

DFARS 252.204-70XX

DFARS 252.204-70xx requires DoD contractors to implement cybersecurity controls and report incidents to protect covered defense information.



What it is

U.S. DFARS 252.204-70xx is a set of cybersecurity clauses within the Defense Federal Acquisition Regulation Supplement that require contractors working with the U.S. Department of Defense to safeguard controlled unclassified information and report cyber incidents. These clauses establish minimum standards to strengthen cybersecurity risk management practices across the defense supply chain.

Issued by the U.S. Department of Defense, DFARS 252.204-70xx applies to defense contractors and subcontractors handling sensitive government data. The clauses specifically address requirements for implementing security controls, incident reporting, and ensuring compliance with the NIST SP 800-171 standard for protecting information systems.

At a glance

PUBLISHER	TYPE	VERSION
U.S. Department of Defense (DoD)	Regulation	DFARS clauses (regulation-type references) do not include explicit version numbers or revision identifiers. Instead, they are typically identified by their issuance or revision dates embedded within their titles. Based on the available data: - **DFARS 252.204-7012** — "Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024)" ([acquisition.gov] (https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.?utm_source=openai)) - **DFARS 252.204-7018** — "Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (JAN 2023)" ([acquisition.gov] (https://www.acquisition.gov/dfars/252.204-7018-prohibition-acquisition-covered-defense-telecommunications-equipment-or-services.?utm_source=openai)) - **DFARS 252.204-7025** — "Notice of Cybersecurity Maturity Model Certification Level Requirements (NOV 2025)" ([acquisition.gov] (https://www.acquisition.gov/dfars/252.204-7025-notice-cybersecurity-maturity-model-certification-level-requirements.?utm_source=openai)) Therefore the

How SmartSuite supports DFARS 252.204-7012

DFARS Clause Control Library

Structure DFARS cybersecurity clauses and associated NIST 800-171 controls with mapped implementation tasks and owners.

Controlled Unclassified Information (CUI) Governance

Track systems, data flows, and environments handling CUI to maintain regulatory compliance.

System Security Plan and POA&M Management

Maintain System Security Plans and Plan of Action & Milestones with remediation tracking.

Vulnerability Remediation and Incident Reporting

Track vulnerability remediation and coordinate incident reporting to the Department of Defense.

Supplier and Subcontractor Cybersecurity Oversight

Monitor subcontractor compliance with DFARS cybersecurity requirements and flow-down obligations.

Contract Compliance and Audit Reporting

Provide dashboards showing control implementation status, open remediation items, and readiness for defense cybersecurity assessments.

Common framework mappings

CMMC 2.0

FAR 52.204-21

FedRAMP Rev. 5

ISO 27001:2022

NIST CSF 2.0

NIST 800-171 Rev. 3

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

DFARS 252.204-7008 Compliance Clause

Defines requirements for safeguarding covered defense information in nonfederal systems.

acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses

DFARS 252.204-7012 Safeguarding Clause

Outlines safeguarding requirements and incident reporting for defense contractors.

acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses

NIST SP 800-171

Defines the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems.

csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Frequently asked questions

What is DFARS 252.204-70xx used for?

DFARS 252.204-70xx cybersecurity clauses are used to ensure adequate protection of Controlled Unclassified Information (CUI) within the Department of Defense (DoD) supply chain. These clauses mandate specific cybersecurity requirements for defense contractors and subcontractors handling DoD information systems or data.

Is compliance with DFARS 252.204-70xx required?

Yes, DFARS 252.204-70xx clauses are mandatory for organizations contracting with the U.S. Department of Defense when the contract involves CUI. Non-compliance can result in penalties, contract termination, or loss of eligibility for future DoD contracts.

Who does DFARS 252.204-70xx apply to?

DFARS 252.204-70xx applies to all DoD contractors and subcontractors who store, process, or transmit Controlled Unclassified Information as part of DoD contracts. This includes organizations of all sizes across the defense industrial base.

What key cybersecurity practices or artifacts are required by DFARS 252.204-70xx?

The clauses require contractors to implement the security controls specified in NIST SP 800-171, conduct system security assessments, and develop System Security Plans (SSPs) and Plans of Action and Milestones (POA&Ms). Regularly reporting cyber incidents and maintaining audit logs are also required.

How can organizations implement DFARS 252.204-70xx requirements?

Organizations should perform a gap analysis against NIST SP 800-171 controls, document deficiencies in POA&Ms, and develop a comprehensive SSP. Implementation also involves continuous monitoring, staff training, and establishing incident response processes.

How does DFARS 252.204-70xx relate to other cybersecurity frameworks?

DFARS 252.204-70xx is directly aligned with NIST SP 800-171, as its controls are the foundation of the regulation. It also complements broader frameworks like the Cybersecurity Maturity Model Certification (CMMC), which incorporates DFARS requirements into its levels.

How would SmartSuite support DFARS 252.204-70xx?

SmartSuite helps organizations manage DFARS 252.204-70xx by enabling risk tracking, mapping and monitoring NIST SP 800-171 controls, and maintaining evidence collections for audits. It provides tools for managing POA&Ms, tracking incident reports, and producing real-time compliance and readiness reports to support audit preparedness.

License included / downloadable: Yes DFARS 252.204-70xx clauses are published by the U.S. Department of Defense and are publicly available via the Defense FAR Supplement on [acquisition.gov](https://www.acquisition.gov). License included with platform

Full framework page and mappings: smartsuite.com/frameworks/dfars-252-204-70xx-defense-federal-acquisition-regulation-supplement-cybersecurity-clauses