wiley

ALERT

# Updates on Cybersecurity Requirements for Government Contractors

November 21, 2024

Part of the Biden Administration's push to enhance U.S. cybersecurity capabilities has focused on imposing new requirements on government contractors. The 2023 National Cybersecurity Strategy suggested, for example, that "[c]ontracting requirements for vendors that sell to the federal government have been an effective tool for improving cybersecurity." Efforts to add new mandates for government contractors continued at pace over the past year, including on secure software development and cyber incident reporting.

This alert notes two developments over the past week that government contractors should be aware of:

**1) NIST Seeks Comment on Enhanced Security Requirements for Protecting Controlled Unclassified Information**

On November 13, the National Institute of Standards and Technology (NIST) issued for public comment the initial public draft of its Special Publication (SP) 800-172r3 (Revision 3), *Enhanced Security Requirements for Protecting Controlled Unclassified Information (CUI)*. SP 800-172 Revision provides recommended cybersecurity controls for CUI on a nonfederal information system when associated with a "high value asset" or "critical program." These requirements supplement NIST's SP 800-171 Revision 3, which was updated in June 2024, and are intended to be read in concert with NIST 800-171 Revision 3. SP 800-172 requirements are selected and imposed by federal agencies on certain contractors. Of note, the Cybersecurity Maturity Model Certification 2.0 (CMMC) program intends to incorporate certain SP 800-172 Revision 2 requirements for contractors subject to CMMC Level 3.

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Joshua K. Waldman
Associate
202.719.3223
jwaldman@wiley.law


## Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance
Strategic Competition & Supply Chain

In this update, NIST adds three new "families" of requirements for consistency with SP 800-171 Rev. 3: Planning, System and Services Acquisition, and Supply Chain Risk Management.

- **Planning**: Expands and identifies specific new controls for security architecture development and supplier diversity.
- **System and Services Acquisition**: Incorporates an expanded discussion of the potential need to enhance the trustworthiness of mission-critical systems.
- **Supply Chain Risk Management**: Adds several new controls or practices, including notification agreements between contractors and suppliers and anti-tampering or-counterfeiting procedures.

The draft SP 800-172 is open for comment through **January 10, 2025**.

**2) DOD Codifies Certain Exemptions for Commercially Available Off-the-Shelf (COTS) Items**

Those monitoring the Federal Register may have noticed that on November 15, the DOD published a final rule mentioning several cybersecurity-related requirements. The rule updates the list of solicitation provisions and contract clauses that are not applicable to COTS purchases. Notably, the rule confirms that five DFARS clauses related to cybersecurity requirements do not apply to COTS purchases: DFARS clause 252.2047012, Safeguarding Covered Defense Information and Cyber Incident Reporting; DFARS provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements; DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements; DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements; and DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls. This action provides helpful clarity and limits the application of these complex information security regimes, but was not a surprise, as it fulfills a statutory requirement to publish a list of existing rules that do not apply to COTS purchases.

**Supply Chain and Cybersecurity Remain in the Spotlight: What Can Organizations Do to Prepare?**

Last week's regulatory activities affirm that supply chain risk and cybersecurity remain top of mind. In addition to revisions to the NIST Cybersecurity Framework 2.0 (February 2024) and NIST SP 800-171 Rev. 3 to more broadly incorporate cybersecurity supply chain risk management issues, regulators have begun to seek to require cybersecurity supply chain actions among their regulated entities:

- The Defense Department released a proposed rule seeking that prospective contractors disclose foreign access to software code.
- The Transportation Security Administration will require cybersecurity supply chain actions among their regulated entities (TSA's recent Notice of Proposed Rulemaking for cybersecurity risk management for the rail, pipeline, and over-the-road bus industries proposes notification requirements between regulated entities and their suppliers).
- The FAR Council continues work on FAR case 2023-002, *Supply Chain Software Security*, that would implement Executive Order 14028, which requires suppliers of software available for purchase by agencies to comply with, and attest to complying with, secure software development requirements.

Contractors should continue to evaluate their supply chains and determine whether, and how, to obtain information from suppliers and subcontractors as needed to fulfill contractual requirements for disclosure and supply chain hygiene.

Our team will continue to monitor these and other developments.