Kiteworks

White Paper

Securing Content Communications for CMMC 2.0

Complexity and Incomplete Visibility Present Barriers to Compliance

Executive Summary

"The federal government spent $682 billion on contracts in FY 2020, the fifth consecutive year that contracting increased."

"The 200 Government Contractors Shaping the Federal Market," Bloomberg Government, accessed January 11, 2022.

With Department of Defense (DoD) contracts approaching half a trillion dollars annually, there are ample opportunities for various private businesses to become part of the Defense Industrial Base (DIB)—and make a healthy profit in doing so. But defense contractors face stringent requirements in many areas, including cybersecurity.

The DoD's Cybersecurity Maturity Model Certification (CMMC) program was recently updated to reduce the number of mandated third-party assessments—a boon to smaller organizations that wish to participate. However, the underlying requirements remain unchanged. Organizations must demonstrate compliance with strict standards from the National Institute of Standards and Technology (NIST) to move to the higher maturity levels that make them eligible to manage highly sensitive data.

Such compliance is easier said than done. When it comes to content communications, many organizations use a fragmented, ad hoc approach to sharing files with external parties. This creates many barriers to compliance—including a lack of full visibility into the supply chain, the inability to control access to all content across the network, and inconsistency in whether content is encrypted. CMMC compliance is extremely difficult for any organization until these issues are addressed.

Department of Defense Contractor Budget

In the federal government of the United States, the $713 billion budget of the DoD in fiscal year 2020 was second only to that of the Department of Health and Human Services.[1] But the DoD was dominant when it comes to contracted services. In fact, an astounding $447 billion—62% of the department's budget—went to contractors.[2] These contracts are awarded to more than 50,000 organizations each year, with a total of nearly 465,000 employees fulfilling their terms.[3] Overall, DoD accounts for 65% of the total spent by the federal government on contracts.[4]

Risks With the Supply Chain

All these organizations and individuals represent links in the DoD supply chain, which is under increasing threat. The size and breadth of this supply chain bring many risks:

Complexity

Lockheed Martin, Raytheon, General Dynamics, Boeing, and Northrop Grumman were the top defense contractors in 2020, and some may think only of large, multinational enterprises like these when the topic is discussed. However, DoD executes contracts with companies of all sizes. In fact, thanks partly to goals set by the Small Business Administration, many defense contractors qualify as small businesses in their fields.[5]

While this diversity in the contractor pool is laudable, the sheer number of contractors—and the broad diversity of functions that they fulfill—makes the DoD supply chain among the most complex in the world. And this complexity is only increasing, with a 45% increase in DoD contract spending from FY 2016 to FY 2020.[6] This trend is counter to the advice of experts such as Gartner, who urge organizations to *reduce* the surface area of supply chains due to cybersecurity risk.[7]

Naturally, DoD holds the country's most sensitive data—information related to intelligence, military strategy and operations, and other aspects of national security. And by all accounts, supply chain attacks are increasing.[8] Such attacks have already impacted DoD and other critical federal agencies.[9] As a result, supply chain security is a critical priority for DoD—and for the nation in general.

Lack of Visibility and Control

Employees and contractors in an organization's supply chain are outside the organization's direct control. The same is true of the hardware and software used by those third parties. But the problem goes beyond a lack of control: In many cases, organizations lack even basic visibility into their supply chains. One recent study found that more than half of organizations lack end-to-end visibility into all their suppliers and partners.[10] Another study found that only 35% of companies even maintain a list of all the third parties with which they share sensitive information.[11]

Given this lack of visibility, it should come as no surprise that according to estimates by industry experts, about 60% of data breaches occur through third-party vendors.[12] Just as alarmingly, according to IBM and the Ponemon Institute, it takes an average of 280 days to detect a third-party breach,[13] giving cyber criminals ample time to find desired content throughout the network and inflict maximum damage.

Risks Inherent With File Transfer and Sharing

Sensitive content is most vulnerable when it is shared with third parties—vendors, clients, partners, and government agencies. DoD contractors must regularly transfer confidential files to other organizations, inside or outside of government. Without a comprehensive, easy-to-use secure file sharing and transfer platform, the path of least resistance is for employees to simply send such files by email without appropriate encryption and other security protocols. Further, in the event a file is too large for an email system, consumer-grade file-sharing sites are ubiquitous and easy to use—a constant temptation for employees who simply want to do their jobs in a timely fashion.

Unfortunately, either option can potentially expose the content to cyber criminals. A recent survey finds that 42% of organizations encrypt some or none of their email content communications, while just 15% encrypt all email. This inconsistency in encryption increases the risk of the content being intercepted.[14] And typical file-sharing services do not provide the level of protection required for a business, especially one that contracts with DoD.

CMMC: Addressing Supply Chain Risk

To address growing supply chain threats, DoD created the Cybersecurity Maturity Model Certification (CMMC) in 2019. The program had a goal of "assessing and enhancing the cybersecurity posture of the Defense Industrial Base (DIB), particularly as it relates to controlled unclassified information (CUI) within the supply chain."[15]

CMMC was announced in the aftermath of a series of supply chain attacks, in recognition that self-reporting of compliance with the National Institute of Standards and Technology's (NIST's) Special Publication (SP) 800-171 was inadequate to address the rapidly evolving threat.[16]

"The fact of the matter is, when it comes to the U.S. supply chain, we mostly haven't got a clue. It's a massively interconnected network that represents an ecosystem—one with risks coming from all angles and multiple points of failure."

Oliver Freeman, "Biden's Supply Chain Intentions Depend on Cybersecurity," Supply Chain Digital, May 10, 2021.

CMMC 1.0: Complexity and Cost Disadvantage Smaller Organizations

The initial iteration of CMMC envisioned five levels of maturity certifications for each member of the DIB, with the requirement of a third-party assessment to verify the first, third, and fifth levels (Figure 1). But the sheer complexity of the framework made it difficult for contractors to even understand what was required for each level.[17]

CMMC 1.0 also had other problems. The requirement for multiple third-party assessments added significant costs for DoD contractors, which were especially onerous for smaller companies. This created a potential for some of the DoD's "best sources of innovation" to bow out of the DIB because of cost constraints.[18] In addition, there was a question as to whether enough assessors would be available to conduct hundreds of thousands of assessments in a timely manner.[19]

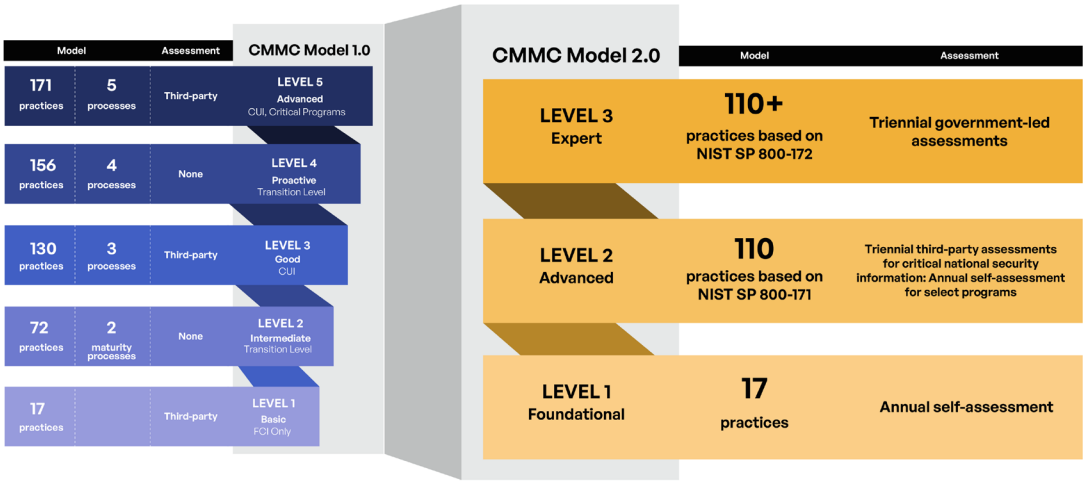

Figure 1. Comparison of CMMC 1.0 and 2.0.

CMMC 2.0: Fewer Steps but More Responsibility

In November 2021, DoD released a new framework, branded as CMMC 2.0, in an apparent attempt to address the shortcomings of the initial CMMC.[20] The number of levels is reduced from five to three, and triennial assessments are required only on Level 3 and on Level 2 for critical national security information (Figure 1).

This new framework dramatically reduces the number of required third-party assessments, minimizing costs for smaller organizations while lightening the workload for DoD's certified independent assessors. But it should be noted that the underlying requirements did not change from CMMC 1.0 to 2.0. Mid-level contractors still need to comply with NIST SP 800-171, and top-tier ones must also align with NIST SP 800-172.

The responsibility for self-assessment should not be taken lightly. Level 1 self-assessments must be conducted annually, three times as frequently as the third-party assessments they replace. And it is likely that the Supplier Performance Risk System (SPRS) scores used with current self-assessments will be replaced by a very detailed report template. In the end, some organizations may find that they still need the help of third parties to complete the report.[21]

"CMMC 2.0 will dramatically strengthen the cybersecurity of the defense industrial base. . . . [T]hese updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements."

Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy, in "Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program," U.S. Department of Defense, November 4, 2021.

Regardless of the format, organizations must dedicate significant staff time to this annual reporting process, and those with a more fragmented approach to security controls must expend even more time correlating data between different tools and platforms. DoD will expect self-assessments to be thorough, accurate, and clear,

Barriers to CMMC Compliance for Secure File Transfer

While CMMC 2.0 reduces the cost and complexity of compliance compared with CMMC 1.0, advancing to the second and third levels of maturity is still no piece of cake. As they work on a strategy to align with CMMC 2.0, defense contractors face several common problems related to secure content communications:

Disparate Content Communication Systems

Unless an organization makes a deliberate effort to unify its content communication technology and processes, the default is a fragmented approach. Content housed in the enterprise resource planning (ERP) system might be shared in one way, while the customer relationship management (CRM) platform might have a different protocol. Content from the human resources information system (HRIS), cloud-based storage solutions, collaboration tools, and industry-specific tools like banking or electronic medical records (EMR) systems might each have a separate process.

Content communications may also be fragmented by recipient. Suppliers, service providers, partners, and government entities may have different protocols. In another scenario, encrypted email could be shared with recipients using the same email encryption standard, while other methods of file sharing must be used when the encryption standard is different.

This complexity can impact operational efficiency and cause stress among front-line users. An external party with whom a specific employee works on a regular basis feels like an insider, and employees tend to prioritize efficient transfer of the information over its security. This problem is exacerbated by the lack of visibility for many organizations into their supply chain.

Difficulty in Tracking Content in Motion or at Rest

With content stored in multiple locations and shared via many different channels, many organizations lack an enterprise view of where its sensitive content resides and how (and to whom) it is distributed. This lack of visibility increases the risk of unintended disclosure of sensitive information. It also means that management may not even be immediately aware when content is inappropriately shared, accidentally or deliberately.

Difficulty in Migrating to Compliant Cloud Resources

Most defense contractors now operate in the cloud, including some cloud-only or cloud-first enterprises. The cloud offers big cost optimization, operational efficiency, and scalability benefits for many organizations. Most cloud-hosted services used by federal contractors must be authorized by the General Services Administration's Federal Risk and Authorization Management Program (FedRAMP) to manage CUI data. One FedRAMP requirement is that encryption must adhere to the Federal Information Processing Standard (FIPS) 140-2 standard.

Naturally, FedRAMP-compliant cloud platforms are easy to find, with Amazon Web Services' GovCloud and the Microsoft 365 Government Community Cloud High (GCC High). One problem with these platforms is the expense and complexity of migration. Organizations often must shut down existing email, storage, and collaboration servers in commercial-grade cloud platforms, replacing them with the FedRAMP-approved alternative.

Once the painful and expensive migration is complete, organizations pay a much higher subscription rate per user, and must absorb these costs even for users that do not handle CUI—unless they want to manage and maintain two separate cloud environments. Worse yet, users in the federal cloud find it much more difficult than before to share information outside the secure environment.

Limited Control Over Content Access

The fragmented nature of content communications at many organizations also increases the risk that sensitive content will be accessed by unauthorized individuals, whether well-meaning or malicious. Access control for

different platforms may be siloed, and there may not be a complete inventory of what content a specific login might provide for a user. Once a user shares content, there is often no record of that data transfer, and the content now sits on a third-party device with no way for the source organization to control it.

Inconsistent Encryption

With content stored and shared in numerous ways, it is virtually impossible to guarantee that content is encrypted when it is in motion to an internal or third-party recipient. Content transmitted by email encounters roadblocks when the recipient's email encryption standard differs from that of the sender, and collaboration and file-sharing platforms often do not encrypt data at all.

Nonintuitive Tools

There are numerous options for CMMC-compliant content sharing and transfer, but many are difficult for non-experts to use. For instance, Secure File Transfer Protocol (SFTP) clients are technically compliant with CMMC—when used correctly. But they are confusing and nonintuitive for front-line users who are simply trying to do their jobs. Faced with this frustration, employees face the constant temptation to use a consumer-grade file-sharing service to expedite file sharing during a busy workday.

Needed: A Comprehensive Approach to Secure File Sharing

In response to the immense risks posed by the need to share content between organizations, corporate legal departments are quick to adopt legal remedies like vendor rationalization, audits, service-level agreements (SLAs), and contractual liability. While these remedies may mitigate financial risk after the fact and provide the accountability needed for a specific entity to improve its practices, they do nothing to prevent data breaches in the first place. Organizations wanting to achieve the Advanced and Expert maturity levels under CMMC 2.0 must move beyond legal remedies to hardened controls that prevent exposure in the first place.

In a nutshell, organizations must demonstrate that they have content communications under control, and that such communications meet security requirements. The best way to achieve CMMC compliance is with a content communications platform that accomplishes four objectives:

- ***Unify*** secure content communication technologies and standardize multiple content audit trails into one centralized system
- ***Track*** comprehensive situational awareness of content, user, and system activity to boost the effectiveness of the security operations center (SOC), report on third-party access, and meet CMMC reporting requirements

CMMC's goal for 2022: "[M]oving the program from the theoretical to the operational level and making CMMC a real, tangible program that contractors must work through rather than just talk about."

Derek B. Johnson, "CMMC Stakeholders Expect Less Talk, More Action to Shore Up Contractor Security," SC Media, January 3, 2022.

- ***Control*** compliance and internal policy requirements by implementing content access and functional rules matched to risk profiles and user roles
- ***Secure*** unintended exposure of sensitive information by implementing content access and functional rules matched to risk profiles and user roles

Deploying a secure content communications platform enables DoD contractors to win contracts that require advanced levels of security maturity. It can also improve operational efficiency enough to make those engagements even more popular.

References

[1] "List of Federal Departments," FederalPay.org, accessed December 21, 2021.
[2] Jon Harper, "2020 Was Good Year for Contractors," National Defense, July 29, 2021.
[3] "Defense Primer: Department of Defense Contractors," Congressional Research Service, updated December 17, 2021.
[4] Ibid.
[5] "Small Business Procurement Scorecard Overview," U.S. Small Business Administration, accessed December 21, 2021.
[6] Robert Levinson, "Fiscal 2020 Pentagon Contracting Hits Record $445 Billion," Bloomberg Government, January 6, 2021.
[7] "Gartner Says Supply Chains Must Reduce Their Surface Area Risk to Reduce the Frequency of Disruptions," Gartner, July 13, 2021.
[8] "Supply Chain Cyber Attacks Expected to Quadruple, Says EU Agency," Homeland Security Today, August 2, 2021.
[9] For example, see Jackson Barnett, "Nearly 40 Defense Companies Were Impacted in SolarWinds Breach," FedScoop, May 18, 2021.
[10] "The Resilient Supply Chain Benchmark: Ready for Anything? Turbulence and the Resilience Imperative," Association for Supply Chain Management, accessed December 22, 2021.
[11] "Preparing for a Cyber Attack Through Your Supply Chain," PwC, January 2019.
[12] "How to Prevent Third-party Vendor Data Breaches," Reciprocity, October 11, 2021.
[13] "2021 Cost of a Data Breach Report," IBM and Ponemon Institute, accessed December 22, 2021.
[14] Global survey by Kiteworks, January 2022, findings to be published in February 2022.
[15] Susan B. Cassidy and Melinda Lewis, "DoD Announces the Cybersecurity Maturity Model Certification (CMMC) Initiative," Inside Government Contracts, July 16, 2019.
[16] Ibid.
[17] Justin Doubleday, "Pentagon Strips Down CMMC Program to Streamline Industry Cyber Assessments," Federal News Network, November 4, 2021.
[18] Derek B. Johnson, "CMMC Overhaul to Change Cybersecurity Requirements for Defense Contractors," SC Media, November 4, 2021.
[19] Ibid.
[20] Ibid.
[21] Ed Bassett, "Debunking Myths About CMMC 2.0," Security Boulevard, November 29, 2021.

Kiteworks

Copyright © 2022 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. To this end, we created a platform that delivers content governance, compliance, and protection to customers. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.