WINSTON & STRAWN LLP

BLOG

Navigating the Maze: A Comparison of Selected Federal Cybersecurity Regulations

APRIL 11, 2025

Cybersecurity requirements for contractors doing business with the U.S. federal government are nothing new. Yet, as cybersecurity threats continue to evolve, federal contractors have been continually confronted by a potentially confusing array of security regulations and requirements for protecting certain categories of information on federal and nonfederal information systems. Four active and proposed contract clauses relating to these cybersecurity requirements likely are top of mind for most government contractors doing business with the U.S. federal government:

- DFARS 252.204-7012, which addresses U.S. Department of Defense (DOD) requirements for protecting covered defense information [1] on covered contractor information systems and for reporting cyber incidents for covered contractor information systems processing covered defense information.
- HSAR 3052.204-72, which provides U.S. Department of Homeland Security contractor requirements for protecting CUI to which contractors have access or that they will maintain on behalf of the agency, and for federal information systems that include contractor systems processing CUI that are operated on behalf of the agency.
- FAR 52.204-XX, which is proposed by the FAR Council as a government-wide acquisition regulation for the protection of CUI.
- FAR 52.204-21, which is the "basic" government-wide acquisition regulation that applies to solicitations and contracts when a contractor or subcontractor may have Federal contract information [2] residing in or transiting through its information system. [3]

While these regulations share the common goal of improving the security of information and systems, they differ in their focus and requirements. For contractors working with multiple federal agencies, understanding these differences is important for achieving and maintaining compliance and avoiding potential penalties. Below is a review of selected aspects of these cybersecurity regulations to help contractors navigate their respective responsibilities.

SYSTEMS TO WHICH THE REGULATIONS APPLY

Both the DFARS and the FAR Basic Rule generally apply to nonfederal information systems and apply NIST SP 800-171 controls or, in the case of FAR 52.204-21, a loose subset of them. The Homeland Security regulations, on the other hand, generally apply to federal information systems and apply the NIST SP 800-53 framework. The proposed

new CUI rule applies to both federal and nonfederal information systems and, accordingly, applies either NIST SP 800-171 or NIST SP 800-53, as the situation requires:

REGULATION	GENERAL APPLICATION AND STANDARD
DFARS 252.204-7012	Generally applies NIST SP 800-171 controls to nonfederal information systems, except for cloud services, which must meet Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.[4] Information Systems that are part of an IT service or system operated on behalf of the government – follow DFARS 252.239-7010 for Cloud Computing Services, and the requirements of the contract for any other such IT service or system.
HSAR 3052.204-72	When federal information systems are involved, the contractor must receive Authority to Operate, complete a security authorization process, and be independently assessed in accordance with NIST SP 800-53 controls.[5]
FAR 52.204-XX	Applies to both federal and nonfederal information systems and, accordingly, applies either NIST SP 800-171 or NIST SP 800-53, as the situation requires.
FAR 52.204-21	Impacts nonfederal information systems and applies 15 requirements that are a loose subset of NIST SP 800-171.

INCIDENT REPORTING TIMELINES

Aside from FAR 52.204-21, each of the regulations carries an affirmative obligation to report cyber incidents that may compromise protected information or systems. Reporting timelines and processes differ between each regulation:

REGULATION	GENERAL RESPONSE REQUIREMENT
DFARS 252.204-7012	Contractors must report cyber incidents within 72 hours of discovery. Reporting must be done via the DoD's cyber incident reporting portal, and affected contractors must also provide forensic evidence if requested. Malicious software that is discovered and isolated in connected with a reported incident must be submitted to the DOD Cyber Crime Center.
HSAR 3052.204-72	The Department of Homeland Security (DHS) mandates a two-tier requirement for cyber incident reporting of known or suspected incidents. Any known or suspected incident that involves Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII), must be reported within one hour of discovery. All other incidents must be reported within eight hours of discovery. Known or suspected incidents must be reported to the security operations center for the applicable homeland security component using Attachment F, *Incident Response*, to

	DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems*.
FAR 52.204-XX	The proposed FAR rule requires the contractor to report CUI incidents occurring in a non-federally controlled facility, within eight hours of discovery of the incident. CUI incidents on a federally controlled facility are to be reported in accordance with agency policy. Additional reporting is required for unmarked and mis-marked CUI, which must be reported within eight hours of discovery.
FAR 52.204-21	No external reporting obligations.

ASSESSMENT AND CERTIFICATION REQUIREMENTS

Similarly, aside from FAR 52.204-21, each of the regulations addresses (or is expected to address) requirements for assessments and certifications.

REGULATION	GENERAL ASSESSMENT AND CERTIFICATION REQUIREMENT
DFARS 252.204-7012	Contractors must comply with assessment and certification requirements based on NIST SP 800-171 controls. DFARS 252.204-7012 is accompanied by DFARS 252.204-7020, which requires assessment of compliance with NIST controls. Cybersecurity Maturity Model Certification (CMMC) under DFARS 252.204-7021 will be phased in for defense contractors (four phases over three years) and will require third-party certification for certain contracts.
HSAR 3052.204-72	Does not require certification, but HSAR requires a third-party assessment of contractor's security and privacy controls as part of obtaining an ATO, which assesses compliance with NIST SP 800-53 and requirements of the security authorization package.
FAR 52.204-XX	Currently, no explicit independent certification requirements have been included in the proposed rule, though the proposed rule requires contractor cooperation with validation actions conducted by other agencies. It is expected that future revisions of the proposed rule may adopt a model similar to CMMC. FAR's proposed rule suggests standardized assessments across federal agencies, but details remain undefined. Contractors must comply with agency assessment requirements, as specified in Form SF XXX.
FAR 52.204-21	No external assessment/certification obligations.

A BRIEF NOTE ON FEDRAMP

Currently 80% of cloud service provider applications for FedRAMP authorization are for the Moderate impact level, which is prescribed for situations "where the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals," and "[s]erious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or physical."[6] FedRAMP baselines are based on NIST SP 800-53, and cybersecurity regulations that address the handling of CUI through commercial cloud services will reference FedRAMP. On March 24, 2025, the General Services Administration launched FedRAMP 20x.[7] FedRAMP 20x presently has announced primary goals that include automation validation, continuous monitoring, improved relationships with industry, and more.[8] FedRAMP 20x does not presently change its use of the FedRAMP Revision 5 baseline for new authorizations.[9]

CONCLUSION

As federal agencies move toward a unified cybersecurity framework, contractors must carefully study and understand the requirements and differences in the cybersecurity regulations.

DFARS 252.204-7012 remains the most stringent of the cybersecurity regulations, with mandatory third-party certification and strict reporting obligations. Meanwhile, the FAR proposed rule introduces a more aggressive eight-hour reporting window that may set a new government-wide standard. DOD contractors are arguably best situated to adjust to any new government-wide standards for nonfederal information systems, whereas non-DOD contractors will have a steeper learning curve. Any way you look at it, cybersecurity requirements are, or are soon to be, a competitive necessity for all government contractors, and all government contractors will be well served by devoting the time and attention necessary in order to understand, apply, and comply with these requirements. Below, for your convenience, we have provided a simple summary comparison chart of some of the cybersecurity aspects discussed in this blog.

Key Takeaways: Contractors should:

- review contracts to ensure that they understand how systems are being characterized and which standards apply;
- assess their current cybersecurity compliance posture against applicable NIST frameworks and agency-specific cybersecurity requirements;
- prepare for incident reporting variations, including complying with the proposed FAR rule's shorter timelines; and
- monitor upcoming FAR rule changes, as such changes may introduce additional certification or assessment requirements.

Comparison of Selected Federal Cybersecurity Requirements

---

[1] Covered Defense Information is defined in DFARS 252.204-7012 and is, in summary, unclassified controlled technical information or other Controlled Unclassified Information (CUI) that requires safeguarding or dissemination controls.

[2] FAR 52.204-21 defines *Federal contract information* as information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites) or simple transactional information, such as information necessary to process payments.

[3] Some definitions in FAR 52.204-21 are proposed for change in the new FAR CUI Rule.

[4] FedRAMP is a government-wide program that evaluates and authorizes commercial cloud services for use by federal agencies. Under FedRAMP's evaluation scheme, commercial cloud service offerings can be authorized to handle data at either the Low, Moderate, or High impact level. The impact levels are based on the "potential impact on an agency's assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction." As cloud services offerings move up in authorization level, the security requirements become more strict.

[5] DHS requires contractors to obtain an Authority to Operate, prior to collecting, processing, storing, or transmitting CUI, which will include completing a security authorization process and satisfying additional requirements. *See, e.g.*, HSAR 3052.204-72(h); *see also* DHS Policy Directive 4300A and Security Authorization Process Guide. *Available at* https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

[6] *Understanding Baselines and Impact Levels for FedRAMP Authorizations*, Federal Risk and Authorization Management Program (last accessed April 3, 2025), https://www.fedramp.gov/rev5/baselines/ .

[7] https://www.gsa.gov/about-us/newsroom/news-releases/gsa-announces-fedramp-20x-03242025

[8] https://www.fedramp.gov/20x/

[9] https://www.fedramp.gov/20x/faqs/

7 Min Read

Authors

William T. Kirkwood

Lawrence S. Sher

Michael Hill

Related Topics

Cybersecurity | FAR | United States Department of Defense | U.S. Department of Homeland Security | Compliance

Related Capabilities

Government Investigations, Enforcement & Compliance | Government Contracts & Grants

Related Professionals

William T. Kirkwood

Lawrence S. Sher

Michael Hill

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.