Website: **https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171**

# Policy - Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 204.73

## Regulatory

**Interim DFARS Rule - Assessing Contractor Implementation of Cybersecurity Requirements (85 FR 61505)**

Interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

- Federal Register

## Policy / Guidance

**Contractual Remedies to Ensure Contractor Compliance with Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, for contracts and orders not subject to Clause 252.204-7020; and Additional Considerations Regarding National Institute of Standards and Technology Special Publication 800-171 Department of Defense Assessments, dated June 16, 2022**

This memorandum reminds contracting officers of the importance of protecting controlled unclassified information on contractor information systems and provides strategies they may employ if a contractor fails to comply with Defense Federal Acquisition Regulation Supplement clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting.” It also clarifies use of Medium or High National Institute of Standards and Technology Special Publication 800-171 Department of Defense Assessments.

- DPC Policy Vault

**DPC Memo - Interim Defense Federal Acquisition Regulation Supplement Rule, 2019-D041, Assessing Contractor implementation of Cybersecurity Requirements, dated November 25, 2020**

This memorandum emphasizes the requirements and ensures the workforce is aware of interim DFARS rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, which was published in the Federal Register (85 FR 61505) on September 29, 2020, and is effective on November 30, 2020.

- DPC Policy Vault

**DPC Memorandum - Supplier Performance Risk System for National Institute of Standards and Technology Special Publication 800-171 Department of Defense Assessment, dated July 1, 2020**

The Supplier Performance Risk System's (SPRS) assessment methodology has been updated for contractors and subcontractors implementing the security requirements in National Institute of Standards and Technology Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. These updates to SPRS include a virtual review capability for high risk assessments, usually performed on site, to protect assessors and Defense Industrial Base personnel by limiting travel and exposure.

- DPC Policy Vault

**USD(A&S) Memorandum - Assessing Contractor Implementation of Cybersecurity Requirements, dated November 14, 2019**

Provides standard DoD-wide methodology for assessing DoD contractor implementation of the security requirements in NIST SP 800-171.

- DPC Policy Vault

**USD(A&S) Memorandum - Strategically Implementing Cybersecurity Contract Clauses, dated February 5, 2019**

Directs development of a standard methodology to recognize industry cybersecurity readiness at a strategic level.

- USD A&S Memorandum

**USD(A&S) Memorandum - Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review, dated January 21, 2019**

Addresses leveraging DCMA's CPSR process to review contractor procedures for the flow down of DoD CUI and for ensuring compliance with DFARS Clause 252.204-7012 and NIST SP 800-171.

- USD A&S Memorandum

**ASD(A) Memorandum - Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base, dated December 17, 2018**

Provides program offices and requiring activities with sample Statement of Work (SOW) language to support development of cybersecurity measures designed to enhance existing protection requirements provided by DFARS Clause 252.204-7012.

- USD A&S Memorandum

**DPC Memorandum - Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**

OUSD(A&S) Memorandum, dated November 6, 2018

- DPC Memorandum

**DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented, dated November 6, 2018**

Provided to: Enable the consistent review of System Security Plans and Plans of Action when such plans are required by the solicitation or contract to be provided to the Government; Address the impact of 'not yet implemented' security requirements on a contractor's unclassified internal information system; Provide clarification on implementing NIST SP 800-171 security requirements.

- DoD Guidance

**Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System, dated November 6, 2018**

Provides a framework of actions that can be tailored by a program office/requiring activity, commensurate with program risk, to assess the contractor's approach to providing adequate security to protect the Department's controlled unclassified information.

- DoD Guidance

## NIST SP 800-171

**NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations**

The publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry. The requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI, or that provide protection for such components.

- NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

**NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information**

This publication provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

- NIST SP 800-171A Assessing Security Requirements for Controlled Unclassified Information

**NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1, June 24, 2020**

Documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012. Updates made to rev 1.2 dated June 10, 2020: Section 4) updated to

address changes made due to COVID-19 and Annex B updated to address changes made in the Supplier Performance Risk System (SPRS).

- NIST SP 800-171 DoD Assessment Methodology

**Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73, PGI Subpart 204.73, DFARS Subpart 239.76 and PGI Subpart 239.76**

The document addresses questions related to, Safeguarding Covered Defense Information and Cyber Incident Reporting.

- DoD Procurement Toolbox FAQs

## Other

**Factsheet - DFARS Case 2019-D041 Assessing Contractor Implementation of Cybersecurity Requirements**

- Factsheet

**Factsheet - The Use of the Supplier Performance Risk System (SPRS) in Implementing DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements**

- Factsheet

## Helpful Links

**Department of Defense Procurement Toolbox**

- DoD Procurement Toolbox