Paragraph (d)

Clause: This section specifies the limitations on contractor access to, use, and disclosure of Government data and Government-related data under the contract, including ensuring that its employees are subject to all such access, use, and disclosure prohibitions and obligations of the clause. This section also states that a contractor can only use Government-related data to manage the operational environment that supports the Government data and for no other purpose unless otherwise permitted with the prior written approval of the contracting officer.

Takeaway: This section does not include the requirements for third-party access requests found in FAR 52.239-YY(i) for non-cloud services and were instead included in a separate section in

²¹ See NIST SP 800-145, The NIST Definition of Cloud Computing.

²² See “FedRAMP Continuous Monitoring Strategy Guide” at https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf.

paragraph (g) in FAR 52.239-XX. But given the broad definition of “Government data” and “Government-related data,” contractors will need to ensure they safeguard and properly handle such data. If not, the clause imposes significant consequences whereby the contractor must indemnify the Government from liability that arises out of the contractor’s unauthorized disclosure. *See* FAR 52.239-ZZ(h).

3. Incident Reporting - Paragraph (e)

Clause: This section refers to FAR 52.239-ZZ, *Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology*, which would require contractors to comply with the security incident and cyber threat reporting requirements outlined in the newly proposed clause.

Takeaway: See our further analysis of FAR 52.239-ZZ in Part 2 of this A&D Insights.

4. Records Management and Government Access - Paragraph (f)

Clause: This section requires contractors to provide and dispose of Government data and Government-related data in the manner and format specified in the contract. Contractors must also provide confirmation to the contracting officer that such data has been disposed of in accordance with contract closeout procedures. The clause also outlines requirements for contractors to assist the Government: (1) in carrying out a program of inspection to safeguard against threats and hazards to the security and privacy of Government data, and (2) conduct audits, investigations, inspections or similar activities. Specifically, the clause would require contractors to provide the Government, which can include Cybersecurity and Infrastructure Security Agency (CISA) (for civilian agencies) or other agencies specified by the contracting officer (e.g., Federal Bureau of Investigation (FBI)), with timely and full access to Government data and Government-related data, contractor personnel, and facilities.

Takeaway: This section (f) of FAR 52.239-XX is exactly the same as FAR 52.239-YY(c). This clause, like other clauses providing for audit rights, gives the Government a broad latitude to access contractor records and information. For instance, the definitions of “Government data” and “Government-related data”

could be broadly construed to include (i) information that is created or obtained by the Government, or by a contractor on behalf of the Government, in the course of official Government business and (ii) information that is created or obtained by a contractor through the storage, processing, or communication of Government data. This clause would also require contractors to confirm the validity of a request from CISA for access by contacting CISA and notifying the contracting officer in writing, imposing additional affirmative actions on the contractor. Accordingly, this type of provision will require contractors to ensure it has proper recordkeeping, documentation handling, and information safeguarding policies and procedures in place.

5. Notification of Third-Party Access Requests - Paragraph (g)

Clause: This section of FAR 52.239-XX requires contractors to notify the contracting officer of any requests from a third-party (including another Federal, State, or local agency) to access Government data or Government-related data. This section also notifies contractors that they must also comply with applicable clauses, regulations, and laws regarding unauthorized disclosure.

Takeaway: This will require contractors to affirmatively notify their contracting officers of third-party access requests, and thus contractors will want to adopt processes for tracking these types of requests and procedures for notifying government customers or such requests.

6. Indemnification - Paragraph (h)

Clause: This section of the clause mirrors paragraph (m) of FAR 52.239-YY, so see above analysis in Section II(11) for this section’s requirements.

Takeaway: According to the proposed rule, the indemnification text was taken from industry terms of service agreements for cloud services providers. Moreover, contractors should be aware that this indemnification provision imposes strict liability for a contractor, removing all potential defenses. Given the broad scope of information referred to in this provision—e.g., CUI, PII, and records maintained on individuals—the proposed clause would pose for contractors a heightened risk of liability.

7. Subcontracts - Paragraph (i)

Clause: This section requires the substance of FAR 52.236-XX to be included in any subcontracts issued under the contract that are for services to develop, implement, operate, or maintain a FIS using cloud computing services.

Takeaway: Given the proposed rule would make FAR 52.239-XX a mandatory flow down for subcontractors providing for services to develop, implement, operate, or maintain a FIS using cloud computing services, prime contractors and subcontractors will need to ensure this is incorporated into their lower-tier subcontractor agreements.

IV. Conclusion

If adopted as currently written, the proposed rule would require clauses for standardizing cybersecurity requirements for FIS across non-cloud and cloud computing services. The existing and proposed new cybersecurity requirements for contractors that perform FIS-related services highlights the importance of understanding the applicable compliance requirements of the FAR and NIST SP guidelines, FIPS Publication standards, CISA BODs and EDs, and FedRAMP requirements. Failure to comply with such requirements could pose significant liability in terms of breach damages, indemnification obligations, and, in some instances, liability for fraud under the False Claims Act (FCA).

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

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.





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

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2023. All rights reserved. BD-REQ-48