eBook

CMMC Compliance: What the NIST?

SteelCloud

SteelCloud

The Department of Defense's CMMC (Cybersecurity Maturity Model Certification) program has undergone multiple changes, revisions, updates, and organizational shifts. Even among multiple deadline shifts, the directive remains clear: CMMC requires contractors, system integrators, and others in the defense industrial base (DIB) to secure their networks according to established controls and checklists, then demonstrate that security.

The CMMC program is focused on protecting sensitive DOD data held by government contractors. CMMC Level Two—the compliance level most of the DIB will need to maintain—requires companies to meet 110 controls on handling controlled unclassified information (CUI) from NIST Special Publication 800-171.

CUI is at the foundation of everything CMMC. You need to worry about everything that processes (or could process) CUI and anything that stands between your system and the internet/physical user or threat. While practicing good cyber hygiene could result in greater profit for your organization, that is not the goal. The goal is to protect CUI. And chances are good, if you are a government contractor, you handle, store or protect CUI.

What CMMC compliance means for the DIB.

The CMMC program suggested for the DIB is focused on protecting sensitive DoD data that is handled or managed by government contractors.

"Day one, not everybody will be required to have a certification to handle CUI. It's going to be a phased-in approach," Bostjanick said. "We have promised to make sure companies would not end up in a scenario where [they] can't get a certification but [they] want to participate in a contract."

Another aspect of CMMC certification the DIB may want to prepare for is DFARS 7020. It requires contractors to provide the Government access to its facilities, systems, and personnel any time the Department of Defense (DoD) is renewing or conducting a medium or high assessment.

Why COMPLY?

Cybersecurity policy compliance is always in your best interests.

There has been a recent increase in the number of commercial organizations mandated or have voluntarily chosen to standardize on the Center for Internet Security (CIS) or STIG benchmarks as cybersecurity best practices. But updating and making sure you are compliant is not enough.

In most cases, updating, vulnerability scanning, and configuration management processes are individually managed to match the underlying technologies. However, the devil is truly in the details, such as specific controls and compliance requirements set against each type of infrastructure. And then, there is ongoing management and maintenance of your secure baseline to prevent compliance drift.

But cybersecurity is not just about compliance and a secure baseline. It's about resiliency, too. While a cybersecurity strategy can help prevent a data breach or reduce the risk of malicious activity, a cyber resilience strategy helps specifically mitigate the impacts of these attacks. Cyber resilience is aimed at continuously delivering the intended outcome, despite the attack. It mitigates the risks and severity of attacks and includes practices such as Zero Trust and continuous diagnostics and mitigation (CDM) for good management configuration.

The upshot is that it shows your government clients you value and understand their security needs and are willing to go the extra mile for the sake of security. As Brian Hajost, COO of SteelCloud, says, "Compliance puts a halo around your proposal" and moves it to the top of the stack.

If that doesn't get your attention, this will.

The Justice Department recently announced a $9 million settlement in a case against a federal contractor accused of misrepresenting their compliance with cybersecurity requirements under the False Claims Act. Deputy Attorney General, Lisa Monaco, says that most contractors "follow all of the contract terms," but if they fail to follow required standards or misrepresent their efforts, the new Civil Cyber-Fraud Initiative will use the False Claims Act to enforce civil fines on government contractors and grant recipients.

This settlement puts contractors and cloud service providers on notice to cross their t's and dot their i's regarding FedRAMP, FISMA/RMS, or CMMC accreditation. It's important to know the difference between these mandates.

Is FedRAMP required for CMMC? And how does FedRAMP fit into the DIB supply chain? In short, cloud providers that provide security need to meet CMMC requirements, but they do NOT need FedRAMP authorization. Only clouds that store processes or transmit CUI need FedRAMP accredition. So how do you get there?

NIST SP 800-53

NIST SP 800-53 makes the "how" a priority.

NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, is easily one of the most foundational documents in modern cybersecurity. And it provides a good start for cloud services providers to become FedRAMP compliant. While many frameworks define goals and requirements, SP 800-53 defines the specific controls to deliver on those goals. And while many standards focus on "what" organizations should do, SP 800-53 defines the "how."

The document emphasizes firmware—monitoring firmware integrity, controlling over firmware configurations and vulnerabilities, and actively managing their supply chain and technology vendors to ensure they are compliant.

Prepare for your FedRAMP accreditation.

FedRAMP accreditation is not only required for cloud providers who handle CUI, but customers inside the government and out are more inclined to trust a provider who has complied with FedRAMP guidelines and is viewed as secure enough to conduct business with organizations the DoD. So FedRAMP is a good decision for your cloud services, regardless of the information you handle.

A recent revision, Rev 5, has changed the number of controls to meet for accreditation. The High baseline will go from 421 controls to 392 controls, the Moderate baseline will go from 325 controls to 304 controls, and the Low and Li-SaaS baselines will increase to 150 controls.

Get help from STIG & CMMC crosswalk documents.

Whether your company needs to be FedRAMP certified or CMMC compliant, system hardening is the foundation of securing systems and documenting compliance activities. If you're an organization that wants to leverage the FedRAMP work you've put into your infrastructure, you will also want to leverage NIST SP 800-53 controls toward your CMMC certification. To validate your CSP, you can also use FedRAMP compliance and their NIST SP 800-53 control mapping to validate their maturity level.

STIGs are at the foundation of NIST 800-53. However, STIGing can be a very time-consuming and resource-draining process. Automating those processes saves time, resources, and the morale, of your IA team. To enable NIST compliance readiness, we've created a series of STIG & CMMC Control Crosswalk documents to assist in the Cybersecurity Maturity Model Certification (CMMC) compliance effort, specific to the controls.

NIST SP 800-172

NIST SP 800-172 takes compliance up another notch.

While most in the DIB handling CUI will be seeking Level 2 CMMC certification, some will need to seek Level 3 certification—for those handling CUI on the DoD's most sensitive programs. For Level 2, you must align with the 110 controls of NIST SP 800-171. Many in the DIB have been doing that for years, but the new CMMC process for certification now requires a self-assessment.

For Level 3, however, you need to align with all those same controls, plus additional ones from NIST SP 800-172. You will also need to submit a third-party audit. Being audit-ready and achieving third party-verified compliance with DFARS and NIST 800 involves much more than documentation. Receiving accreditation cost-effectively for your organization is paramount. Understanding the relationship between NIST and CMMC and having a well-defined Plan of Action & Milestone (POAM) by leveraging automation will shorten your compliance efforts.

First things first—identify vulnerabilities.

They say the first step is the hardest. But with cybersecurity, it doesn't have to be as hard as you think.

The first step is to identify vulnerabilities in your system. You may do this through a regular internal system review, or you may be informed by a third party during an audit. The easy part is that you can scan for issues using an automated solution like SteelCloud's aConfigOS that works in any environment and remediates the issues, which is your second step.

The goal is to create a secure baseline from which to operate. Maintaining endpoints is critical because every time you update configurations, install a security patch or purchase a new server, your system can fall out of compliance. The baseline acts as a fallback position—a configuration you know works while sorting out the details of the new configuration.

Every time you update, you can automate the remediation of any issues that crop up. Automation reduces your operational costs and downtime while ensuring system stability over time. It also removes a huge and annoying burden from the shoulders of your IA staff.

NIST SP 800-172

Meeting CMMC assessment criteria with POAMs.

So, you've scanned and remediated, but maybe not all your controls have been met. You can still operate, but you need a plan of action for when and how you will remediate.

Software applications are rarely designed to operate in government and commercial organizations with mandated compliance requirements, so they get stuck on the starting line, waiting months for the authority to operate (ATO). POAMs and waivers provide additional flexibility to organizations by allowing a plan of actions and milestones (POAM) and a waiver process that can waiver certification on a limited basis and in mission-critical instances. In that way, POAMs accelerate timelines, objectives and CMMC security requirements.

Reporting is a critical component of your cybersecurity efforts.

NIST 800-172 and its advanced CUI protections build on the basic requirements of NIST 800-171 and include three mutually supportive and reinforcing components:

- ✓ **Penetration-resistant architecture (PRA)**
- ✓ **Damage-limiting operations (DLO)**
- ✓ **Designing for cyber resiliency and survivability**

These measures require continual scanning and remediation of your system, as well as careful documentation of your efforts. But, again, automation provides the means for doing all of the above quickly and error-free.

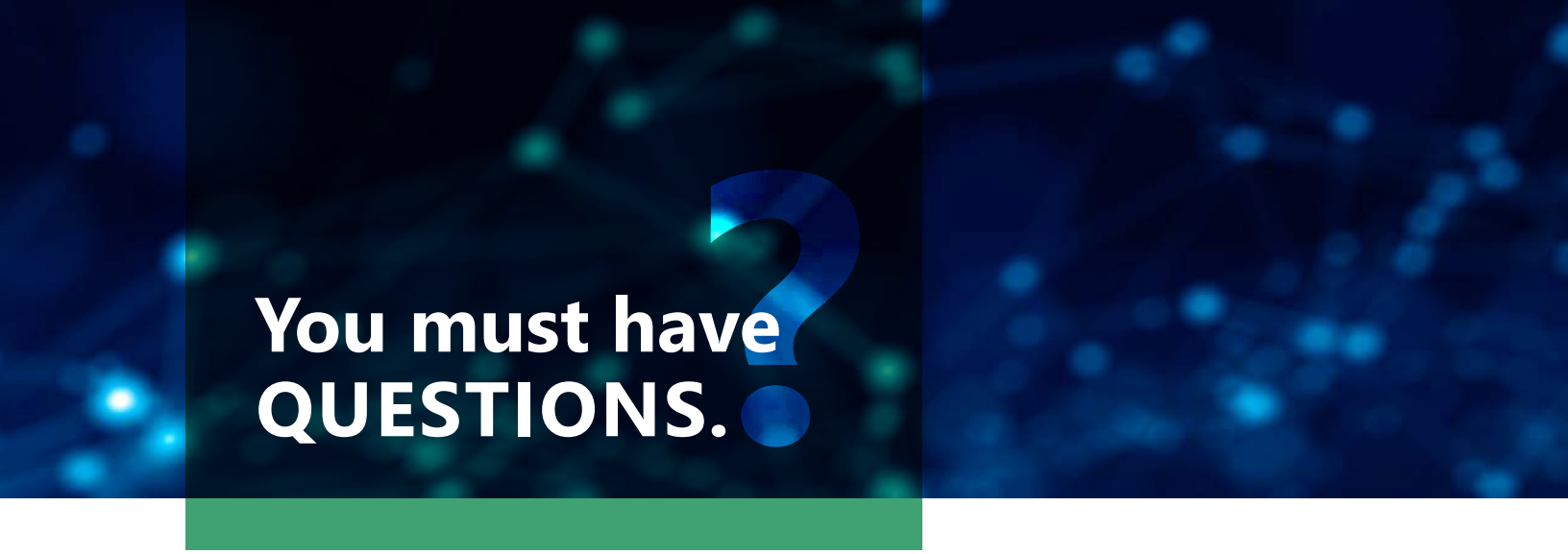
Get HELP

Putting it all together into a cohesive cybersecurity roadmap.

All you need to do is seamlessly knit together regulations, cybersecurity standards, and best practices to meet each CMMC maturity level and reduce your risk against threats. By next summer. **Clear as mud?** Here are some tools that can help:

1. NIST 800-128 outlines the National Checklist Program (NCP) that helps you find the specific controls you need to target to get your organization and its products and services secure and compliant
2. Security Technical Information Guides (STIG) and Center for Information Security (CIS) controls are long-established pathways to help you get where you need to go
3. Automation is key to achieving compliance in a timely, affordable manner. SteelCloud's ConfigOS is the STIG and CIS hardening and automation standard in the DoD, and 8 out of the top 10 system integrators use it. It can accomplish what it would take qualified engineers weeks or months to do…in just an hour

You will need specialists to understand all the best practices, how they interlink and how to identify all the controls. But, with automation, you won't need a whole team of them to make you compliant and keep you that way. And, even if you start tomorrow, you can easily beat any deadline and show your customers you are just as proactive and dedicated to cybersecurity as they are.



What is CUI?

CUI is the term used to cover a category of data that isn't classified but still needs protection. This can be any personally identifiable information, proprietary business information, "For Official Use Only" information, legal information, and more. In other words, it's data that others can act on and use to wind their way into government systems. NIST SP 800-172 provides a set of enhanced security protocols for protecting the "confidentiality, integrity, and availability of CUI in nonfederal systems and organizations from the persistent threat when the CUI is associated with a critical program or high-value asset."

The DoD estimates that over $600B in critical information is exfiltrated from official networks each year. Therefore, the protection of CUI is not the government acting out of an abundance of caution. Instead, it's the government's goal to protect our national assets and to thwart increasingly sophisticated cyberattacks and data breaches that impact their systems, the defense industrial base (DIB), and the privacy of those with whom they do business.

Where does CUI originate?

You may have noticed "CUI" in the banner and footer to indicate the document contains controlled, unclassified information on documents, emails, and other media.

The Defense Counterintelligence and Security Agency (DCSA) indicates that "anyone can create CUI as long as it is generated for, or on behalf of, an Executive Branch agency under a contract, and it falls into one of the over one hundred DOD CUI categories. CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government-wide policies. It can be a piece of note paper or even a conversation.

The best answer is "it depends," do you use an in-house network only, or do you utilize the "cloud (other people's computers), do you have remote employees, do you allow WIFI access to the corporate environment, do you allow users to access all email via their phone, do employees get issued laptops or do they bring in their own device. It's messy and really depends on the nature of your environment.

At the end of the day, you, as their partner, are helping them protect and handle data correctly.

NIST SP 800-171 reduces the controls contractors need to implement to harden their systems, become CMMC compliant, and protect CUI. Agencies are required to use NIST SP 800-171 for all nonfederal information systems. Its use will also be incorporated into the CUI FAR clause. This grounds technology protections in an existing standard (moderate confidentiality) that most agencies were already applying, and most contractors were already required to meet and provides much-desired clarity and streamlining for contractors, via NIST SP 800-171, as we see increased cyber threats.

Is FIPS 140-2 still required?

For CMMC and FedRAMP requirements, the Federal Information Processing Standard 140-2 (FIPS 140-2) crypto requirements are still required to meet mandates. FIPS is a cryptography standard that non-military U.S. federal agencies, government contractors, and service providers must comply with to work with any federal government entities that collect, store, transfer, share, and disseminate sensitive but unclassified (SBU) information like CUI.

What about the DFARS 7020 NIST 800-171 DoD assessment requirement?

Defense Federal Acquisition Regulation Supplement 7020 (DFARS 7020) requires contractors to provide access to their facilities, systems, and personnel any time the DoD is renewing or conducting a medium or high assessment. It is a set of restrictions for the origination of raw materials intended to protect the US defense industry from the vulnerabilities of being overly dependent on foreign sources of supply. Contracting professionals are expected to be aware of these requirements.

Is there any way to simplify and speed CMMC certification?

CMMC certification isn't just one thing. It comes in many flavors, depending on the amount of CUI you handle, whether you meet cryptography standards, and what level of DFARS assessment you require. And CUI requirements are essential to meeting CMMC requirements and complying with the NIST SP 800-171 controls and checklists that secure your system against attack.

SteelCloud is a leader in CMMC and the many flavors of compliance. Our ConfigOS is used by most of the DoD and 8 of the Top 10 system integrators to automate compliance with NIST SP 800-171. SteelCloud's ConfigOS software reduces the time, cost, and effort it takes to harden around an application stack. It makes meeting CMMC compliance much more manageable. And it protects you from costly fines for non-compliance.

What about collecting SIEM and eMASS data?

SteelCloud's ConfigOS features SIEM 2.84 capabilities, creating bulk STIG Viewer checklists and integrating human and machine controls into data feeds for eMASS and Splunk integration. With data presented through ConfigOS DashView, this integration dramatically reduces the time spent monitoring, detecting, and maintaining your enterprise's DISA STIG or CIS Benchmark infrastructure hardening compliance. And SteelCloud's ConfigOS keeps you in compliance, preventing configuration drift. When all is said and done, ConfigOS reduces the effort to harden an endpoint by 90% and remediate and maintain an endpoint by 70%.

Automation is the industry standard when it comes to compliance.

Automation is the key to making security compliance a more efficient and affordable process, particularly when hardening government-mandated STIG and CIS controls. Yet, some are still doing the same things the same way while encountering the same recurring problems repeatedly. After all, it's familiar and how it has always been done. And if configuration management and compliance weren't so important and increasingly complex and demanding, that would be fine. But as demands grow, so does the need for an automated helping hand.

Members of the DIB that handle sensitive information are continually vulnerable to adversarial attacks. It is a known fact that the protection of Controlled Unclassified Information (CUI) in non-federal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government. So get a head start and go back to NIST 171 and streamline the process of creating a hardened system with STIG automation, in preparation for CMMC. Security compliance is critical to reducing risk and protecting CUI at all costs. Automation makes achieving compliance on all 110+ controls for CMMC Level Two and Level Three faster and more efficiently.

ConfigOS is proven to speed compliance with multiple government mandates, such as STIG and CIS, each incorporating NIST SP 800-171 components and some from 172. They are similar and, in most cases, have more stringent mandates than CMMC. So ConfigOS has you covered as you move through the accreditation and CMMC certification process that will secure your enterprise, enhance your government relationships, and protect CUI.

ConfigOS reduces the effort to harden an endpoint by 90% and remediate and maintain an endpoint by 70%.

Next STEPS

Automate what you can to make shorter work of CMMC compliance.

Cybersecurity and supply chain attacks are increasing every year. And fines are steep for misrepresenting your compliance. So, don't give the government reason to cite you.

Automation is the key to making security compliance a more efficient and affordable process, when hardening government-mandated STIG and CIS controls. Yet, some are still doing the same things the same way while encountering the same recurring problems repeatedly. After all, it's familiar and how it has always been done. And if configuration management and compliance weren't so important and increasingly complex and demanding, that would be fine. But as demands grow, so does the need for an automated helping hand.

SteelCloud's approach to configuration management is automated. ConfigOS was built from the ground up specifically to address every phase of DevOps security and in every type of environment, from air gap classified environments to regular on-prem environments to the cloud. Furthermore, it is purpose-built, to attain authority to operate (ATO) and maintain it over time, scanning and remediating endpoints 24/7.

If managing your compliance efforts is using too many resources or taking too much time—or if you haven't even gotten off the ground—contact SteelCloud and get on the pathway to compliance today!

Automation is the key to making security compliance a more efficient and affordable process, when hardening government-mandated STIG and CIS controls.

About ConfigOS

SteelCloud's ConfigOS software is currently implemented in hundreds of commercial and government organizations. Use cases for ConfigOS range from business, cloud, SCADA, and weapon systems. ConfigOS scans and remediates hundreds of system-level controls in minutes. In addition, automated remediation rollback, comprehensive compliance reporting and SIEM dashboard integration, are provided. ConfigOS was designed to harden hundreds of system-level controls around an application stack in about 60 minutes - typically eliminating weeks or months from the RMF accreditation timeline. ConfigOS addresses Microsoft Windows workstation and server operating systems, SQL Server, IIS, IE, Chrome, and all of the Microsoft Office components. The same instance of ConfigOS addresses CISCO network devices, Apache, Red Hat Enterprise 5/6/7/8, SUSE, CENTOS, Ubuntu, and Oracle Linux.
Learn more at https://www.steelcloud.com/configos-cybersecurity/.

About SteelCloud

SteelCloud develops STIG and CIS compliance software for government and commercial customers. Our products automate policy and security remediation by reducing the complexity, effort, and expense of meeting government security mandates. SteelCloud has delivered security policy-compliant solutions to enterprises worldwide, simplifying implementation and ongoing security and compliance support. SteelCloud products are easy to license through our GSA Schedule 70 contract. SteelCloud can be reached at (703) 674–5500 or info@steelcloud.com. Additional information is available at www.steelcloud.com, or contact Jamie Coffey at jcoffey@steelcloud.com.

SteelCloud
20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**