DoD Compliance, Explained: NIST 800-53 Rev 4, 800-171, and CMMC

To secure Department of Defense (DoD) and other government contracts, organizations must demonstrate compliance with specific frameworks that help protect federal contract information (FCI) and controlled unclassified information (CUI), such as CMMC 2.0 and NIST SP 800-171. NIST SP 800-53 rev 4[1] provides a complementary framework, but it's not mandatory like the other two. Still, SP 800-53 substantially informs and maps to SP 800-171 and CMMC 2.0.

Differentiating Between NIST 800-53 Rev 4, 800-171, and CMMC

The US government's cybersecurity compliance frameworks can be incredibly confusing due to regular revisions and nebulous mapping. To simplify the relevant compliance frameworks for organizations seeking contracts disbursed by the DoD, your shortlist of relevant compliance frameworks should include:

- NIST Special Publication 800-53 (SP 800-53)
- Cybersecurity Maturity Model Certification (CMMC 2.0)
- NIST Special Publication 800-171 (SP 800-171)
- NIST Special Publication 800-172 (SP 800-172)

Below, we'll decipher these frameworks for DoD compliance and their relationships, prioritizing the comprehensive yet often misunderstood National Institue for Standards and Technology's SP 800-53.

Note that NIST SP 800-53 rev 4[2] was withdrawn on September 23, 2021, having been replaced by NIST SP 800-53 rev 5.

Ultimately, the only compliance framework currently required for DoD contractors is Cybersecurity Maturity Model Certification (CMMC) 2.0. Per the DoD, compliance is mandatory by fiscal year 2026.

Understanding the DoD Compliance Developments Over Time

Until the release of the CMMC, the DoD required organizations within the defense industrial base (DIB) to self-report their compliance with NIST SP 800-171's 110 Requirements (both Basic and Derived). This compliance process was mandated under Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7019 regarding the protection of federal contract information (FCI) and controlled unclassified information (CUI).

---

[1] Spelling/Capitalization/Grammar to match provided SEO keywords.
[2] Spelling/Capitalization/Grammar to match provided SEO keywords.

Then, the DoD released the Cybersecurity Maturity Model Certification (CMMC) framework in January 2020. It's overseen by the Office of the Under Secretary of Defense for Acquisitions and Sustainment (OUSD(A&S)) and the Cyber AB—formerly known as the CMMC Accreditation Body (CMMC-AB).

This action established a new benchmark for DoD compliance while integrating SP 800-171 in full for CMMC Level 2 compliance. SP 800-172 was similarly incorporated into CMMC Level 3 compliance, although not in its entirety.

Per DFARS clause 252.204-7021, contractor organizations must maintain a valid CMMC certificate:

- Not older than three years
- Throughout the contract's duration

However, in late 2021, the DoD suddenly announced the revision and consolidation of the CMMC. Version 2.0 significantly condensed the grouping of stipulated controls and requirements from five to three Levels, largely to remove or ease contractors' compliance burden.

So, where does SP 800-53 fit into this compliance structure and timeline?

What is NIST SP 800-53?

The National Institute of Standards and Technology's Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, is an industry-agnostic compliance framework intended to establish organizations' baseline information security controls. It's among the most robust NIST frameworks and, having been initially released in 2005, its five revisions have informed those required for compliance like CMMC 2.0.

Although most pertinent to organizations earning and holding government contracts, the guidance contained within SP 800-53 is ubiquitously applicable.

As mentioned above, the current version—revision 5—has replaced the NIST SP 800-53 rev 4, Control Families[3] and all.

[3] Spelling/Capitalization/Grammar to match provided SEO keywords.

Overview of NIST SP 800-53

NIST SP 800-53 comprises 20 Control Families. Each Family is designated by a two-letter abbreviation and groups relevant controls—referred to as "Base Controls." The controls stipulate the process or capability that an organization must implement to safeguard FCI and CUI.

Each Base Control in the framework is expanded upon by:

- **Discussions** — Providing further context, considerations, and examples of a given control
- **Related Controls** – Other controls with relevant implementation considerations
- **Control Enhancements** – Augmentations to implemented Base Controls

If a given control contains brackets, then the organization retains some choice in how they implement it. Brackets containing “Assignments” allow more custom implementation, whereas “Selections” provide a limited list of options from which organizations can choose. Furthermore, controls can be implemented multiple times and in different ways to accommodate additional policies, scenarios, or narrower scopes.

NIST SP 800-53 Control Family Breakdown

The 20 Control Families of SP 800-53 are:

- **AC** – “Access Control,” which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. AC pertains to the access privileges and activities of users, and the Family includes:
    - 25 Base Controls
    - 108 Control Enhancements

- **AT** – “Awareness Training,” which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. AT pertains to security program training and policy documentation, and the Family includes:
    - Six Base Controls
    - 10 Control Enhancements

- **AU** – “Audit and Accountability,” which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. It also somewhat maps to the “System and Information Integrity” Domain and Requirement Family. AU pertains to internal processes for logging and reviewing system activities, and the Family includes:
    - 16 Base Controls

    - 41 Control Enhancements

- **CA** – "Assessment, Authorization, and Monitoring," which largely maps to the CMMC's "Security Assessment" Domain and the equivalent SP 800-171 Requirement Family. CA pertains to the security assessments, monitoring, and response, and the Family includes:
    - Nine Base Controls
    - 17 Control Enhancements

- **CM** – "Configuration Management," which largely maps to the CMMC's Domains of the same name, "Asset Management," and "Risk Management." It also maps to 800-171's "Configuration Management" Requirement Family. CM pertains to the establishment of baseline security configurations, and the Family includes:
    - 14 Base Controls
    - 42 Control Enhancements

- **CP** – "Contingency Planning," which largely maps to the CMMC's "Recovery" Domain and SP 800-171's "Media Protection" Requirement Family. CP pertains to an organization's recovery processes following a cybersecurity incident, and the Family includes:
    - 13 Base Controls
    - 37 Control Enhancements

- **IA** – "Identification and Authentication," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. IA pertains to the verification of user identities, and the Family includes:
    - 12 Base Controls
    - 43 Control Enhancements

- **IR** – "Incident Response," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. IR pertains to the execution of predetermined response plans following a cybersecurity incident and relevant training. The Family includes:
    - Nine Base Controls
    - 31 Control Enhancements

- **MA** – "Maintenance," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. MA pertains to maintaining the other SP 800-53 control implementations and other organizational security efforts. The Family includes:
    - Seven Base Controls

    - 21 Control Enhancements

- **MP** – "Media Protection," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. MPpertains to practices for organizing, storing, and transmitting various media types. The Family includes:
    - Eight Base Controls
    - 12 Control Enhancements

- **PE** – "Physical and Environmental Protection," which largely maps to the CMMC's "Physical Protection" Domain and the equivalent SP 800-171 Requirement Family. PE pertains to safeguards against natural disasters and physical threats. The Family includes:
    - 23 Base Controls
    - 29 Control Enhancements

- **PL** – "Planning," which largely maps to the CMMC's "Security Assessment" Domain and the equivalent SP 800-171 Requirement Family. PL pertains to the coordination of an information security program and its ongoing management. The Family includes:
    - 11 Base Controls
    - Three Control Enhancements

- **PM** – "Program Management," which somewhat maps to the CMMC "Situational Awareness" and "Risk Management" Domains and the equivalent SP 800-171 Requirement Families. PM also pertains to the coordination of an information security program, but more specifically to the roles and personnel involved with its oversight. The Family includes:
    - 32 Base Controls
    - Five Control Enhancements

- **PS** – "Personnel Security," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. PS pertains to the practices an organization adopts to safeguard its people, and the Family includes:
    - Nine Base Controls
    - Eight Control Enhancements

- **PT** – "PII Processing and Transparency," which is one of the few SP 800-53 Control Families that does not correlate to the other DoD compliance frameworks. PT pertains to safeguarding Personally Identifiable Information separate from data categorized as FCI or CUI. The Family includes:

    - Eight Base Controls
    - 13 Control Enhancements

- **RA** – "Risk Assessment," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. RA pertains to an organization's ability to identify, assess, and prepare for reasonably anticipated threats. The Family includes:
    - 10 Base Controls
    - 13 Control Enhancements

- **SA** – "System and Services Acquisition," which somewhat maps to the CMMC "System and Communications Protection" Domain and the equivalent SP 800-171 Requirement Family. SA pertains to safeguarding resource allocation, service delivery, and the systems responsible for both. The Family includes:
    - 15 Base Controls
    - 90 Control Enhancements

- **SC** – "System and Communications Protection," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. SC pertains to safeguarding network connections and data (either transmitted across them or at rest). The Family includes:
    - 47 Base Controls
    - 92 Control Enhancements

- **SI** – "System and Information Integrity," which largely maps to the same CMMC Domain and SP 800-171 Requirement Family. SI pertains to an organization's efforts to ensure systems and data remain free of malicious or accidental manipulation and compromise. The Family includes:
    - 22 Base Controls
    - 78 Control Enhancements

- **SR** – "Supply Chain and Risk Management," which is one of the few SP 800-53 Control Families that does not correlate to the other DoD compliance frameworks. SR pertains to safeguarding third-party partnerships against vulnerabilities. The Family includes:
    - 12 Base Controls
    - 15 Control Enhancements

The list above presents control mapping from SP 800-53 to CMMC 2.0 and SP 800-171. However, reversing the mapping direction helps clarify why SP 800-53 is an important DoD framework despite not being mandatory.

Almost every single CMMC Practice maps to SP 800-53. So if you implement the latter, you'll have virtually implemented CMMC 2.0. And as SP 800-171 is included within CMMC 2.0 at Level 2, you'll also have implemented that framework. Likewise, achieving Level 3 will require implementing some SP 800-172 controls.

But an SP 800-53 implementation with 308 total Base Controls and 1,310 Control Enhancements should be considered a rigorous undertaking. As a result, it's best conducted by partnering with an experienced cybersecurity and compliance firm like [CLIENT REDACTED].

What is NIST SP 800-53b?

SP 800-53 is further supplemented by SP 800-53b, *Control Baselines for Information Systems and Organizations.* The supplemental guidance outlines control baselines, which provide organizations with tailored groupings of SP 800-53 controls according to categories such as:

- Threat information
- Mission or business requirements
- Types of systems
- Sector-specific requirements
- Specific technologies
- Operating environments
- Organizational assumptions and constraints
- Individuals' privacy interests
- Laws
- Executive orders
- Regulations
- Policies
- Directives
- Standards
- Industry best practices

Control baselines are divided between "Security Control Baselines" and "Privacy Control Baselines." Security control baselines are ascribed differentiated by levels (i.e., low-impact, moderate-impact, high-impact) depending on the correlating result should systems' confidentiality, integrity, or availability be compromised.

You can leverage SP 800-53b to perform a partial implementation of relevant SP 800-53 controls.

Achieving DoD Compliance

As mentioned above, NIST SP 800-53 is *not* required for DoD compliance; only CMMC 2.0 is. So, how does an organization seeking DoD contracts—or preferred contractor status—demonstrate CMMC 2.0 compliance?

Your CMMC implementation must be assessed and verified by an official "Certified Third-Party Assessor Organization" (C3PAO), like [CLIENT REDACTED].

The only exception is the Level 1 self-assessment of 17 practices, required annually. But organizations looking to take on more substantial DoD contracts will need to prove Level 2 or 3 compliance.

The timelines for Levels 2 and 3 are:

- **Level 2** – Triennial third-party assessments for critical national security information and annual self-assessments for some information security program efforts

- **Level 3** – Triennial government-led assessments

Unfortunately, CMMC 2.0 compliance is not a "set and forget" process. You'll need to update your certification every three years to remain eligible for DoD contracts.

Ensure DoD and Government Compliance with [CLIENT REDACTED]

Adhering to regulatory compliance frameworks is challenging enough without the constant changes and revisions that DoD contractors experience. For obligatory frameworks like CMMC 2.0, you'll have to partner with an approved third party.

But compliance doesn't start and stop with third-party assessment. [CLIENT REDACTED] will help you rethink your CMMC, NIST SP 800-171, and NIST SP 800-53 compliance to streamline and simplify your ongoing, triennial efforts.

Contact us today to learn more about our compliance services—which span CMMC 2.0, HIPAA, PCI DSS, SOC2, and more!

Sources:

DFARS. *Part 252 - Solicitation Provisions and Contract Clauses.* https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS-252.204-7019

National Institute of Standards and Technology. *National Institute of Standards and Technology.* https://www.nist.gov/

NIST. *NIST SP 800-53.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. *NIST SP 800-53b.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

OUSD A&S. *Acquisition and Sustainment*. https://www.acq.osd.mil/

US Department of Defense. *DOD to Require Cybersecurity Certification in Some Contract Bids.* https://www.defense.gov/News/News-Stories/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/