DoD Cybersecurity Requirements: Tips for Compliance

blog.netwrix.com/2022/09/28/dod_cyber_security_requirements

Kevin Joyce

The IT systems and data of the Department of Defense (DoD) and its network of contractors are a matter of national security. Accordingly, the DoD maintains cybersecurity requirements that organizations must meet in order to be an approved vendor for the DoD.

This article provides an overview of the most pertinent documents that inform the DoD's cybersecurity expectations for defense industrial base (DIB) organizations, a review of useful frameworks, and tips for implementing DoD requirements.

Handpicked related content:

[Free Guide] CMMC 2.0 Compliance Starter Checklist

What are the DoD's cybersecurity requirements?

The requirements for cybersecurity can be found in the following three documents, which support and reference each other:

- **Defense Federal Acquisition Regulation Supplement (DFARS) —** Clause 252.204-7012 outlines the expectations for cyber hygiene for DIB organizations.
- **NIST 800-171 —** Based on DFARS, NIST 800-171 provides detailed guidelines for companies to assess their cybersecurity practices.
- **CMMC —** The CMMC provides a clear plan for DIB organizations to attain the cyber hygiene certification required to be an approved DoD vendor.

DFARS

DFARS states the requirements for companies that conduct business with the Department of Defense. Cybersecurity is covered under clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."

What types of data must be protected?

The DoD's cybersecurity requirements protect two main types of digital and physical records: Controlled Unclassified Information (CUI) and Federal Contract Information (FCI)

CUI includes the following:

- Personally identifiable information (PII)
- Proprietary Business Information (PBI)
- Unclassified Controlled Technical Information (CTI)
- For Official Use Only (FOUO)

FCI includes the details of a contract between the government and an organization. FCI does not include information that is already public knowledge (like that on government websites) or transactional information. PCI is never intended for public release.

Organizations that want to work with the DoD need to be able to identify the CUI and FCI they store and process, so they can protect it in accordance with DoD requirements.

Who needs to be compliant?

While the DoD's standards provide useful guidelines for cybersecurity in general, they are a requirement for some businesses. Any contractor working with the DoD that stores, processes or circulates CUI must comply with DFARS standards. This includes ensuring that all unclassified DoD data is protected with proper safeguards, minimizing system vulnerabilities and potential consequences of a breach, and implementing good incident reporting practices.

NIST 800-171

In response to DFARS, the National Institute of Standards and Technology (NIST) developed NIST 800-171 to provide a detailed breakdown of cyber hygiene best practices. Specifically, NIST 800-171 is designed to help DoD contractors protect CUI data. It does not cover protection for FCI data.

NIST 800-171 control families

NIST 800-171 breaks down security controls into the following 14 families:

Control Family	Description
1. Access Control	Monitor all access events within a system, and limit each user's access to systems and data to the minimum required to do their job.
2. Awareness and Training	Ensure staff receives sufficient training on security policies, practices and risks appropriate to their access privilege. Train regularly so users are prepared to respond to threats.
3. Audit and Accountability	Maintain proper audit logs, log management practices and audit reporting. Limit access to auditing systems.
4. Configuration Management	Configure hardware and software to restrict access to nonessential features and programs and prevent unauthorized software installation.
5. Identification and Authentication	Prevent unauthorized use of systems by implementing multifactor authentication (MFA) and strong password policies.
6. Incident Response	Develop and test procedures to ensure prompt detection and response threats.

Control Family	Description
7. Maintenance	Perform system maintenance to prevent CUI disclosure. Monitor employees, prevent offsite use of devices with CUI, and check media for malicious code.
8. Media Protection	Control access, protection and disposal of media that contain CUI. Use cryptography to protect digital data.
9. Physical Protection	Prevent hardware, software, networks and data from physical damage by limiting access and maintaining audit logs
10. Personnel Security	Monitor users' activity, especially around shifts in personnel.
11. Risk Assessment	Perform vulnerability testing of systems and frequently evaluate the potential risks to your organization.
12. Security Assessment	Define system boundaries and implement a plan to reduce vulnerabilities. Refine security requirements frequently.
13. System and Communications Protection	Secure the communication of CUI. Use separate networks or subnetworks for unprotected information, and set defaults to deny network communications (whitelisting).
14. System and Information Integrity	Quickly identify system flaws. Immediately respond to security breaches and system errors. Update security software as soon as new versions are released.

More details on the NIST 800-171 controls can be found here.

Handpicked related content:

[Free Guide] Achieve NIST SP 800-171 with Netwrix solutions

NIST updates

NIST 800-171 was created in 2015 and receives periodic updates. Each time an update occurs, contractors have a set amount of time to achieve compliance with the new regulations or risk losing their approved vendor status with the DoD.

CMMC

While the DFARS clause outlines best practices for enterprise cybersecurity, the Cybersecurity Maturity Model Certification (CMMC) assesses the quality of an organization's cybersecurity programs and provides a set of certifications attesting to this quality. These certifications standardize the approval of DoD vendors. CMMC certifications apply to both FCI and CUI data.

Who does CMMC apply to?

CMMC standards apply to all organizations that receive funding from the DoD to conduct business or provide services. Referred to as the defense industrial complex, this includes over 300,000 organizations that provide goods or services for the DoD.

CMMC timeline

Virtually anyone who has followed the evolution of the CMMC has questions about the timeline. After version 1.0 and the subsequent “interim rules” for the CMMC, the second version of the certification was released in November 2021. However, it has not gone into effect; CMMC 2.0 is still in the rule-making process, which could take up to two years.

This does not mean the certification standards should not be a priority for companies. Contractors are prioritizing compliance with the new standards within their supply chains in hopes of getting ahead. Compliance with CMMC 2.0 will also align your company with the NIST 800-171 guidelines.

CMMC compliance levels

The DoD made several changes between CMMC 1.0 and 2.0 to simplify compliance levels. The first version had five levels with varying standards of assessments. In version 2.0, there are three levels of CMMC compliance, depending on the type of data and intensity of the contract with the DoD. The different levels have different expectations for assessments. Refer to the chart below for more detail on the CMMC 2.0 compliance levels.

Level	Assessment Type	Who Must Comply
Level 1. Foundational	Annuaself-assessmentsl self-assessments	Companies dealing with FCI only
Level 2. Advanced	Third-party assessments every three years and annual self-Third-party assessmentsassessments	Companies that handle CUI
Level 3. Expert	Additional government-led assessments every three years	Specified in individual DoD contracts

How to comply with the CMMC

Adhering to the CMMC requires compliance with the 17 sets of standards. These include the 14 control families from NIST 800-171 reviewed above and the following three additional groups:

Additional Area	Description
Recovery	Create a recovery plan in the event of a data breach or loss.

Additional Area	Description
Situational Awareness	Understand your IT environment in order to efficiently learn about cyber threats and respond to them appropriately.
Asset Management	Identify assets, particularly CUI data, and define your procedures for handling and classifying those assets.

For support, download this CMMC compliance starter checklist.

DoD Frameworks

As a deputy CIO or CISO for a DoD-affiliated organization, you may find the requirements of DFARS, NIST and the CMMC to be overwhelming. But a wealth of resources are available to help you achieve DoD cybersecurity compliance, such as this compilation of reference material. Below, we provide useful resources to help you with many critical aspects of compliance.

Developing a cybersecurity strategy

Organizations should create a 4–5 year cybersecurity strategy that enables them to modify processes and implement controls. The following resources can help you create a solid cybersecurity strategy:

- **NIST SP 800-37** — Provides a risk management framework
- **NIST SP 800-39** — Provides guidance on managing information security risk
- **DODD 8000.01** — A directive to give responsibility for information resource management to your DoD CIO

Building defensible networks

Building a defensible network requires implementing monitoring, automation, threat detection and incident response tools and processes. The following resources can help:

- FIPS 199 — Provides standardized categories for federal information systems based on their risk level, which can help you establish priorities for your security strategy
- FIPS 200 – Defines minimum security requirements depending on the level of risk of information, and explains the process for selecting security controls based on the risk level of your information
- NIST SP 800-53 — Provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting appropriate controls

Establishing critical infrastructure protection

Critical infrastructure protection (CIP) refers to a comprehensive strategy of creating resilient systems, networks and databases. This includes harm prevention and data protection as well as incident mitigation, response and recovery. There are many resources for CIP plans and policies that can support CIOs and CISOs. For example, the ISA/IEC 62443 standards provide security tools and best practices for asset owners, service providers and suppliers.

Managing access

The following resources can help you properly manage access to your data, applications and other IT assets:

- NIST SP 800-60 — Informs access management practices by providing guidance for categorizing information as CUI and controlling who has access to it
- NIST SP 800-133 — Helps you protect sensitive data using approved cryptographic algorithms

Sharing information

Sharing information about cyber threats and attackers is crucial to bolstering cybersecurity. The following resources can help.

DoD Cyber Exchange — Provides guidance and training for cyber professionals inside and outside the DoD

Building a cybersecurity workforce

The following resources can help you in onboarding, qualifying and managing people who work in IT or cybersecurity:

- NIST SP 800-16 — Provides concepts for IT security training in modern cyberspace while allowing flexibility for future software and technologies
- NIST SP 800-100 — Provides guidance for managers on establishing an information security program

Tips on staying cyber secure

The National Cybersecurity and Communication Integration Center (NCCIC) has compiled seven key strategies for getting started in complying with the DoD's cyber hygiene standards:

- **Use application whitelisting (AWL)** — Define a list of approved software and block everything else. This is far more effective than attempting to blacklist every unwanted application.
- **Practice proper configuration and patch management —** Implement secure baseline configurations and promptly correct any drift. Ensure that critical updates are applied in a timely manner.

- **Reinforce your network security —** Minimize the potential points of entry for attackers, and segment your network into multiple enclaves to quarantine attackers.
- **Implement multifactor authentication —** Use MFA, especially for accounts with privileged access to CUI.
- **Secure remote access —** Control remote access using MFA and operator-controlled and time-limited standards. Regularly look for hidden back doors that could allow attackers to gain remote access to a system.
- **Constantly monitor systems —** To speed threat detection and response and ensure accountability, implement continuous monitoring with threat intelligence for IP traffic at ICS boundaries, IP traffic within the network and admin account activity.
- **Establish and regularly test an incident response plan —** Create a comprehensive response plan for security incidents. Response actions can include disconnecting all devices from the internet, disabling specific accounts, isolating network segments, conducting a malware search, and immediately requiring a password reset. Test and revise the plan periodically.
- **Develop a cybersecurity scorecard according to DoD standards and frameworks** — A scorecard will help you measure your progress toward stronger cybersecurity.

How Netwrix can help

Achieving and maintaining compliance with the DoD's cybersecurity standards is necessary to a place on the government's approved vendor list. Netwrix solutions offer a holistic approach to cybersecurity challenges by securing your organization across all the primary attack surfaces: data, identity and infrastructure.

Learn more about our top solutions:

- Data access governance — Reclaim control over access to sensitive data.
- Active Directory security — Secure your , on premises and in the cloud, from end to end.
- Ransomware protection — Mitigate the risk of ransomware infections and catch attacks in progress.
- Privileged access management — Slash the risk from privileged activity.
- Information governance — Make your data organized, discoverable and more secure.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.