

The Latest

on

DOD'S CMMC

INSIDE:

Q&A: DOD's Katie Arrington on CMMC.....	3
Infographic: What is CMMC?	7
Accelerating CMMC Compliance	8
Securing IP for National Security	13

SPONSORED BY

ninjaOne

From the editor's desk



Sarah Sybert, Managing Editor

CMMC Critical for Tomorrow's Cyber Threats

Cybersecurity isn't about compliance; it's about resilience. As cyber threats become more advanced, the Defense Department is rethinking how it protects sensitive information across its massive network of contractors and suppliers. The Cybersecurity Maturity Model Certification, or CMMC, sits at the center of that shift.

Inside, you'll learn how CMMC is designed to keep pace with real-world threats. Certification under the latest CMMC 2.0 framework is mandatory for any vendor bidding on defense contracts.

Pentagon CISO Katie Arrington, who is currently performing the duties of the CIO, discussed her push to make CMMC more dynamic

to respond more quickly to emerging threats. She is back leading the program after launching it under the first Trump administration. She also highlighted how tools like AI can streamline compliance and support a stronger cybersecurity culture across the Defense Industrial Base.

Stacy Bostjanick, the department's lead for DIB cybersecurity, went further. She called attention to new threats to the nation's intellectual property that CMMC can help thwart. From fighter jet designs to sensitive communications, the stakes are high. For Bostjanick, CMMC is about protecting the nation's technological edge and the warfighters who depend on it. ✨

Table of Contents



Ross Gianfortune,
Senior Staff Writer

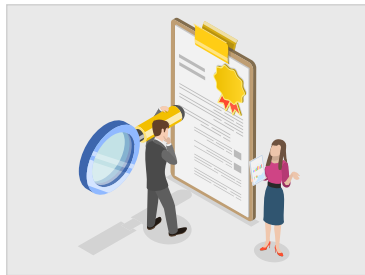


Q&A

CMMC Needs to Adapt to Evolving Cyber Threats

Pentagon cyber chief Katie Arrington sees acquisition reform and stronger cybersecurity culture as major priorities amid CMMC.

BY ROSS GIANFORTUNE



INFOGRAPHIC

What is CMMC?

CMMC is a Defense Department cybersecurity standard to evaluate and improve the cybersecurity of organizations in the Defense Industrial Base.



PARTNER INTERVIEW

Modern Platforms Accelerate CMMC Compliance

Modern IT platforms with automation, visibility and rapid deployment capabilities are helping bridge the gap left by addressing aging legacy systems and workforce shortages.

Aaron Kinworthy, VP Public Sector, NinjaOne



ARTICLE

DIB Cyber Chief: CMMC is a National Security Imperative

Stacy Bostjanick touts the program for ensuring robust cybersecurity to protect against cyber espionage and secure the nation's competitive advantage.

BY ROSS GIANFORTUNE

CMMC Needs to Adapt to Evolving Cyber Threats

Pentagon cyber chief Katie Arrington sees acquisition reform and stronger cybersecurity culture as major priorities amid CMMC.

BY ROSS GIANFORTUNE

What is your long-term vision for CMMC and its role in DOD cybersecurity?

I see CMMC being enduring. What we're hoping to do, as it goes into effect this year, is figure out how to evolve it and make it more dynamic. It's going to have problems. There are going to be issues when it rolls out. I always say, I like to fail early and fail often to get to what I need.

The department is committed to this, but I do have concerns as we look forward. How do I make the NIST SP 800-171 dynamic? As we go through these processes of getting a NIST standard, public comment periods and then another year's review to do another DFARS rule, I hope — with the executive orders on FAR and acquisition reform in the DOD — that we find a way to streamline cyber requirements more effectively. Because the threat today is not going to be the threat tomorrow.

CMMC, just like passwords were 10 years ago — now we're at multifactor authentication and moving beyond that. I'm looking to see how CMMC grows into a more dynamic tool to help not only be safe but ensure compliance. Compliance keeps companies in business — it doesn't put them out.



How are you approaching acquisition reform amid CMMC?

With the executive order on acquisition reform, I've got sprint teams to respond to the executive order and figure out how we can make acquisition better and faster. One of the efforts is streamlining cyber requirements.



Katie Arrington

Performing the Duties of the CIO, DOD

I think something very beneficial would be, once a NIST standard is approved, it automatically becomes the standard for CMMC the following year. I don't even know if that's fast enough. It's just what we have today to work within. I hope that in the future we can use more AI tools, more large language model tools to help CMMC as a compliance check to ensure you have a cyber culture.

How are we going to see that in 10 years? I don't know. But for today, tomorrow and the next five to seven years, this is what we've got. I think once quantum computing and more AI tools emerge, we'll be able to streamline the audit much better, but we still need the requirements to be dynamic enough.

What does a cyber requirement look like today that still matters in three years? Is it smarter to say, "Do you have 256 encryption?" or "Are you using the latest and greatest encryption?" Those are the things we have to get to, and we need industry's help. It should be a living, breathing culture.

How are you approaching the department's Risk Management Framework?

With the executive order on acquisition reform, I've got sprint teams to respond to the executive order and figure out how we can make acquisition better and faster. One of the efforts is streamlining cyber requirements.

I think something very beneficial would be, once a NIST standard is approved, it automatically becomes the standard for CMMC the following year. I don't even know if that's fast enough. It's just what we have today to work within. I hope that in the future we can use more AI tools, more large language model tools to help CMMC as a compliance check to ensure you have a cyber culture.

How are we going to see that in 10 years? I don't know. But for today, tomorrow and the next five to seven years, this is what we've got. I think once quantum computing and more AI tools emerge, we'll be able to streamline the audit much better, but we still need the requirements to be dynamic enough.

What does a cyber requirement look like today that still matters in three

“I hope that in the future we can use more AI tools, more large language model tools to help CMMC as a compliance check to ensure you have a cyber culture.”

— Katie Arrington, Performing the Duties of the CIO, DOD

years? Is it smarter to say, “Do you have 256 encryption?” or “Are you using the latest and greatest encryption?” Those are the things we have to get to, and we need industry’s help. It should be a living, breathing culture.

How are you enacting changes in government, which historically faces bureaucratic barriers?

We’re doing it now. When you have leadership that wants change. When you want something, you’ll make it happen. You’ve got a lady in charge right now who wants to make things happen. You’ve got a president who wants to make things happen. It’s the perfect time for me to be in this position.

It’s absolutely about leadership’s desire to listen to the community. When I said, “Let’s blow up the RMF,” nobody in the room said no. Everyone’s been waiting for the opportunity to speak.

Now, we move to the process. It’s group by group, iteration by iteration, and letting industry chop on it. Then in the end, it’s a majority vote within my shop. The CIOs and CISOs will have a seat at the table. After all the summer conversations, I want a new policy in place by August. We vote on each one — 51% majority rules — and we move out.

To listen to the full interview, find it on CyberCast by searching GovCIO Media & Research Podcasts wherever you listen to podcasts. 🎧

CMMC Needs to Adapt to Evolving Cyber Threats

Katie Arrington says DOD needs to strengthen dynamic cybersecurity in the age of AI and quantum.

Featuring: Katie Arrington, Performing the Duties of the DOD CIO



According to officials, the Defense Department's Cybersecurity Maturity Model Certification (CMMC) program is a national security imperative to protect intellectual property and maintain an American competitive advantage in defense technology.

At AFCEA TechNet 2025 in Baltimore, Katie Arrington, performing the duties of the DOD CIO, says CMMC needs to adapt dynamically to evolving cyber threats. With evolving tech like AI and quantum, acquisition rules

need to adjust to evolving technologies while maintaining security standards. Arrington says that the Defense Department needs to continue to streamline cyber requirements through required standards, guidance and executive orders.

She also discusses the need for a cultural shift towards continuous cybersecurity, the new Software Fast Track Initiative and baking cybersecurity into all DOD functions. 🌸

[Listen to the Full Episode!](#)

What is CMMC?

CMMC is a Defense Department cybersecurity standard to evaluate and improve the cybersecurity of organizations in the Defense Industrial Base.

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 model, requiring progressively advanced protections based on the data's sensitivity. CMMC levels are verified through assessments and are mandatory for contract eligibility.

Level 2

Broad Protection of Controlled Unclassified Information (CUI)

Requires either a self-assessment or a third-party (C3PAO) assessment every three years, based on the type of information handled. Also requires annual affirmation and compliance with 110 controls from NIST SP 800-171.



Level 1

Basic Safeguarding of Federal Contract Information (FCI)

Requires an annual self-assessment and affirmation of compliance with 15 security requirements outlined in FAR 52.204-21.



Level 3

Advanced Protection of CUI

Requires prior Level 2 certification, a DIBCAC assessment every three years, and annual affirmation of compliance with 24 additional controls from NIST SP 800-172.



**CERTIFICATION
LEVELS**

PARTNER INTERVIEW

ninjaOne

Modern Platforms Accelerate CMMC Compliance

Modern IT platforms with automation, visibility and rapid deployment capabilities are helping bridge the gap left by addressing aging legacy systems and workforce shortages.

 **What are some of the key cybersecurity challenges agencies face today?**

Kinworthy Legacy IT creates blind spots adversaries exploit. Hardware, siloed systems and patchwork solutions make it incredibly difficult to apply modern security protocols or keep pace with evolving threats. Agencies also struggle with visibility. Without centralized insight into endpoints, vulnerabilities often go unnoticed until it is too late. (ctd.)

A black and white portrait of Aaron Kinworthy, a man with short dark hair and a light beard, wearing a white button-down shirt. He is smiling slightly and looking towards the camera. The portrait is positioned on the right side of the page, partially overlapping the text.

▲
Aaron Kinworthy
VP Public Sector,
NinjaOne

“Vulnerabilities often go unnoticed until it is too late.”

— Aaron Kinworthy, VP Public Sector, NinjaOne

What are some best practices for agencies trying to move toward a more modernized IT infrastructure?

Kinworthy Automation is no longer a nice-to-have. It is essential for achieving scale, speed and consistency. Agencies need tools that can automate patching, configuration and alerting. This reduces manual effort and minimizes human error. Another best practice is to focus on unified platforms that consolidate IT operations and security functions. This leads to better control, reduced complexity and faster incident response.

How does NinjaOne support federal compliance frameworks like CMMC?

Kinworthy Under CMMC 2.0, liability doesn't just rise, it shifts. Contractors and federal agencies are now on the hook for proving endpoint security continuously, not just annually. Federal IT leaders face a new mandate to prove endpoint compliance continuously, at scale, while under pressure from CMMC 2.0, FedRAMP and mission risk. 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.

What sets NinjaOne apart from other IT operations platforms?

Kinworthy Simplicity and speed. Our platform is cloud-native, which means agencies can deploy it rapidly and manage their IT environment from anywhere. We offer an intuitive interface with powerful automation under the hood. NinjaOne is also trusted by over 30,000 customers across the public and private sectors, including federal agencies. That trust comes from delivering results without adding unnecessary complexity.

How should agencies balance modernization with risk management?

Kinworthy Agencies should take an incremental approach. Start with the highest-risk areas, typically the endpoints, and build from there. Modernization does not have to be disruptive if it is well-planned. With the right platform, agencies can improve their cybersecurity posture while maintaining continuity of operations. (ctd.)

 **As federal agencies continue their modernization efforts over the next 12 months, what trends or innovations are you most excited about?**

Kinworthy The shift to cloud has been phenomenal. It has led to solutions like NinjaOne that can be a software-as-a-service (SaaS) offering that is fast and nimble. Our deployments with customers are averaging less than 30 days from procurement to production, which was unheard of during legacy periods. Credit

to the cloud service providers for building clouds that are secure and enabling agility. That trend is not going to stop.


The SaaS offering today is going to continue, and that trend is evolving. If you look at what the government is doing to change procurement processes and break down barriers of the old way of doing procurements, SaaS is being adopted. It's here to stay, and it's also the future. 

Photo credit: Gorodenkoff/Shutterstock



“Our deployments with customers are averaging less than 30 days from procurement to production, which was unheard of during legacy periods.”

— Aaron Kinworthy, VP Public Sector, NinjaOne

Secure, fast, modern endpoint management for the Federal Market

NinjaOne delivers automated endpoint management that meets federal demands and standards. We help your team stay secure and compliant while you scale to meet changing demands.

With NinjaOne, organizations serving the Federal Market can:

- **Reduce costs and tool sprawl:** Many customers report replacing 2-4 tools with NinjaOne* and reducing IT operational workload by up to 40%.**
- **Simplify and secure operations:** Gain real-time visibility into all your endpoints to proactively identify and resolve issues and maintain security and compliance.
- **Increase efficiency:** Automate routine tasks, streamline workflows, and manage all your devices from the single unified console to free up your team to focus on mission-critical projects.

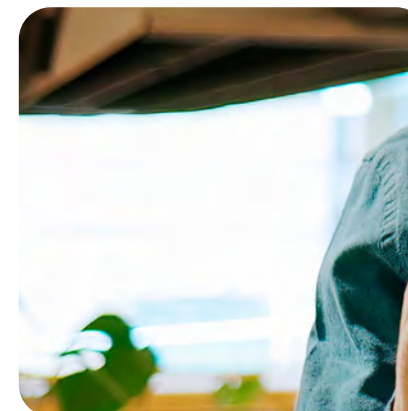
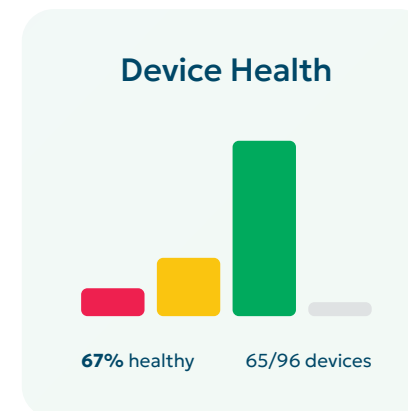
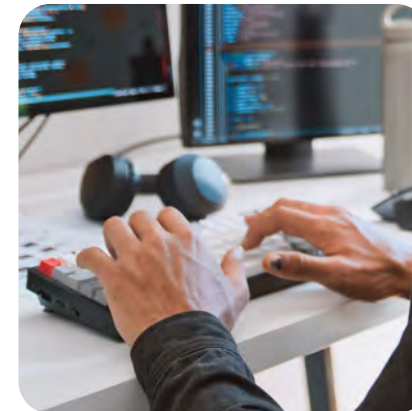
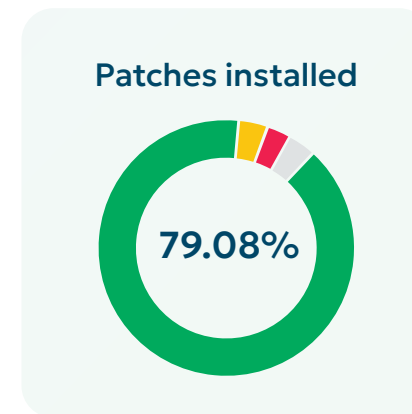
✓ NinjaOne for Government has achieved **FedRAMP® “In Process” designation** at the Moderate Impact Level.

About NinjaOne

NinjaOne, the automated endpoint management platform, delivers visibility, security, and control over all endpoints for more than 30,000 customers in 130+ countries.

* Omdia: Leading IT Trends for 2024: Embracing Automation, Security, and Consolidation

**Enterprise Strategy Group, a division of TechTarget, Research Publication, Managing the Endpoint Vulnerability Gap: May 2023



Central Resources
1 Server, 3 Workstations
Northwest Security
3 Servers, 1 Cloud, 1 VM Host, 20 VM Guests
Northeast Research
3 Servers, 1 Workstation, 1 Remote, 1 Cloud
Northeast Access
2 Servers, 2 Workstations

ninjaOne®

DIB Cyber Chief: CMMC is a National Security Imperative

Stacy Bostjanick touts the program for ensuring robust cybersecurity to protect against cyber espionage and secure the nation's competitive advantage.

BY ROSS GIANFORTUNE

The Cybersecurity Maturity Model Certification (CMMC) program is not only a compliance exercise but rather an imperative to secure sensitive information, protect innovation and safeguard warfighters as cyber espionage continues to rise, a key CMMC official said at a conference in Washington, D.C. in March 2025.

"It's something we need to do as a nation. If we want to protect our lifestyle, we want to protect the way that we in this nation have grown to be the innovators and the leading edge for technology," said Defense Department Chief Defense Industrial Base Cybersecurity and Deputy CIO for Cybersecurity Stacy Bostjanick.

Adversaries are targeting intellectual property, not only threatening financial losses but also the nation's competitive advantage.

"We are losing our intellectual property and sensitive data from the government by leaps and bounds. [Approximately] \$200 to \$600 billion a year in IP ... is lost, and sadly, many of our citizens are unaware," said Bostjanick.

According to national security experts, Chinese actors conducted cyberattacks to steal sensitive military information, including designs for the F-35 Lightning II and the F-22 Raptor to produce their own aircraft — the J-35A stealth fighter and the J-20 Mighty Dragon, respectively. These attacks targeted major Defense Industrial Base (DIB) contractors like Lockheed Martin within the



aircraft's supply chains, as part of broader Chinese cyber espionage this century against the United States and the DIB.

"How many of you are aware that the Chinese have an aircraft that looks just like our F-35?" she asked the crowd. "Are you more aware that designs to our F-22 have been taken?"



Stacy Bostjanick

Chief Defense Industrial Base
Cybersecurity and Deputy CIO
for Cybersecurity, DOD

Bostjanick explained that DOD initiated CMMC in response to significant cybersecurity challenges that plagued the DIB. She explained that initial reviews of compliance in 2017 revealed stark gaps in contractors handling controlled unclassified information (CUI), with some contractors providing insufficient documentation.

“We found 50% of companies failing to meet basic compliance, leading us to develop CMMC to validate that contractors were actively fulfilling their cybersecurity commitments,” Bostjanick said.

Warfighters “depend on the integrity of” CUI, she explained. CMMC compliance, she said, supports the need for a robust cybersecurity framework in manufacturing and technology. She added that unsecured CUI could potentially compromise technological advantages, impacting frontline military capabilities.

Bostjanick said the necessary evolution of CMMC brings the potential for incorporating stronger zero-trust principles in the future. The slow regulatory process is also a challenge to firms working to comply with CMMC requirements, she added.

“CMMC is metamorphic,” she stated, emphasizing the need to stay relevant with emerging threats. “As soon as we close one gap, another one opens. We’re going to have to stay relevant with that.”

“I view CMMC as the toll before the crawl, before the walk, before the run,” she said.

Bostjanick added that the DOD is working on providing more accessible resources, including bite-sized YouTube videos, to help small and medium-sized businesses navigate the certification process.

“I’ve heard from a lot of the smalls, ‘I don’t have time to go into a two-day training. I got maybe 30 minutes,’” she said. “We’re going to try to produce some bite-size training videos for people to be able to use to navigate their way through CMMC safety.” ❁

**“I view CMMC as
the toll before
the crawl, before
the walk, before
the run.”**

**— Stacy Bostjanick, Chief Defense Industrial Base
Cybersecurity and Deputy CIO for Cybersecurity, DOD**