Why NIST 800-171 & CMMC Policies Matter For Your Business

TechRounder PDF Edition

Live article: https://www.techrounder.com/business/why-nist-800-171-cmmc-policies-matter-for-your-business/

By Vipin PG | Published April 18, 2025 | Updated January 8, 2026 | Format: Explainer | 4 min read

In brief

Many businesses view cybersecurity compliance from a regulatory standpoint and would only comply with relevant cybersecurity requirements to avoid noncompliance penalties.

Many businesses view cybersecurity compliance from a regulatory standpoint and would only comply with relevant cybersecurity requirements to avoid noncompliance penalties.

But when it comes to NIST 800-171 and CMMC policies, compliance goes beyond aligning your company on the right side of the law. In this article we are checking what NIST 800-171 and CMMC is, and how adhering to these cybersecurity compliance standards may benefit your organization.

Introducing NIST 800-171

NIST (the National Institute of Standards and Technology) standards are a set of protocols and procedures designed to encourage compliance with various government regulations. A United States agency developed these controls under the same name.

NIST standards are particularly targeted at federal entities, although any organization can implement them. NIST 800-171 is a subset primarily concerned with protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations.

While optional, adopting NIST 800-171 ensures that non-federal contractors safeguard the confidentiality of controlled unclassified information in their systems. The framework contains 110 security controls spread across 14 control families. Among the focus areas include access control, cyber awareness and training, routine audits, and incident response.

About CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity assessment framework developed by the US Department of Defense (DoD). It requires defense vendors to fulfill certain controls with a view to safeguarding the defense supply chain from unforeseen cyber-attacks.

CMMC fosters compliance with various NIST standards. The program specifically controls how Defense Industrial Base (DIB) companies handle two types of federally-designated sensitive information - Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

The recently released CMMC framework has three levels, down from five in its previous iteration.

NIST 800-171 and CMMC - Exploring Similarities and Differences

NIST 800-171 and CMMC are designed to safeguard critical infrastructures from advanced cybersecurity risks. The primary difference is that compliance with NIST 800-171 is optional but mandatory for CMMC.

Remember that CMMC is based on NIST standards. The program aligns with NIST 800-171 and 800-172 controls. So, while NIST doesn't impose mandatory compliance in and of itself, organizations seeking CMMC certification may need to comply with NIST 800-171 standards.

NIST 800-171 compliance specifically applies to CMMC Level 2, while both NIST 800-171 and 800-172 compliance are required for Level 3 certifications.

Reasons to Consider NIST 800-171 and CMMC Compliance

1. Required By Law

NIST 800-171 compliance may be optional. However, aspiring defense vendors must adhere to CMMC controls under their respective maturity levels.

Earlier CMMC iterations emphasized compliance for prime contractors. However, according to the recently unveiled CMMC framework, all DIB companies will be required to meet the relevant CMMC protocols regardless of their size.

2. Offers Lucrative Business Opportunity

Prospective defense suppliers must comply with CMMC protocols to be considered for any contract. Noncompliance can have you knocked off the merit list, forfeiting what could have been a lucrative business opportunity.

Fulfilling NIST 800-171 and CMMC requirements for your cybersecurity certification level can provide a critical incentive when bidding for defense tenders.

3. Guards Against Penalties

Getting disqualified from defense tenders is devastating enough. However, existing vendors have more stringent penalties to contend with.

The Department of Defense can immediately terminate your contract for CMMC non-compliant companies. Moreover, your business may be slapped with punitive fines, jail terms, or both.

4. Bolsters Your Systems' Security

Although many regard NIST 800-171 and CMMC compliance as a preserve of federal contractors, any organization can adhere to the controls outlined in these frameworks to bolster its cyber hygiene.

Note that obtaining CMMC certification is a process that involves scoping your organization for gaps and vulnerabilities. By leveraging the insights from these audits, you can better understand your cybersecurity posture and update your cyber policy templates accordingly.

5. Reinforces Personal Accountability

NIST 800-171 and CMMC Level 1 call for annual self-audits. Obligating companies to self-affirm ensures every DIB player is accountable for securing the defense supply chain.

Nonfederal players may also take advantage of annual self-audits to identify and thwart threats across their supply chains.

6. Helps Avert Reputational Damage

Adhering to NIST 800-171 and CMMC controls can safeguard your business's reputation in two ways.

First, compliance is a significant step towards warding off major cyber-attacks. This can endear more clients to your business, translating to increased revenues.

Besides, fulfilling NIST 800-171 and CMMC requirements protects your company from noncompliance penalties. It prevents undue operational downtimes caused by business disruptions, which could erode consumer confidence in your brand.

7. Proactive Threat Monitoring

Cyber threats are constantly lurking in the shadows. Sometimes, dropping your guard for a minute is all it takes for a breach to occur.

Implementing NIST 800-171 and CMMC guidelines allows you to detect threats proactively and respond more decisively to breaches. It also lets your business streamline the cybersecurity assessment process, reducing the financial burden of unscheduled audits.

Further, regular NIST 800-171 and CMMC assessments allow you to stay ahead of emerging regulatory trends in the constantly evolving cybersecurity landscape.

Conclusion

Adhering to NIST 800-171 and CMMC protocols can cushion your business from noncompliance fees, which could cripple your operations depending on the severity of the infraction.

Complying with NIST 800-171 and CMMC frameworks provides a competitive advantage. It prequalifies your company for lucrative federal tenders, allowing you to enjoy operational continuity while your competitors grapple with noncompliance disruptions.

Remember, both NIST 800-171 and CMMC programs are constantly changing. Keeping abreast of recent developments is necessary to adjust your cybersecurity frameworks accordingly.

References

1. complianceforge.com - nist-800-171-cmmc-policy-templates - https://complianceforge.com/nist-800-171-cmmc-policy-templates/

2. dodcio.defense.gov - cmmc / About - https://dodcio.defense.gov/cmmc/About/