



**NEXTGOV/
FCW**

CMMC:

Securing the Defense Industrial Base

As the Defense Department moves forward on its cybersecurity requirements for contractors, a growing ecosystem of technology providers is helping companies navigate the journey to certification

In partnership with: C3 | Cytellix
Cyturus | HP Federal | Keeper Security
PreVeil | Quzara | Zscaler

carahsoft.

Learn more at carahsoft.com/innovation

- S-14** Advancing DOD's quest for information security
- S-16** Better visibility results in better risk management
- S-18** Securing even the smallest link in the supply chain
- S-20** The importance of endpoint security by design
- S-22** New year, new CMMC password requirements
- S-24** Reducing the cost and complexity of compliance
- S-26** Augmenting security teams for a defense-in-depth strategy
- S-28** A secure, streamlined path to CMMC compliance
- S-30** Cyber AB's role in the certification process
- S-31** How Carahsoft helps companies meet CMMC requirements

Advancing DOD's quest for information security

The Defense Department is fine-tuning its Cybersecurity Maturity Model Certification program to ensure that contractors' systems are a bulwark against data breaches

When the Defense Department released its long-awaited proposed rule for CMMC 2.0 in December, it marked the latest evolution in the department's years-long effort to secure the sensitive government information held on contractors' systems.

Companies in the defense industrial base (DIB) are attractive targets for adversaries because of the sensitive information that flows through their systems. "The DIB encompasses a wide variety of entities, including commercial firms operated on a for-profit basis, not-for-profit research centers and university laboratories, and government-owned industrial facilities," a Congressional Research Service [report](#) states. The researchers also note that the DIB provides a wide range of products and services, including sophisticated weapons systems, highly specialized operational support, general commercial products and routine services.

According to the [Cybersecurity and Infrastructure Security Agency](#) (CISA), the DIB includes more than 100,000 companies that work under contract to DOD. Not surprisingly, that adds up to a lot of contracting dollars. According to a Government Accountability Office [analysis](#), DOD committed \$414.5 billion in spending with contractors in fiscal 2022, the most recent year for which numbers are available. That compares to \$279.7 billion for all civilian agencies combined.

Securing contractor IT systems is of paramount importance given the central role that the DIB plays in U.S. military operations. In just one example that underscores the urgency of the problem, the FBI, the National Security Agency and CISA released a joint cybersecurity advisory in February 2022 stating that they had observed "regular targeting of U.S. cleared defense contractors by Russian state-sponsored cyber actors" since at least January 2020. And some of

those attempts were successful, with potentially grave consequences.

"By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment," the advisory states.

Addressing the basics of cyber hygiene

Adversaries don't need to resort to sophisticated weapons to undermine U.S. military activities. Instead, "these actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data," according to the advisory.

Such common weaknesses in IT systems are what DOD's Cybersecurity

CMMC by the numbers

Sources: Cybersecurity and Infrastructure Security Agency, Government Accountability Office, Nextgov/FCW

100K

The number of companies and subcontractors that perform under contract to the Defense Department

\$414.5B

The amount DOD committed in spending with contractors in fiscal 2022, compared to \$279.7 billion for all civilian agencies combined

82%

Nextgov/FCW survey respondents who said CMMC certification will enhance their companies' cybersecurity and competitiveness in the marketplace

39%

Nextgov/FCW survey respondents who cited a lack of leadership understanding and buy-in as one of the biggest challenges to achieving CMMC certification at their companies

Maturity Model Certification program is meant to address. “CMMC is blocking and tackling — the basics of cyber hygiene,” Matthew Travis, CEO of the Cyber AB, told Nextgov/FCW. His organization plays a central role in helping DOD implement the CMMC program and helping companies comply with it.

CMMC targets controlled unclassified information (CUI), which is described as information that does not require classification but is still sensitive enough to need special protection. Examples include personally identifiable information, health records, technical drawings and blueprints, and proprietary business information.

Since 2017, defense contractors have had to comply with the 110 security requirements in the National Institute of Standards and Technology’s Special Publication 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.” In 2020, however, DOD intensified its focus on the security of contractors’ systems by publishing an interim rule that explained its initial vision for the CMMC program, referred to as CMMC 1.0. The rule outlined key features of the framework — a tiered model for compliance, required assessments and implementation through contracts — and went into effect in November 2020 with a five-year phase-in process.

By early the following year, DOD officials had received several hundred public comments in response to the interim rule and decided to launch an internal review to refine the policy and its implementation. The result was CMMC 2.0, which was announced in November 2021. Two years later, in December 2023, the department finally released a proposed rule for the next phase of the program. It is open for public comment until Feb. 26, 2024.

Progressively advanced levels of security

According to [DOD](#), “CMMC requires that companies entrusted with national

security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information.”

The proposed CMMC 2.0 is divided into three levels:

- **Level 1** — 15 requirements, annual self-assessment and annual affirmation.
- **Level 2** — 110 requirements aligned with NIST SP 800-171, triennial third-party assessment and annual affirmation, and triennial self-assessment and annual affirmation for select programs.
- **Level 3** — 110-plus requirements based on NIST SP 800-171 and 800-172, triennial government-led assessment and annual affirmation.

For the higher levels, companies must undergo certification by an independent CMMC third-party assessment organization (C3PAO). Responsibility for accrediting the C3PAOs rests with the Cyber AB.

Nick Wakeman, editor-in-chief of Nextgov/FCW sibling publication Washington Technology, noted in a recent opinion piece that “earning a certification at levels two and three will be expensive and time-consuming,” and although many experts had expected waivers or extensions for small businesses, the proposed rule has no special dispensation for those companies.

“If DOD gave small businesses a pass, adversaries would know the weak points to exploit,” Wakeman pointed out. “Not having a different set of expectations for small businesses also is a clear signal of how seriously DOD takes the cybersecurity threat in the supply chain.”

Companies don’t have to go it alone

In a recent survey of Nextgov/FCW readers who work for government contractors, 82% of respondents agreed with the statement that CMMC certification will enhance their companies’ cybersecurity and competitiveness in the marketplace.

We also asked what progress their companies have made toward achieving compliance with CMMC. A total of 57% have begun the process, are halfway through it or have achieved certification under CMMC 1.0, while 27% are just starting to talk about it. Only 16% are not thinking about pursuing certification.

Respondents said the biggest challenges to achieving CMMC certification are lack of leadership understanding and buy-in (cited by 39% of respondents), the ongoing need to educate employees about cyber hygiene (34%), entrenched internal processes (33%), difficulty finding a third-party assessment organization (33%) and the expense and time involved in pursuing certification (32%). By contrast, only 28% cited a lack of appropriate technology, and 27% cited a lack of employees with the right skill set.

Last on the list was confusion about the process at 23%, which speaks to the efforts of DOD, the Cyber AB and industry to work together to ensure that CMMC offers a clear path to certification. Along the way, an ecosystem of vendors has arisen to help companies prepare for and successfully complete the certification process with a wide range of technology solutions and advisory services.

Travis said the Cyber AB has played a lead role in developing a practitioner community whose goal “is to help businesses, especially small businesses, understand the requirements and to offer advice on how to comply with them. So companies don’t have to go it alone, but they need to start now because CMMC is coming.”

Indeed, many experts have warned companies not to wait until CMMC 2.0 is formalized and incorporated into contract requirements. The certification process is complex and time-consuming, Travis said, and it “involves the entire company because DOD wants to see that cybersecurity is inculcated in how the business operates.” ■

CYTELLIX

Better visibility results in better risk management

Combining governance, risk and compliance with managed detection and response truly transforms cybersecurity



Brian Berger
Cytellix

Visibility is crucial for understanding the true cybersecurity posture of a company and improving its risk management. It involves identifying cloud-based assets; hard assets such as switches, routers and servers; software-based behaviors and operational technologies; and internet-of-things technologies, such as cameras and sensors.

The goal is to understand where those assets are connecting to the network, how they're behaving and what/who they're communicating with so that any anomalous behavior can be detected, responded to and remediated to better protect the business' critical information.

Governance, risk and compliance (GRC) is a category of solutions that helps determine how a company is aligning to a cybersecurity framework, such as the

A comprehensive approach to compliance

That's where security efforts start to move into Managed Detection Response (MDR), which includes endpoint and log management through capabilities such as security information and event management and Endpoint Detection Response (EDR). GRC and MDR are typically handled separately, with one part of the company responsible for regulatory compliance and another responsible for security and incidents. When companies combine GRC and MDR capabilities, however, they create a measurable and comprehensive approach to cybersecurity risk and compliance.

Cytellix has developed a security platform, Cytellix Cyber Watch Platform (CCWP™), that brings together GRC, MDR and a third category called Extended Detection Response (XDR). That

combination helps our customers protect critical information as required by regulatory requirements, including CMMC. It also helps them understand whether they are under attack, whether information is leaking out of the organization and whether

any employees are acting in a way that increases the company's security risks.

Our CCWP™ prepares a company for audit and certification by a CMMC third-party assessment organization, and it works across on-premises, cloud-based and hybrid environments. We monitor and respond to security events that include all assets, virtual environments and networks, and in real time, we can identify changes



For companies that want to achieve CMMC compliance and win and maintain government contracts, the time to start is now.”

Defense Department's Cybersecurity Maturity Model Certification (CMMC). Dynamic GRC tools can offer a deeper understanding of an overall cyber posture and network design and provide visibility into assets and their behaviors to uncover violations of a company's policy and/or a framework's objectives. However, the company won't know that a violation has occurred without some sort of monitoring of changes in posture.

iStock



in employee behavior, data leakage and attacks by bad actors to prevent a change that would put companies in violation of cybersecurity compliance frameworks.

The long timeline to certification

Companies that need assistance complying with CMMC or other cybersecurity frameworks should seek an expert that can help them understand what's necessary from a capabilities perspective and guide them through the entire process so that they gain ongoing, real-time situational awareness of their security posture and the cyber risks they face.

We're on a timeline to mandatory CMMC compliance over the next three years, with the first contracts requiring CMMC expected to appear in the early part of fiscal 2025. That might sound like plenty of time, but achieving compliance takes much longer than many companies expect.

For the past six years, we have measured new clients' cybersecurity postures against the industry framework, and the average score is about 29% out of 100%. So companies typically have a long way to go.

The preparation work to secure the company including: Employees,

Infrastructure and Applications may include development of policies, configuration management and/or technology procurement — typically takes 12 to 18 months.

For companies that want to achieve CMMC compliance and win and maintain government contracts, the time to start is now. The infrastructure for helping suppliers meet compliance is not unlimited, and certification could bottleneck as we get closer to contract issuance. Be proactive! ■

Brian Berger is president of Cytellix.



The **ONLY** place GRC meets XDR.

One Platform. Better Visibility.
Better Risk Management.



cytellix.com

info@cytellix.com
(949) 215 - 8889

CYTURUS

Securing even the smallest link in the supply chain

Adversaries can undermine U.S. defense capabilities by making a slight alteration in a tiny subsystem



Robert Hill
Cyturus

Some larger companies have the resources to facilitate compliance with new regulatory requirements, such as the Defense Department's Cybersecurity Maturity Model Certification (CMMC) program. However, many smaller companies question the criticality of having every link in the supply chain comply with what can seem like overly demanding requirements.

To demonstrate why this is important, I like to use the hypothetical example of a small manufacturing company with only five employees that produces a single specific gasket for the F-35 fighter jet. This small manufacturing operation does not have an IT manager, it does not employ a security compliance officer, and the office is simply connected to local Wi-Fi via a cable modem. While it is a cost-effective solution for this small

changed the operating parameters. As a result, the company produces 10,000 gaskets that are technically defective because they were fabricated using the replaced parameters. Those gaskets go into the supply chain and eventually into the U.S. combat aircraft.

Soon that defective part causes a jet to flame out and crash, but because the military doesn't know why this happened, the entire fleet of the most advanced combat fighter aircraft in the world is grounded without our enemy firing a single physical shot. The weapons deployed on today's battlefield are virtual and in many instances are fired months in advance of the apparent impact.

A purpose-built platform for security compliance

The Cyturus Compliance and Risk Tracker (CRT) platform was designed to facilitate and simplify the compliance process. The proprietary Self-Guided Assessment module walks companies through their initial self-assessment to understand where their deficiencies are, establish a SPRS

score, and identify areas that need remediation via development of a Plan of Action and Milestones and a System Security Plan (SSP). This process is unique to the industry.

An Organization Seeking Certification (OSC) can simply log into the Membership Portal at the website of the Cyber AB (which administers the CMMC program)



The weapons deployed on today's battlefield are virtual and in many instances are fired months in advance of the apparent impact."

organization, it is not CMMC-compliant.

Let's say that several months ago an aggressive nation-state bad actor accessed an unprotected PC on that cable company-supplied Wi-Fi connection. During the undetected intrusion, the bad actor made a minor adjustment to that specific gasket's dimension, decreasing it from 31 millimeters to 27 millimeters. The difference is not visually apparent but

iStock



and select a Registered Provider Organization (RPO), or vice versa, and those two entities become affiliated with each other within the Membership Portal system. As a Cyber AB RPO benefit, a Registered Practitioner (RP) or Registered Practitioner Advanced (RPA) can then be affiliated with the OSC to help it prepare for the certification assessment. Once affiliated, the RP/RPA can access the CRT tool via single sign-on integration to review the OSC's self-guided assessment and drill into the specific objectives and implementation solutions. When the OSC is ready for the certification

assessment, it can align with a CMMC Third-Party Assessment Organization.

Throughout this entire process, the OSC maintains complete control of its compliance evidence and proprietary information.

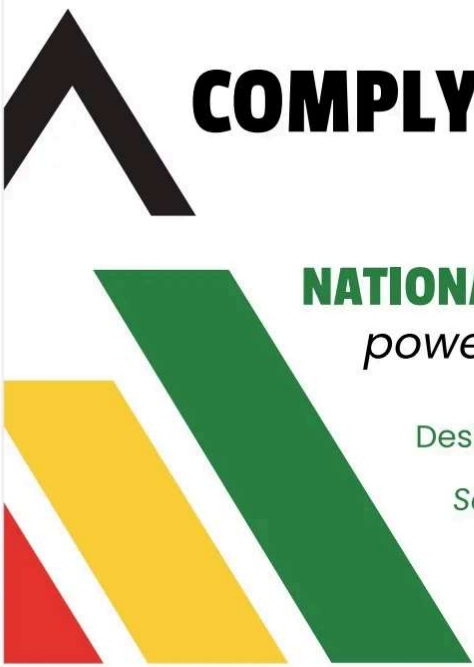
Why CMMC represents a paradigm shift

CMMC requires a different mindset and consequently a different set of procedures. Instead of demonstrating how they comply with security mandates now or have done so in the past, companies must show how

they will continue meeting those requirements in a consistent manner for the next 36 months.

It is a paradigm shift from offering a lens into historical security once a year to an organizational commitment to a more sustainable approach to operational security now and into the future. ■

Robert Hill is the CEO and founder of Cyturus.




COMPLY WITH CONFIDENCE

NATIONAL DEFENSE GRADE COMPLIANCE

powered by Cyturus

Designated CMMC Platform of Cyber AB
Securing every link in the supply chain
Supporting the CMMC ecosystem
Safeguarding the DIB

cyturus.com



HP FEDERAL

The importance of endpoint security by design

Delivering highly secure endpoints hinges on innovation and a holistic approach to supply chain decisions



Matt Barry
HP Federal

Endpoints can be vectors for bad actors to insert themselves into a company's network, which means endpoint security is a critical component of efforts to protect government and contractor systems. And it has long been a particular focus of HP's product development.

We think deeply about security by design right from the outset and take an integrated approach to how we source components and create products. When we design more secure solutions upfront, that security carries through the entire life cycle.

Furthermore, endpoints are intelligent devices. They have IP addresses, so as soon as they are powered up, they become part of a potential attack surface. To address such risks, HP has innovated

confidence. We help our customers minimize their attack surface and strengthen their overall security posture. For example, each time a user powers up his or her device, HP Wolf Security compares the device's firmware to a copy on an embedded security controller chip. If malware changes the firmware, the security tool will recognize it and revert to the gold-standard version.

HP Sure Admin provides modern security for PC firmware configuration management by enabling remote administrators to securely manage BIOS settings. It also enables field support personnel to obtain secure in-person access to BIOS setup. Use of digital certificates and public-key cryptography eliminates the risks associated with legacy password-based approaches by using QR codes that return a one-time password when scanned by the Sure Admin phone app.

These tools ensure that our customers' resilience is significantly enhanced and downtime is minimized in the event of an attack.

Partnering with the government to advance

cybersecurity

HP has acquired companies over the years to provide our customers with holistic solutions and integrations to enhance the end-user and IT experience. One of my personal favorites is our acquisition of a company called Bromium. We've fully integrated and further developed the solution and call it Sure



Endpoints are intelligent devices. They have IP addresses, so as soon as they are powered up, they become part of a potential attack surface.”

for years at distinct levels — below the operating system, in the operating system and above the operating system.

Enhancing resilience and minimizing downtime

So much of our innovation in cyber-physical security revolves around managing risks in endpoints with

iStock



Click Enterprise. We use it every single day at HP. If I come across something malicious when I open an attachment or visit a website, it would ordinarily infect my device. But with Sure Click Enterprise, my activities run in a micro virtual machine so that my device still operates cleanly after I exit the session. That technology has prevented billions of attack vectors from infecting machines in our environment and our customers' environments. And this software works in any Windows 10/11 environment, not just on HP hardware.

HP helps companies strengthen their risk and compliance programs

by taking a zero trust approach to developing our hardware and by aligning with the Cybersecurity and Infrastructure Security Agency's and the National Institute of Standards and Technology's (NIST) guidelines. We also partner with the government to advance its cybersecurity programs and certifications. HP has been an industry editor with NIST on a number of special publications focused on cybersecurity. Firmware resilience is one example. The Cybersecurity Maturity Model Certification (CMMC) program is an important development in safeguarding the defense industrial base and, by extension, our nation's cybersecurity,

and HP has been a strong advocate of the program from the early days.

CMMC has gone through multiple iterations over the years, and I am confident that when the formal rule is fully deployed, defense contractors will step up to the challenge of protecting their networks from attackers. With the provisional CMMC rule published in late December, the time to act is now. ■

Matt Barry is chief operating officer at HP Federal.



carahsoft.

HP WOLF SECURITY

Who are cyber criminals targeting?

You! Government entities attract bad threat actors because highly sensitive information such as Personal Identifiable Information (PII) is a lucrative business. Resource and budget constraints make it difficult to protect sensitive data effectively.

Where do threat actors target?

The PC endpoint where the internet, user and data all intersect allowing human error to facilitate attacks.

Enter HP Wolf Security

- Gain full stack endpoint protection and resiliency from hardware extending across software.
- Improve supply chain attack protection.
- Reduces the addressable attack surface to simplify your PC protection.
- Minimize risks, boost IT efficiency, and enhance user productivity



Ask us about HP Sure Click Enterprise, Protection for Endpoint Security

Built to complement your current detection solutions!

Learn more at: 

KEEPER SECURITY

New year, new CMMC password requirements

Companies can satisfy several CMMC controls with a password manager and privileged access manager rooted in zero trust



Mike Eppes
Keeper Security

The much-anticipated CMMC 2.0 proposed rule was officially published in the Federal Register on Dec. 26, 2023. The final rule is expected to be out sometime this spring. Although the rule is long and complex, the basic purpose of the Cybersecurity Maturity Model Certification (CMMC) program is to ensure that every organization that does business with the Defense Department is certified via a third-party audit that demonstrates its basic cyber hygiene.

One area of cyber hygiene that the new CMMC rule addresses is password management. The majority of CMMC's current security controls are based on the National Institute of Standards and Technology's Special Publication 800-171 Revision 2, which was released in 2020. NIST 800-171 Revision 3 will be released in the coming months and will

Adopting a zero trust mindset

These seemingly simple requirements are of vital importance to our nation's security. DOD is entrusted with highly sensitive, classified information. And contractors often have access to controlled unclassified information, such as personally identifiable information, health documents, proprietary material and information related to legal proceedings.

Every member of DOD, including contractors, must adopt a zero trust mindset. This "never trust, always verify" attitude requires companies and individuals to take responsibility for the security of their data, devices, applications and assets. It also means users are granted access only to the data they need and only when needed.



A 'never trust, always verify' attitude requires companies and individuals to take responsibility for the security of their data, devices, applications and assets."

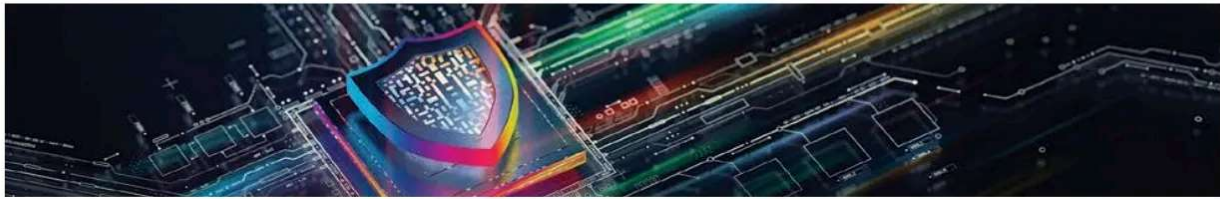
include new requirements for passwords. Defense contractors will need to account for these new requirements, such as changing passwords when they have been compromised and ensuring that new or updated passwords are not on lists of commonly used, expected or compromised passwords.

With zero trust, password management is one of the simplest ways to protect sensitive systems and data. Seventy-four percent of all breaches involve the human element, with the majority due to weak or stolen passwords. Yet most IT administrators have no visibility, security or control over their employees' passwords and credentials.

A FedRAMP-authorized solution

Keeper Security gives IT and security teams visibility into the strengths and weaknesses of their organizations' passwords and alerts administrators when

iStock



passwords have been compromised or when users are not complying with organizational password policies, such as prohibitions on password reuse. This approach allows administrators to proactively address weaknesses and prevent data breaches.

Keeper Security Government Cloud (KSGC) is a password manager and privileged access manager that is FedRAMP-authorized to protect against cyberthreats. The zero trust solution is further strengthened with zero knowledge security. KSGC provides an advanced cloud authentication and network communications model built for the highest levels of privacy, security and trust.

Each end user is provided with a vault to store passwords, and the contents of the vault are protected with multiple layers of safeguards and encryption. Decrypting a user's vault requires decryption of the data key, which can include a user's master password. For users who log in with single sign-on or passwordless technology, elliptic curve cryptography is used to encrypt and decrypt data at the device level.

KSGC is also StateRAMP-authorized and validated under FIPS 140-2. Hundreds of defense industrial base organizations rely on Keeper to protect their passwords, secrets and privileged

credentials from the dynamic threats facing our nation's military.

It's expected that the CMMC proposed rule will be final by the end of 2024 and start to appear in contracts in 2025 so it's important to start preparing now. Many people look at CMMC as another security checklist, but I hope it's also encouraging companies to make a long-term commitment to zero trust by securing every user on every device and in every location. ■

Mike Eppes is director of public sector at Keeper Security.



Easily address CMMC controls across multiple domains with Keeper Security Government Cloud

Keeper Security Government Cloud (KSGC) password manager and privileged access manager protects every user with easy-to-use and cost-effective security.

- FedRAMP Authorized
- FIPS 140-2 validated
- Available in the AWS GovCloud

Hundreds of Defense Industrial Base (DIB) organizations rely on Keeper to protect their passwords, secrets and privileged credentials.



FedRAMP



FIPS 140-2



AWS GovCloud

Learn more at keepersecurity.com

PREVEIL

Reducing the cost and complexity of compliance

Innovative, encrypted email and file-sharing system simplifies information protection under CMMC and DFARS



Sanjeev Verma
PreVeil

Email and files are obvious sources of interest to adversaries, especially for defense contractors because they frequently contain sensitive controlled unclassified information that must be protected in a manner compliant with the Defense Federal Acquisition Regulation Supplement (DFARS) and the Defense Department's Cybersecurity Maturity Model Certification (CMMC). Design specifications containing CUI, for example, are stored and collaborated on across a company so if adversaries can compromise such systems, they can gain access to virtually every piece of sensitive data a company has.

PreVeil's is an easy-to-use, end-to-end encrypted email and file-sharing system that protects data for CMMC and DFARS compliance. It is extraordinarily easy to deploy because it simply overlays the email and file-sharing tools a company

is protected even if an attacker breaches a server or email system. PreVeil's system also foils attackers by requiring authorization from multiple administrators to decrypt information and by eliminating passwords.

Precise and accurate documentation

The CMMC program is closely related to DFARS, which already applies to defense contractors that handle CUI. DFARS requires contractors to protect CUI using the 110 controls of the National Institute of Standards and Technology's Special Publication 800-171 but allows contractors to submit self-evaluations to demonstrate compliance. CMMC takes it one step further by requiring companies to work with independent third-party assessment organizations to certify that they are adhering to those 110 controls.



Zero trust security relies in part on end-to-end encryption so information is protected even if an attacker breaches a server or email system.”

PreVeil's system is designed to cover about 102 controls. Each control is either fully met by using PreVeil or partially met, with the client handling the other part. For example, we protect CUI, but the

client must institute a policy requiring its employees to use PreVeil, so it's a shared responsibility.

already uses rather than requiring an expensive rip and replacement of existing systems.

Furthermore, demonstrating evidence of compliance with security regulations relies heavily on extensive documentation. That documentation must be precise and accurate, and it often costs tens of thousands of dollars to bring all the information together. PreVeil simplifies the

PreVeil protects CUI using zero trust, the modern approach to cybersecurity that acknowledges that perimeter defenses will inevitably fail to prevent attackers from reaching the information. Zero trust security relies in part on end-to-end encryption so information

iStock



process enormously by providing users with the necessary documentation. Companies that use PreVeil not only raise their Supplier Performance Risk System scores with DOD but also provide documented evidence of compliance to both government assessors and prime contractors.

Low cost and high assurance of compliance

Furthermore, PreVeil reduces costs because it's designed to be deployed only to the employees who handle CUI. If a company has hundreds of employees but only 50 handle CUI, it can achieve compliance by only deploying PreVeil and its associated

documentation to an enclave of those 50 employees. In addition, the cost of a PreVeil license is inherently less expensive than alternatives.

All these elements help PreVeil address the needs of small to medium defense contractors, which often lack the technical and compliance sophistication to meet DOD's rigorous security demands. PreVeil offers a low-cost, simplified approach that brings high assurance of compliance and uncompromising security for CUI. Several PreVeil customers have demonstrated perfect 110/110 compliance scores in rigorous DFARS and CMMC assessments.

At PreVeil, we believe it is vital to reduce the cost and complexity involved in achieving compliance with DFARS and CMMC without cutting any corners on cybersecurity because it's a matter of national security. We do the hard work to provide a complete solution so that small and medium enterprises can approach compliance with a simplified check-the-box mindset and typically achieve 60% savings over alternatives. ■

Sanjeev Verma is founder and chairman of PreVeil.



The Industry Leading CMMC Compliance Solution

TRUSTED BY OVER 1000 DEFENSE CONTRACTORS • EASY TO USE • SAVE 60% VS. ALTERNATIVES

PreVeil is the leading solution for CMMC and DFARS compliance. Our comprehensive 3-part solution includes:

1. An email + file sharing platform to protect CUI,
2. Documentation to demonstrate compliance, and
3. Certified consultants and auditors.

This saves contractors over 60% vs alternatives, while securing their data with military-grade end-to-end encryption.



PREVEIL

For more information about PreVeil, please visit www.preveil.com/cmmc-compliance

QUZARA

Augmenting security teams for a defense-in-depth strategy

Quzara Cybertorch™ enhances an organization's ability to understand and respond to threats



Saif Rahman
Quzara

The defense industrial base (DIB) faces continuous adversary attacks, given its crucial role in national security and involvement in sensitive transactions. Compliance serves as a vital tool, enabling DIB organizations to establish robust security operations. Frameworks like the Cybersecurity Maturity Model Certification (CMMC) outline specific requirements for DIB organizations, placing a strong emphasis on security monitoring, auditing and the generation of security logs. These logs are essential for empowering security teams to understand the threats they face.

Additionally, the CMMC framework includes criteria for incident management and the prevention of data exfiltration, which is particularly crucial when dealing with controlled unclassified information that may potentially leave the organization. Without proper visibility,

Meaningful analysis and insight into vulnerabilities

As organizations progress through the CMMC levels, aligning with the National Institute of Standards and Technology's Special Publication 800-172 (CMMC Level 3), the emphasis on heightened security visibility is evident by the requirement to establish and maintain a security operations center (SOC) capability, deploy advanced automation and analytics capabilities, and conduct cyberthreat hunting activities. These requirements reinforce the framework's commitment to robust cybersecurity practices that provide meaningful analysis and insights into an organization's vulnerabilities.

As a leading managed extended detection and response provider, Quzara is dedicated to addressing the myriad security threats that organizations encounter. Through our innovative

Quzara Cybertorch™ solution, subscribing organizations inherit a comprehensive set of controls covering auditing, logging, incident response and account monitoring.

Choosing Quzara Cybertorch™ means seamlessly integrating robust defense-in-depth measures into your cybersecurity framework. Our team meticulously reviews logs to offer insightful analysis and

identify vulnerabilities. But it doesn't end there. We actively collaborate with our customers to craft tailored solutions that ensure a proactive and adaptive security posture. Quzara empowers organizations to navigate the dynamic threat landscape by providing not just a service but a fortified cybersecurity foundation.



Establishing trust in a security provider is paramount for any organization because it directly influences the trust built with the end customer.”

an organization remains vulnerable to ongoing attacks. For example, if an employee's computer is communicating with a device in a country that is not a U.S. ally, it signals a potential incident that requires investigation. The ability to produce logs that facilitate such investigations is critical for enhancing overall cybersecurity measures.

iStock



Beyond a one-and-done activity

Quzara provides support through a professional advisory services division that assists organizations in conducting gap assessments and understanding their overall readiness for CMMC compliance. Additionally, our FedRAMP High Ready, 24/7 SOC as a service (SOCaaS)/MXDR, staffed exclusively by U.S. citizens, is anticipated to be the only SOCaaS/MXDR authorized at the FedRAMP High Baseline by the FedRAMP Joint Authorization Board in early spring 2024.

In situations where organizations aiming for CMMC compliance lack a robust IT or security team, Quzara

takes a proactive approach. We extend our support beyond mere compliance, working to augment our customers' security teams continually. Our commitment is not a one-time activity focused solely on achieving compliance; it's an ongoing 24/7 operation in collaboration with our customers.

Establishing trust in a security provider is paramount for any organization because it directly influences the trust built with the end customer, particularly in the case of the Defense Department. An authorized FedRAMP High Ready service provider, such as Quzara, differs significantly from providers that offer existing

services without undergoing the government's rigorous review process.

When DOD officials observe that a contractor's provider has a robust compliance background, it instills confidence in the contractor's ability to safeguard government data and networks effectively against potential adversaries. Quzara's commitment to FedRAMP High authorization underscores our dedication to providing top-tier security solutions for our clients. ■

Saif Rahman is CEO and co-founder of Quzara.



Cybertorch®

Division of Quzara, LLC
Detection. Response. Analytics.

Security Operations Center as-a-service (SOCaaS) provider Quzara Cybertorch™ enables robust Cyber Threat Management

Quzara Cybertorch™, the first FedRAMP HIGH Ready SOC-as-a-Service, provides the following security capabilities to Materion's ecosystem:

- 24/7/365 Security Monitoring
- Managed Extended Detection and Response (MXDR) to cyber threats
- Adhere to multiple security Compliance frameworks
- Detecting, preventing, and investigating suspicious activities
- Vulnerability management and Threat Remediation

quzara.com/cybertorch

ZSCALER | C3 INTEGRATED SOLUTIONS

A secure, streamlined path to CMMC compliance

A partnership between C3 and Zscaler takes the guesswork out of meeting CMMC's requirements



Jeffrey Adorno
Zscaler



Ryan Heidorn
C3 Integrated Solutions

Everybody understands the need to protect classified information for national security reasons. Controlled unclassified information (CUI), however, is still sensitive because if someone were to aggregate and correlate it, they could start to derive government secrets, such as how we build fighter jets or make certain technology. Blueprints, technology drawings and manufacturing specifications fall into the CUI category.

The Defense Department's Cybersecurity Maturity Model Certification (CMMC) program seeks to enforce requirements that already exist to protect CUI on contractor networks. In other words, the challenge is not a new one. Back in 2019, Ron Ross, a fellow at the National Institute of Standards and Technology and the principal author of the security requirements that underpin CMMC, said: "We are literally hemorrhaging critical information about key programs." He made the statement in the context of sensitive, taxpayer-funded intellectual property stored on contractor networks.

each other. Zero trust empowers CMMC programs with a modern cybersecurity framework that increases threat intelligence and enables adaptive just in time/just enough access. In contrast, CMMC approaches cybersecurity in a programmatic way so that when defense contractors leverage a zero trust architecture, they can easily achieve and maintain a higher level of maturity under CMMC.

One of the core tenets of zero trust is to stop insider threats and adversaries from stealing sensitive intellectual property even while assuming that breaches will happen. That means zero trust is uniquely suited for contractors that are designing systems not only for compliance but for security resilience as well.

Zero trust can accelerate a contractor's compliance with CMMC because it offers a way to mitigate technical bloat and debt, such as on-premises legacy technologies. Approaches to CMMC compliance typically start with a gap assessment to understand a company's current ability to meet security controls and create a plan for remediation. However, if a company can redefine its network boundary using zero trust capabilities that provide context-based access, it can create a shorter path to compliance.

“

Zero trust is uniquely suited for contractors that are designing systems not only for compliance but for security resilience as well.”

Finding a way around technical debt

Contrary to some misconceptions, zero trust and CMMC do not run counter to

Limiting preparatory work by consolidating security tools

The partnership between C3, a managed services provider that accelerates the CMMC compliance process, and Zscaler, which is a

iStock



technology leader in cloud security, offers companies a secure, streamlined route to CMMC compliance and ongoing protection against the myriad threats they face.

Zscaler helps contractors consolidate their security tools into a single cloud-native security fabric, which is a key reason why C3 chose to partner with Zscaler. In the language of CMMC, each security protection asset must conform to security requirements. If a company has 150 security tools, its level of effort is multiplied across all those tools to prove that it is meeting requirements.

Therefore, tool consolidation is an important strategy for limiting the amount of preparatory work that a contractor must perform before a CMMC assessment.

C3 also teamed with Zscaler because its solutions have FedRAMP authorization, validated cryptography and ITAR compliance. In addition, Zscaler enables C3 customers to leverage Zscaler's API integrations to adopt modern technologies such as intrusion detection and prevention systems and endpoint detection and response to support a

work-from-anywhere model, which is a requirement for most companies in the post-COVID world.

The bulk of the DOD supply chain is small businesses, and C3 and Zscaler understand the unique needs of those companies. Together, we work with them to find the right solution at the right price to achieve their security goals. ■

Jeffrey Adorno is senior manager of strategic initiatives at Zscaler, and **Ryan Heidorn** is CTO at C3 Integrated Solutions.





Secure. Simplify. Transform.

Protect your agency with the most accredited security cloud in the world. FedRAMP Moderate and High, DoD IL5 and StateRAMP authorized.

- Protect data from cyberthreats
- Reduce IT cost and complexity
- Improve user experience
- Meet mandates with confidence

Learn more at
zscaler.com/federal



© 2024 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

EXECUTIVE VIEWPOINT

A conversation with

Matthew Travis

CEO, The Cyber AB



Why is the Cybersecurity Maturity Model Certification program such an important component of the Defense Department's cybersecurity efforts?

This is the first time the department has taken assertive steps to stop the theft and exfiltration of intellectual property from our defense industrial base, which we know has been a problem for awhile.

Initially, the department made it a contractual requirement to implement the National Institute of Standards and Technology's cybersecurity standards for controlled unclassified information. When officials realized that wasn't working, they went to self-attestation, requiring companies to legally announce that they had implemented the standards. And then they realized that wasn't working.

CMMC is trailblazing because it's the first time that third-party validation of cybersecurity is being implemented on such an ambitious level. There are other conformity regimes out there, such as FedRAMP and ISO, but CMMC is larger and more involved, and it has

more moving parts than anything like this before.

How do companies become certified under CMMC, and what is the Cyber AB's role in that process?

We do a lot of things, but our primary role will eventually be to authorize and accredit the CMMC third-party assessment organizations, or C3PAOs. For the CMMC program to succeed, there has to be trust and confidence in the system, and defense firms must know that when they undergo an assessment, it will be fair and impartial, and it will use consistent procedures and official documentation.

There are no shortcuts. There's no inside game. A small company in New England will get the same assessment as a large aerospace firm in Southern California. Conflicts of interest will be disclosed, mitigated and/or prevented. And there will be a transparent appeals process, if and when there's a technical disagreement on a particular practice implementation.

Without someone who's in the middle of it all ensuring that consistency, CMMC won't be able to succeed. That's what we do.

Regarding how CMMC will work, companies that want to become certified will reach out through our marketplace at CyberAB.org. Right now, there are 50 authorized C3PAOs. Companies can contact those organizations and negotiate in terms of what they charge and when they're available, and ultimately sign up for an assessment. That assessment involves looking at the company's

system security plan, observing the implementation of cybersecurity practices and asking questions of the employees.

The C3PAO is empowered to issue a certification upon confirming the successful implementation of the CMMC standard, which is based on NIST Special Publication 800-171. That certification allows the defense company to bid on and win DOD contracts that have CMMC requirements.

What do you see as the future of CMMC?

I believe this approach will go beyond DOD. I suspect that federal civilian agencies and even state and local agencies will likely require third-party validation that contractors have implemented basic cybersecurity protections. They will no longer just take someone's word for it. And that will extend to business partnerships and the entire supply chain. Companies will need to show teaming partners, customers and suppliers that they have implemented the basics of cybersecurity.

Although this sounds very new and ambitious, a few years down the road, it will be the norm — just like public companies expect to have their financials audited. It is validation that everything is as it should be in terms of protection for data and networks.

That's where I see all this going. It may take a while, but I'm proud that we get to be involved in helping DOD blaze this trail. ■

This interview continues at carahsoft.com/innovation.

EXECUTIVE VIEWPOINT

A conversation with

Alex Whitworth

Sales Director, Carahsoft



How is industry scaling to support the defense industrial base for the Cybersecurity Maturity Model Certification program?

The ecosystem that supports the DIB is responding to the challenges created by CMMC, and industry is realigning itself to support companies and help them increase their cyber resilience. The offerings for advisory consulting services, managed services and purpose-built technology continue to grow in breadth and depth. That variety of choices will help companies accelerate their CMMC journey. It allows for a more ideal fit for individual companies based on their unique environments, their in-house talent and resources, and how much money they have to spend. That environment also breeds competition and innovation, which drive down costs.

In each of the major categories, the base of capabilities is growing. We're also seeing more managed service providers and managed security service providers tailor offerings for CMMC. Those offerings include architecture, migration, security operations center-as-a-service and CMMC-compliant enclave environments. In addition, governance, risk and compliance

providers are tuning their technology to manage the CMMC life cycle as they have already done for other frameworks.

How is CMMC changing the cybersecurity expectations for government contractors?

Within the Defense Department's supply chain, companies are raising their levels of cyber maturity and cyber resilience. CMMC's influence is also spreading to the civilian side and even to foreign governments.

The Department of Homeland Security released a proposed cybersecurity readiness evaluation factor for assessing the cyber maturity of its contractor base. The questionnaire is rooted in the National Institute of Standards and Technology's Special Publications 800-171 and 800-172, which are the same controls that CMMC will likely be based on. In addition, the General Services Administration has released a draft questionnaire for a cybersecurity supply chain risk management effort. Some sections are closely aligned to CMMC and NIST's Cybersecurity Framework.

The global nature of CMMC has raised some interesting challenges for our allies. For example, Canadian defense companies that supply goods and services to DOD need to comply with CMMC, but they don't have the local infrastructure of advisory service providers to help them. Adopting CMMC and creating an ecosystem to support those suppliers would benefit Canada's own defense industry. The government of Canada has announced that it is implementing a mandatory certification program modeled on NIST

standards, and the U.K. is evaluating similar options.

How does Carahsoft help companies address CMMC requirements so they can achieve certification?



























Carahsoft is proud to be part of the CMMC ecosystem. We have about 800 employees focused on cybersecurity offerings, and we represent about 100 cybersecurity vendors. We track policies and trends to align our customers' needs with the technology that can help them address those needs. We promote "better together" integrations with our customers, vendors and partners every day so we can provide deep, valuable CMMC-focused capabilities for customers.

We partner with companies that address every CMMC maturity level and capability domain. We have CMMC subject-matter experts that can identify the right technology for unique environments. We can connect companies with service providers and advisory consultants that can help them prepare for or execute a CMMC assessment. We also offer news, educational material, events and other resources to help companies gather information and make informed choices.

Decisions about what to buy to fill security gaps and achieve CMMC compliance are extremely important. It is costly and time-consuming to implement those technologies, so companies want to get it right the first time. Carahsoft can guide them through all the available options and help them make the decision that is best suited to their unique needs. ■

Meeting CMMC 2.0 Requirements

The Department of Defense created the Cybersecurity Maturity Model Certification (CMMC) to raise the level of information security across the entire Defense Industrial Base (DIB) and better protect our nation's critical information. Carahsoft and our partners have assembled products and services to help the defense community achieve the right compliance level, safeguard sensitive information and maintain public trust.

 abacode	 ARMIS®	 aws	 BeyondTrust
 CYTELLIX	 CYTURUS	 FORESCOUT	 Gigamon®
 HP WOLF SECURITY	 KEEPER®	 Kiteworks	 Lookout®
 Microsoft	 okta	 paloalto® NETWORKS	 PREVEIL
 proofpoint.	 qmulos®	 Quzara.com Cloud. Security. Analytics	 RSA®
 salesforce	 splunk>	 tenable	 Trellix
 Trustwave®	 virtru	 zscaler™	+ many others!

To learn more about Carahsoft's CMMC solutions, including a list of vendors matched to each CMMC control, please visit carah.io/CMMC. To gain access to leading cyber vendors, align to service providers or MSPs that can implement solutions, and learn about the latest updates to the CMMC program, contact CMMC@carahsoft.com or (571) 591-6222.

carahsoft® The Trusted Government
IT Solutions Provider®

©2024 Carahsoft Technology Corp. All Rights Reserved.

