ninjaOne® | FedRAMP®

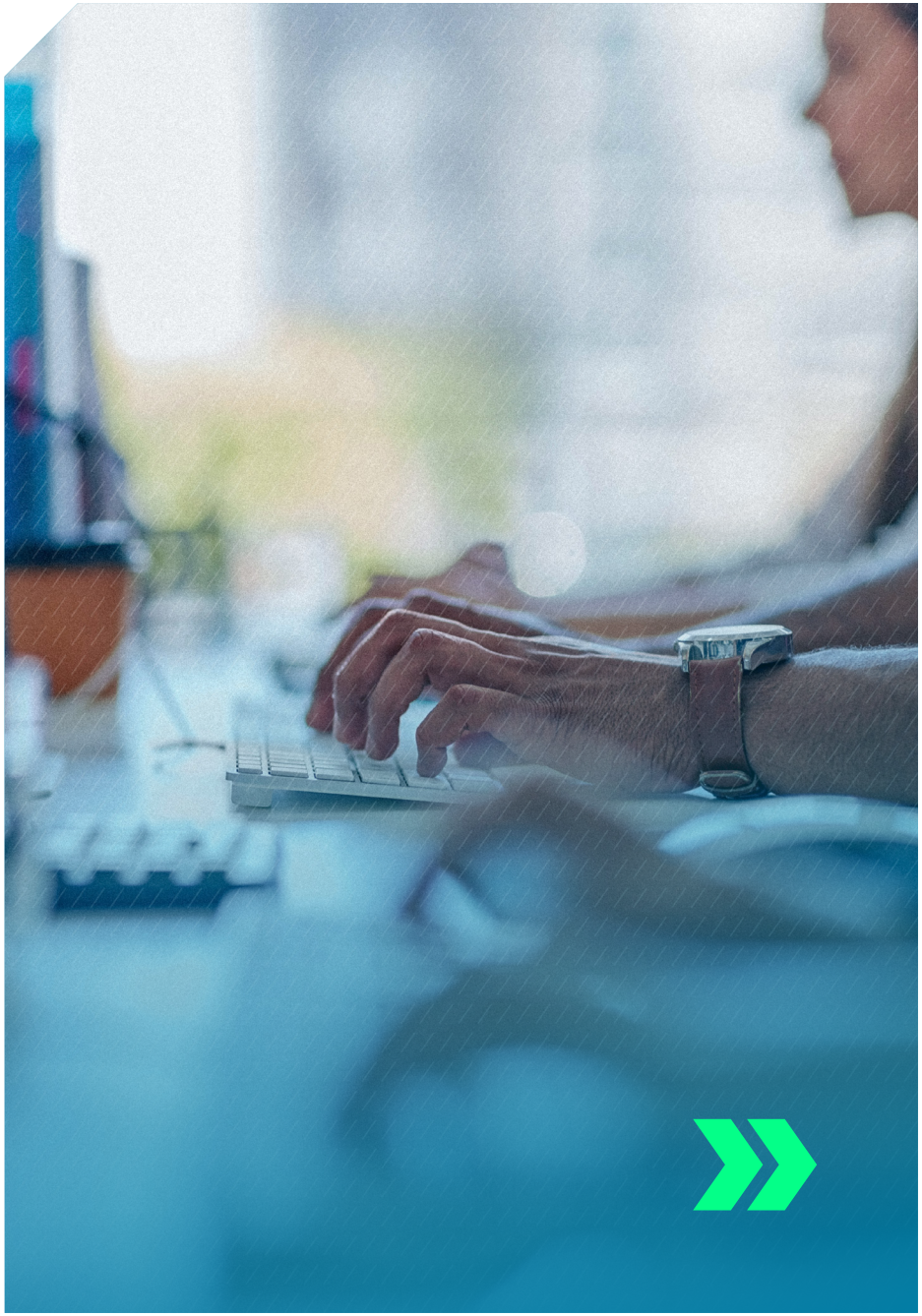
The NinjaOne Guide to CMMC

Cybersecurity Model Maturity Certification

Strengthening cyber resilience for the Defense Industrial Base (DIB)

Table of contents

Table of contents	2
Introduction	3
What Is CMMC?	5
Managing cybersecurity risk	6
Protecting against cyber attacks	8
Detecting security incidents	10
Minimizing incident impact	11
Conclusion	12



Introduction

In October 2024, the Defense Department published the Cybersecurity Maturity Model Certification (CMMC) final program rule that organizations in the Defense Industrial Base (DIB) can use to evaluate and improve their cybersecurity posture. It outlines security controls that federal contractors must have in place to protect Federal Contracting Information (FCI) and Controlled Unclassified Information (CUI).

Effective November 2025, the Pentagon's finalization of the Cybersecurity Maturity Model Certification (CMMC) rule represents a historic turning point in U.S. defense contracting. By embedding enforceable cybersecurity requirements directly into contracts, the Department of Defense is raising the bar for every vendor in its supply chain. No longer an aspirational framework, CMMC is now a contractual mandate that compels organizations to prove their ability to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). For contractors, this shift means that cybersecurity readiness is no longer a competitive differentiator; it is the baseline for participation in the defense industrial base, underscoring the growing reality that security and compliance are inseparable from doing business with the government.

It's important to understand that the CMMC is a framework to verify and validate compliance with existing Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) provisions. The CMMC is not a separate set of rules, nor is it the requirement in and of itself. It aligns with NIST SP 800-171/172

and formalizes verification. Additionally, the phase-in period for the CMMC does not relieve federal contracting organizations of compliance with the data protection rules that are already in FAR/DFARS. (FedNews Network)

CMMC reinforces existing Defense Department cybersecurity requirements to protect sensitive unclassified information shared with contractors and subcontractors. It ensures that companies handling this information meet appropriate security standards through a tiered certification model (see table on page 5). Each tier in the model requires progressively advanced protections based on the data's sensitivity and is verified through assessments that are mandatory for contract eligibility.

NinjaOne directly supports key controls required by CMMC such as patch management, endpoint visibility, backup, and reporting as well as monitoring, security, data protection, documentation. Because NinjaOne is delivered in a FedRAMP environment, customers gain the assurance of government-grade security and a simpler path to adoption — making NinjaOne an 'easy button' for agencies working toward CMMC readiness.

FULL DEPLOYMENT
IN LESS THAN
30 days

TECHNICIAN PROFICIENCY
IN LESS THAN
10 days

U.S.-BASED WITH FEDRAMP
CUSTOMERS SUPPORTED
100 %
ON U.S. SOIL

What is CMMC?

Most organizations will begin their journey at Level 2, which represents broad protection of CUI.

CMMC Model	Model	Assessment	Requirements
LEVEL 1 Basic safeguarding of FCI	**15 requirements** aligned with FAR 52.2024-21	+ Annual Self Assessment + Annual Affirmation	+ Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.
LEVEL 2 Broad protection of CUI	**110 requirements** aligned with NIST SP 800-171 R2	+ C3PAO certification assessment every 3 years, or + Self assessment every 3 years for select programs + Annual Affirmation	+ Either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation. + Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems. + Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.
LEVEL 3 Advanced protection of CUI (with third-party assessment)	**134 requirements** (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	+ DIBCAC certification assessment every 3 years + Annual Affirmation	+ Achieve CMMC Status of Final Level 2. + Undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). + Provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.

CMMC Authorization vs. Certification

Authorization is a self-assessment process demonstrating that an organization meets the DoD's requirements for protecting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). **Certification** is the formal, third-party validation of that compliance by an accredited Certified Third-Party Assessment Organization (C3PAO).

Managing cybersecurity risk

Managing cybersecurity risks includes governance, risk management, asset visibility, and supply chain security. Let's look at how each of these factors contribute to effective management of cybersecurity risks.

Governance

Using the CMMC guidelines, an organization should evaluate its governance framework and revise it as needed to provide effective IT and cybersecurity leadership, accountability, and risk policy that aligns to the CMMC guidelines.

NinjaOne enables organizations to implement a comprehensive cybersecurity governance policy by providing visibility, control, and proactive management of security risks across their IT infrastructure.

+ Vulnerability management provides comprehensive vulnerability tracking and reporting
+ Policy management allows IT teams to create granular security policies for efficient device management
+ Reporting and monitoring tools provide detailed security reports, device health status tracking, and more
+ Additional security features include support for MFA and IAM frameworks

Managing cybersecurity risk *(continued)*

Risk management

involves continuously assessing threats, monitoring endpoints and attack surfaces, and remediating any threats that make it through your cyber defenses. It's not enough to have a sometimes-on, manual process checking for threats. Your endpoint management solution must include real-time alerting and proactive remediation to identify threats and address them before they become full-scale breaches. In addition, it should offer an automated patching solution that patches critical vulnerabilities quickly minimizing exposure to potential threats.

NinjaOne delivers on these requirements through:

+ Real-time alerts and proactive remediation that identify potential issues and address them before they affect your infrastructure.
+ Autonomous patching that automatically identifies critical vulnerabilities and deploys the appropriate security patches rapidly to minimize exposure and maintain system stability.

Asset visibility

ensures you know everything you need to know about your IT infrastructure, the devices on it, and the data those devices are accessing, making it difficult for bad actors to get away with nefarious actions.

NinjaOne's autonomous endpoint management platform delivers automation, visibility, and control across all endpoints. IT teams can monitor and manage all workflows, end-user devices, servers, VMs, and networking devices from a single, easy-to-use interface.

NinjaOne Warranty Tracking simplifies asset management for IT teams by providing easy access to device warranty status and information. This allows you to prioritize and plan for endpoint renewals, budget effectively, and efficiently offboard devices that are no longer supported, thereby reducing vulnerable threat surfaces.

Supply chain security

is protected and enhanced when you can minimize third-party vulnerabilities. Too many tools from too many vendors can introduce more risk. Consolidating tools reduces your attack surface while offering efficiencies.

NinjaOne consolidates core IT operations into a single, intuitive platform which reduces tool sprawl, minimizes complexity, and reduces vulnerabilities. In addition, by consolidating endpoint and patch management, backup, ticketing, documentation and more into the single dashboard IT teams benefit from streamlined workflows. This enables lean IT teams to prioritize strategic initiatives without compromising compliance or service continuity.

> "Our platform automates patch management, configuration enforcement and alerting. This simplifies the process of maintaining compliance. Agencies can generate audit-ready reports and track their posture over time. We remove the guesswork from endpoint security and compliance."
>
> **AARON KINWORTHY**
> Vice President of Public Sector at NinjaOne

Protecting against cyber attacks

To earn and maintain CMMC certification, organizations need more than deep endpoint management and visibility; they need an autonomous endpoint management solution that supports well-defined security policies, identity and access management (IAM), secure, encrypted data backups, automated patching, and an informed workforce that is alert to potential threats and how to prevent them. Let's take a closer look at each of these capabilities.

Security policies and controls

enable IT teams to manage endpoint controls through a centralized policy management interface. This allows for consistent and precise device management across an entire organization. NinjaOne policy controls enable IT teams to create comprehensive policies that can be inherited across different device roles. Technicians can set granular conditions and controls including application management, software installs, patch management, security restrictions, and more to ensure policies and security are consistent across devices.

Identity & Access Management

is important to CMMC status because IT administrators can use it to define user roles and access levels, authenticate user identities via MFA and set least privilege policies. IAM also authorizes appropriate resource access.

NinjaOne's robust role-based access control (RBAC) enables IT teams to create and configure permissions based on a user's role. Technicians can be given customized controls based on their area of expertise. End users' roles can be granularly assigned based on job function. Regardless of whether the user is a Program Analyst, Contract Specialist, or IT Specialist / IT Support Specialist, NinjaOne's role-based access ensures that the right people have access to the right information at the right times.

As part of its RBAC, NinjaOne creates comprehensive audit logs so your team can check user logins using SSO and other authentication processes. You can also see when MFA is bypassed or an authentication method is changed. With the single dashboard view, all user roles and permissions are visible in one place.

Protecting against cyber attacks *(continued)*

Data security

is obviously a critical aspect in gaining and retaining CMMC authorization. Remote work has complicated data security efforts with users able to access agency data from laptops, smartphones and other mobile devices while in the field. Organizations must demonstrate the ability to secure data, especially classified data, while at rest, in transit, and at the time of disposal or deletion.

System security

is in part maintained by hardening endpoints through consistent, accurate patch management. An automated patch management solution identifies, acquires, and deploys patches to remediate vulnerabilities and improve the overall stability and security of systems and applications. Effective patch management is crucial for preventing cyber attacks, minimizing disruptions, and maintaining compliance with Federal regulations like CMMC.

NinjaOne Autonomous Patch Management correlates scanner data, CVEs, and asset insights to streamline patching. Patch Intelligence AI prioritizes patches based on real-world threat severity, blocks unstable patches, and auto-approves safe updates with AI-driven analysis. NinjaOne autonomous patching minimizes patch-related disruptions, reduces operational risk, and increases endpoint security.

Network resilience protocols

provide continuous business operations even in the event of system failures or data breaches. A resilient IT network is resistant to disruptions, but in the event of a system failure or data breach, the network is able to maintain critical services. Recovery protocols ensure you can quickly recover so your devices and data are restored to peak operating conditions, and your end users remain productive.

NinjaOne supports network resilience by ensuring all endpoints are managed, monitored, up-to-date, and secure. Autonomous patching backed by Patch Intelligence AI prioritizes and deploys patches quickly to cut security risk and prevent disruptions from unstable updates. Flexible policies, off-hours scheduling, and optional patch caching accelerate deployments, reduce network load, and align remediation to your organization's risk tolerance.

In addition, proactive alerting and remediation ensure potential issues are addressed before they affect end users and system processes.

Awareness and training

are important, yet often-overlooked, aspects of a strong cybersecurity posture. Your IT team should understand how to use the tools at their disposal to build and maintain cybersecurity resilience. There are many software tools that play a part in maintaining effective cybersecurity. Learning to effectively implement and manage each could be a long process, making tool consolidation key to facilitating your team's confidence in their ability to manage network cybersecurity.

NinjaOne's platform deploys quickly with even large installations fully deployed in under 30 days. It's easy to learn and use as evidenced by an average of less than 10 days to technician proficiency. Always free and unlimited onboarding, training, and support ensure your team is using NinjaOne to its maximum effectiveness.

NinjaOne's unified endpoint management solution brings endpoint and patch management, backup, ticketing, warranty tracking, and more into a single, unified dashboard.

Detecting security incidents

Even IT infrastructures with strong security protections as described in the previous section can come under attack by bad actors. Therefore, a component of protection against threats is your ability to detect security incidents before they affect your end users or your network infrastructure. Continuous monitoring and proactive threat detection are your first line of defense against security incidents.

Continuous monitoring

through error logs, incident alerts, and visibility into all your endpoints, whether on-prem or remote, is key to helping ensure you discover and address potential cyber threats before they become disasters.

NinjaOne's deep visibility into and comprehensive monitoring of all your endpoints helps bolster security protection. Real-time, proactive alerts, autonomous vulnerability remediation, and automated threat detection ensure potential trouble spots and data breaches are identified before they affect end users or disrupt your operations.

Proactive threat detection

identifies anomalies and advanced threats to your IT infrastructure. It's vital that potential threats are addressed quickly and effectively to maintain data and endpoint security.

With all monitoring and remediation managed through the single NinjaOne dashboard, IT teams eliminate context switching so they can more quickly and effectively remediate threats and keep their network secure.

Minimizing incident impact

Part of maintaining CMMC authorization is showing the capability to minimize the impact a cyber incident could have on your infrastructure. Managing cybersecurity through governance, asset visibility, and supply chain security; protecting against attacks, and early detection of threats reduce the likelihood of a successful cyber incident. However, should a data breach occur, your organization must have a plan in place to minimize such an event. Key components of this plan include an Incident Response and Recovery plan (IRP) and a system for evaluating the root cause of the event with plans for preventing similar attacks in the future.

Incident Response & Recovery Plan (IRP)

is a documented strategy for how your organization will detect, respond to, and recover from cyber threats and security incidents. The IRP outlines how your organization will:

+ Limit damage to systems, data, and reputation
+ Maintain critical business operations during and after the incident
+ Restore normal operations while minimizing downtime
+ Address any legal and regulatory requirements related to data breaches
+ Identify response team members and define each member's roles and responsibilities
+ Conduct containment, recovery, and reporting exercises, including communications to employees and clients/customers

NinjaOne supports IRPs through its Unified Backup solution, Documentation tool and included customer support.

+ NinjaOne Backup is an essential part of an IRP because it provides immutable, chainless backup for workstations, servers, or files and folders, ensuring your data is always protected and easily recoverable.
+ NinjaOne Documentation is a centralized IT knowledge base that enables your technicians to find answers in seconds, focus on recovering from the cyber incident, and getting back to optimal system performance quickly.
+ NinjaOne provides complimentary, expert-level support and resources that empower your team to resolve issues faster, reduce disruption, and drive continuous value from day one.

Document lessons learned

by conducting a root cause analysis and creating a report of the findings. This is an important step in prevention because it helps organizations understand why an incident happened, not just what happened. With this understanding, your team will be better able to implement preventative measures that protect against and respond to future threats.

The NinjaOne agent generates post-incident logs that you can use to help complete your documentation. These activity logs can provide insight into who detected the incident, when it was discovered, and what remediation actions were taken.

NinjaOne's automated policy updates are helpful in building your IRP because they can be used to automatically trigger condition-based alerts, update device health status, modify security policy settings based on the detected threats, and create system-level activities documenting the incident and subsequent response.

Conclusion

CMMC verifies that FARS/DFARS legal obligations are being met. It is not a substitute for these obligations. CMMC is intended to ensure defense contractors are following requirements for protecting controlled unclassified information (CUI).

By aligning your IT staff, cybersecurity policies, endpoint monitoring and management solutions and continually reassessing the efficacy of this alignment, you can implement successful compliance processes and procedures.

NinjaOne is dedicated to providing the US Defense Industrial Base with the secure, unified endpoint management solution they need to modernize their endpoint management, secure their infrastructure, control costs, and achieve and maintain compliance.

Try NinjaOne Free for 30 days.

Contact NinjaOne for a personalized assessment or demo.

ninjaOne® | FedRAMP®

FedRAMP™