SmartSuite

Framework / Cybersecurity / CMMC

DFARS 252.204-70XX

DFARS 252.204-7012 requires DoD contractors to protect covered defense information with NIST SP 800-171 and report cyber incidents within 72 hours; related clauses add SPRS scores and CMMC.



What it is

DFARS 252.204-7012 is the contract clause that requires Department of Defense (DoD) contractors to protect covered defense information on their systems with NIST SP 800-171 and to report cyber incidents to DoD within 72 hours of discovery. It is written into solicitations and contracts under the Defense Federal Acquisition Regulation Supplement (DFARS), has applied since the final rule of October 21, 2016, and flows down to subcontractors.

At a glance

PUBLISHER
Defense Acquisition Regulations System (DARS), U.S. Department of Defense

TYPE
Regulation

VERSION
Clause 252.204-7012 (MAY 2024); 252.204-7019 and -7020 (NOV 2023); 252.204-7021 and -7025 (NOV 2025)

EFFECTIVE
October 21, 2016 (final rule); clause revision MAY 2024

DOMAIN
Cybersecurity

FAMILY
CMMC

REGION
United States

INDUSTRY
Aerospace & Defense

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Why it matters

- **A defined data scope** Covered defense information is unclassified controlled technical information or other CUI that is marked in the contract or handled in support of it (paragraph (a)).
- **A named control set** Covered systems must meet NIST SP 800-171 in effect when the solicitation is issued, or as the contracting officer authorizes (paragraph (b)(2)(i)).
- **A 72-hour clock** "Rapidly report" means within 72 hours of discovery of any cyber incident that affects a covered system or its data (paragraphs (a) and (c)).
- **Evidence that must be kept** The contractor preserves images of affected systems and packet capture data for at least 90 days from the incident report (paragraph (e)).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports DFARS 252.204-7012

Covered Systems and CDI Register

List each covered contractor information system, the contracts it supports and the covered defense information it handles (paragraph (a)).

NIST SP 800-171 Requirement Library

Assign an owner, implementation status and evidence to each requirement and record variance requests to the contracting officer (paragraph (b)(2)).

Assessment Score Tracking

Record the Basic, Medium or High assessment date, score out of 110 and SPRS posting, and flag assessments approaching three years old (252.204-7019 and -7020).

Incident Reporting Workflow

Time each incident from discovery against the 72-hour clock, capture the DIBNet report number and medium assurance certificate holder (paragraph (c)).

Evidence Preservation Log

Track image and packet capture preservation for 90 days, malware submissions and forensic access requests (paragraphs (d) to (f)).

Subcontractor Flow-Down

Record which subcontracts carry the clause, each subcontractor's variance notices and incident numbers, and CMMC levels flowed down (paragraph (m) and 252.204-7021).

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 does DFARS 252.204-7012 require?

It requires contractors to provide adequate security on covered contractor information systems, meeting NIST SP 800-171 in effect when the solicitation is issued (paragraph (b)(2)), and to report cyber incidents within 72 hours of discovery (paragraph (c)). It also requires preserving images for 90 days and flowing the clause down to subcontractors.

What is covered defense information?

It is unclassified controlled technical information or other CUI that is marked or identified in the contract, or collected, developed, received, transmitted, used or stored by the contractor in support of the contract (paragraph (a)). Public information without restriction is excluded.

How do contractors report a cyber incident?

They report through the DoD DIBNet portal and need a DoD-approved medium assurance certificate (paragraph (c)). Any malicious software they isolate is submitted to the DoD Cyber Crime Center, not to the contracting officer (paragraph (d)).

 © 2026 SmartSuite Inc. All rights reserved.

What are DFARS 252.204-7019 and -7020?

They require a current NIST SP 800-171 assessment, not more than three years old, with the summary score posted in the Supplier Performance Risk System. A Basic Assessment is a contractor self-assessment, while Medium and High assessments are conducted by the Government.

How does CMMC relate to DFARS 252.204-7012?

DFARS 252.204-7021 and provision 252.204-7025 require a CMMC status at the level the solicitation names, under 32 CFR part 170. They sit beside 252.204-7012 rather than replace it, and the CMMC rule has applied in contracts since November 10, 2025 in phases.

License included / downloadable: Yes The clauses are U.S. federal regulation published free by the Defense Acquisition Regulations System on acquisition.gov and are included with the platform for reference.

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