Cybersecurity Maturity Model Certification (CMMC):

How to Prepare Your Organization with Data-Centric CUI Protection from Virtru

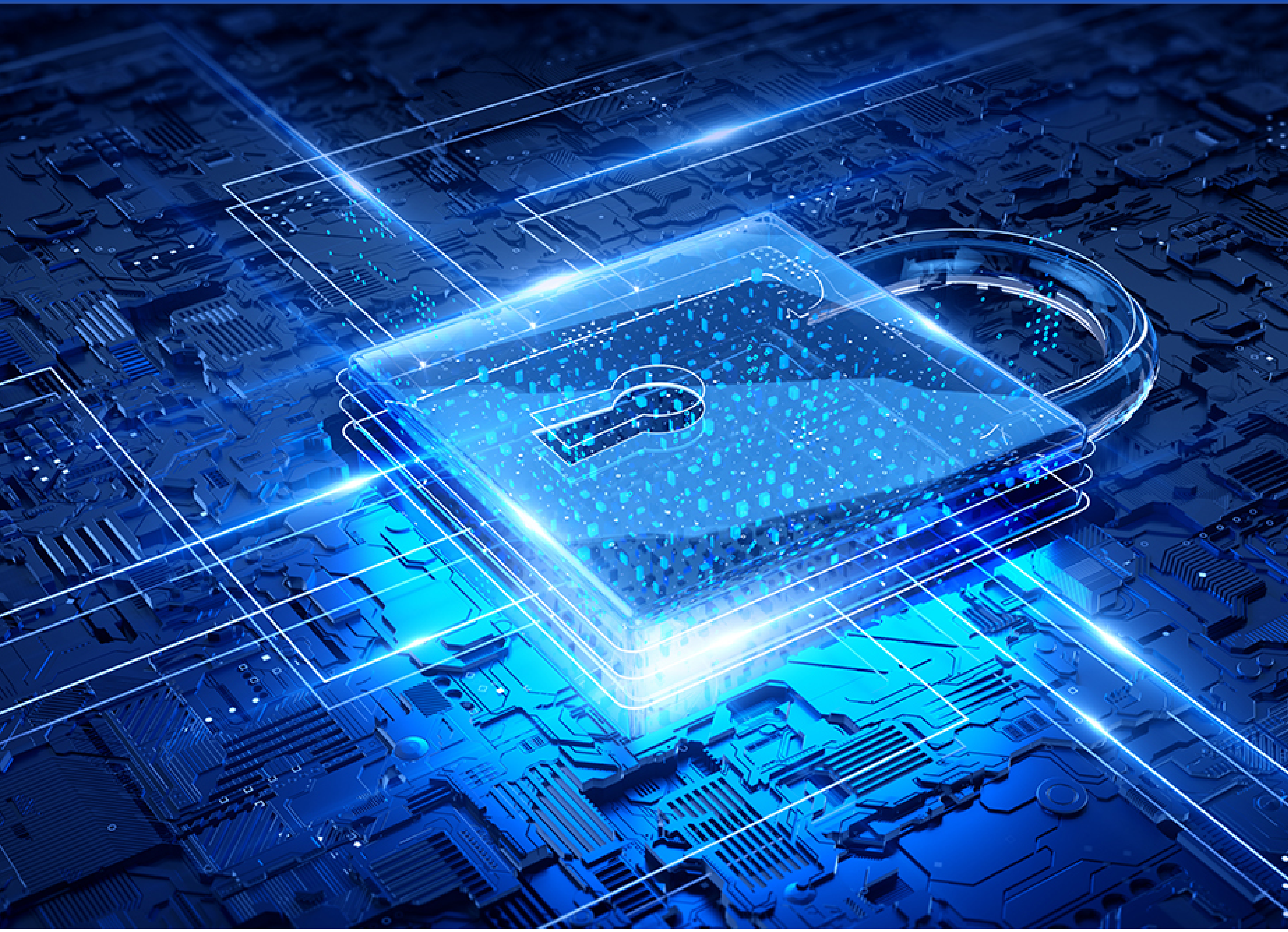


Table of Contents

CMMC: Future-Proofing the Defense Industrial Base 3

CMMC Framework 3

Practices, Processes, and Domains 4

Certification Levels 5

Alignment with DFARS and NIST 6

CMMC Preparedness Action Plan 7

Importance of Email and File Protection for the Supply Chain 7

Email and File Protection Evaluation Criteria 7

Virtru for CMMC Level 3 10

Solution Overview 10

The Virtru Difference 12

Appendices 14

Appendix 1: Virtru Support for Level 3, 4, and 5 CMMC Practices 14

Appendix 2: Virtru Support for NIST SP 800-171 Security Requirements and DFARS 252.204-7012 17

CMMC: Future-Proofing the Defense Industrial Base

The importance of cybersecurity to the defense industrial base (DIB) and supply chain has become increasingly apparent in recent years. Emerging digital capabilities have advanced research, engineering, development, production, and operations initiatives, fortifying Department of Defense (DoD) systems, networks, capabilities, and services and ultimately strengthening national security.

Digital capabilities have also opened new attack vectors for US adversaries. Cloud networks, Internet of Things (IoT), and Artificial Intelligence (AI) have added billions of new devices and network nodes to the cyber domain, and as these technologies accelerate, the cyber domain becomes an even more compelling target for espionage. Without standardized security practices and procedures across the DIB, malicious cyber activities threaten to weaken not only US national security but global trade as a whole.

Cybersecurity Maturity Model Certification (CMMC) was born out of these concerns and developed by the Office of the Under Secretary of Defense Acquisition & Sustainment (OUSD A&S) in partnership with key DoD stakeholders from industry, academia, and federally-funded research centers. The chief purpose of CMMC is to protect unclassified information throughout the defense supply chain from cyber threats. CMMC will achieve this by requiring DIB contractors to implement unified cybersecurity standards, validated by third-party assessments. Going beyond the "set it and forget it" approach of existing standards, CMMC promotes the institutionalization of cybersecurity processes to continuously evolve the maturity of the DIB's security posture.

The first version of CMMC was introduced in January 2020. By Fall 2020, the DoD plans to add CMMC requirements to a small set of contracts, expanding into subsequent years. By Fall 2026, all new DoD contracts are expected to include CMMC requirements.

CMMC Framework

Practices, Processes, and Domains

CMMC encompasses maturity processes and cybersecurity best practices sourced from multiple existing cybersecurity standards as well as discussions with the DIB and cybersecurity industry stakeholders.

> **Practices** are cybersecurity techniques, capabilities, methods, etc. such as protecting sensitive data with end-to-end encryption.
>
> **Processes** are institutionalized procedures that ensure effective implementation of the practices (as opposed to ad hoc), such as deploying end-to-end encryption tools for end users and configuring policies to enforce their usage.

CMMC categorizes these practices and processes into several **domains**, or groupings of similar security-related areas. Those domains and their abbreviations are illustrated in the figure below:

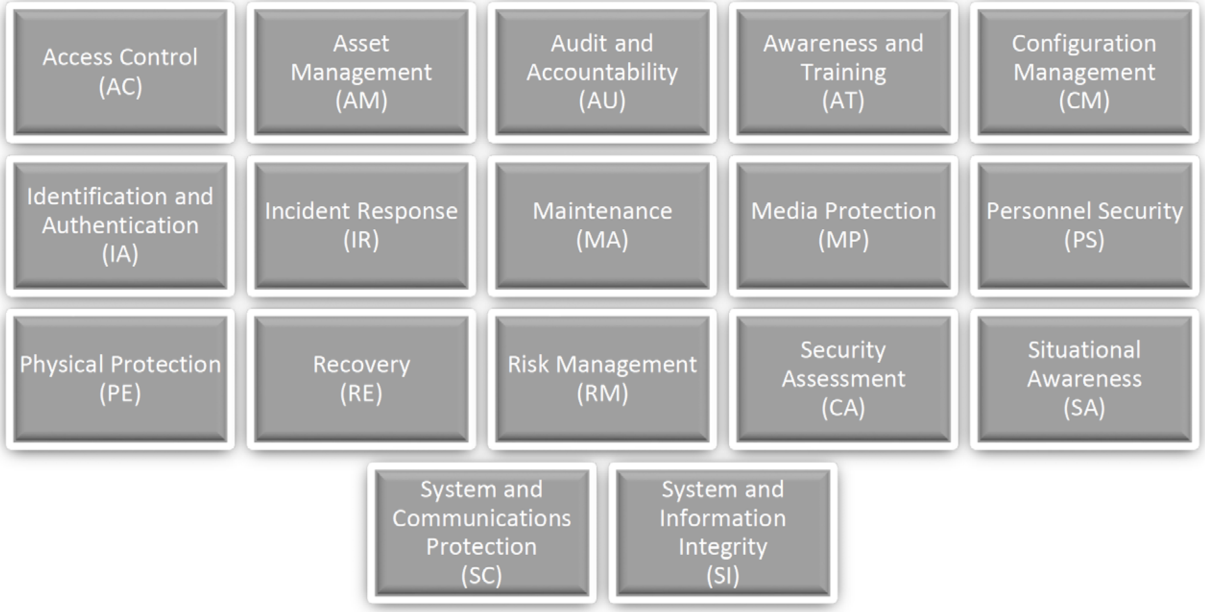


Figure 4. CMMC Domains

([Source: CMMC v1.02])

CMMC's domains, practices, and processes interact in a hierarchical manner to reinforce each other, reflected in the diagram below:

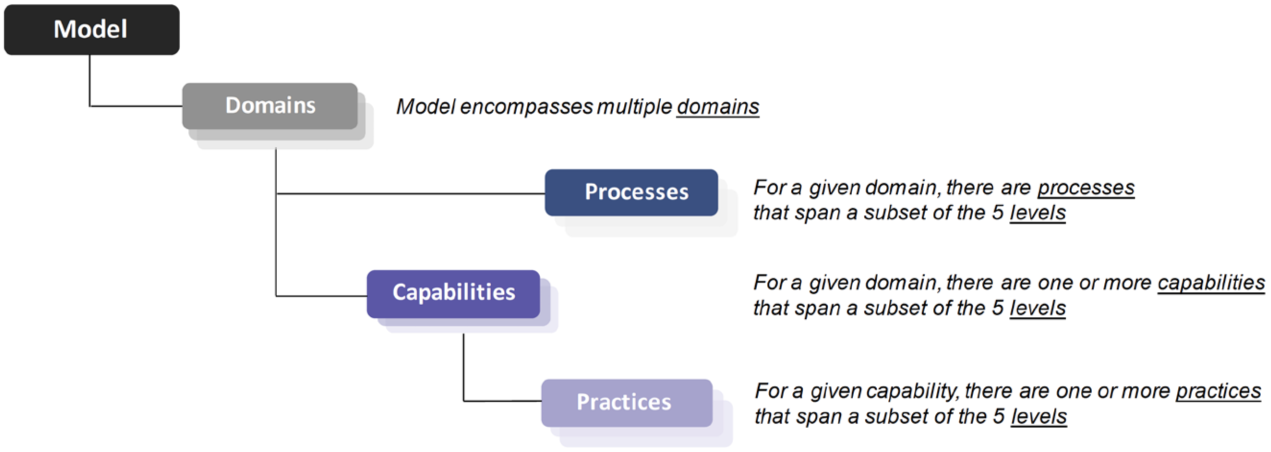


Figure 1. CMMC Model Framework (Simplified Hierarchical View)

([Source: CMMC v1.02, p. 3])

Certification Levels

CMMC also introduces five tiered certification levels to reflect increasing maturity and preparedness.

Level 1 is concerned with basic cyber hygiene for Federal Contract Information (FCI), or information provided by or generated for the government for a contract that delivers a product or service to a federal agency.

Levels 2 through 5 are concerned with protecting Controlled Unclassified Information (CUI), or information shared throughout supply chain workflows that requires controls to protect it from general public access. Higher levels are concerned with protections for increasingly sophisticated attacks. The CMMC levels are summarized below:

> **Level 1** - Safeguard FCI: implement basic cyber practices to protect FCI using basic processes that ensure they're performed.
>
> **Level 2** - Prepare for CUI Protections - deploy transitional practices and document processes to evolve from basic cyber hygiene for FCI to intermediate cyber hygiene for CUI protection.
>
> **Level 3** - Protect CUI - implement intermediate cyber hygiene practices with processes that are actively managed and monitored.
>
> **Level 4 and 5** - Reduce Risk of Advanced Persistent Threats (APTs) - implement proactive, progressive cyber security best practices to defend against sophisticated attacks on multiple vectors.

Achievement of a specific CMMC Level also requires achieving any preceding lower levels. The figure below reflects the cumulative nature of the levels:

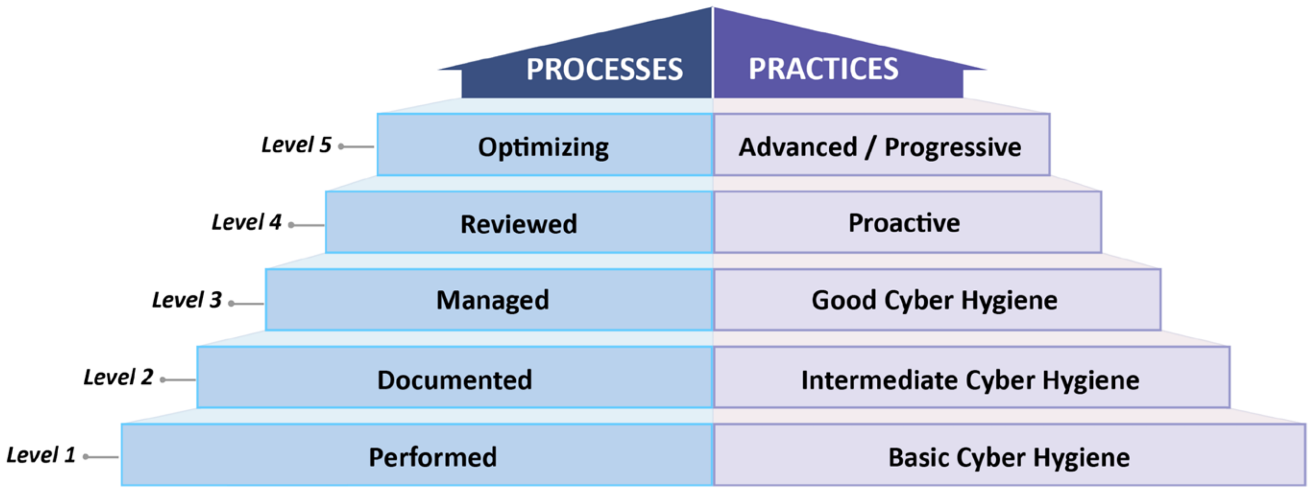


Figure 2. CMMC Levels and Descriptions

([Source: CMMC v1.02, p. 4])

CMMC'S focus on processes cultivates a future-facing cybersecurity posture that will address more advanced threats as attack vectors evolve. As the levels progress, organizations must step up their efforts in institutionalizing cybersecurity processes. The table below provides additional context on how the processes evolve throughout successive levels:

Table 2. CMMC Processes

Maturity Level	Maturity Level Description	Processes
ML 1	**Performed**	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	**Documented**	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	**Managed**	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	**Reviewed**	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	**Optimizing**	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

(Source: CMMC v1.02, p. 4)

Alignment with DFARS and NIST

In Fall 2016, the DoD included a new clause in the Defense Federal Acquisition Regulations Supplement (DFARS)—"Safeguarding Covered Defense Information and Cyber Incident Reporting" (DFARS 252.204-7012). This clause was informed by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (for more details, see Appendix 2). NIST SP 800-171 outlines specific guidelines and safeguards for protecting CUI in nonfederal information systems, and DFARS clause 252.204-7012 introduced new requirements related to incident reporting and other practices.

CMMC incorporates DFARS 252.204-7012 and NIST SP 800-171 guidelines as well as other risk mitigation practices from other standards. But crucially, the CMMC framework works to ensure the practices are implemented to align with a cybersecurity program that advances in maturity over time, as opposed to the "set it and forget it" approach of previous guidelines.

CMMC Preparedness Action Plan

Understanding the CMMC framework is a crucial first step, but with that understanding comes two key follow-up questions: What certification level should my organization prepare for? And what does my organization need to do to prepare for that CMMC Level?

Level 1 is a good starting place for most DIB firms, but beyond that, the key is understanding how frequently your firm handles CUI throughout the course of contracting, development, and miscellaneous supply chain operations. If you do frequently handle CUI, CMMC Level 3 will be your goal. For Level 3, preparedness starts with understanding how CUI is stored and shared throughout your supply chain collaboration workflows, then mapping CMMC practices to these workflows to keep CUI protected.

Importance of Email and File Protection for the Supply Chain

CUI is shared frequently and rapidly throughout supply chain collaboration workflows. Examples include communications and project management documentation shared between subprime and prime contractors, or product and engineering documentation like specifications, blueprints, or industrial designs shared internally and externally.

CUI takes many forms beyond these examples, but it is frequently stored and shared via email and files. For end users, email and files are convenient, ubiquitous collaboration tools that enable rapid CUI sharing, helping jumpstart joint development initiatives and cement partner relationships. For IT admins, email and file tools meet end-user needs while cloud-based deployments present opportunities for agility, efficiency, and cost-savings.

For the security and compliance teams that must implement appropriate CMMC processes and practices, however, cloud-based email and files present challenges. Email and file workflows often sacrifice security for ease of use and collaboration, and CUI shared via email and files in cloud environments limits security teams' visibility and control of CUI.

CUI is still almost certain to end up being stored and shared via email and files in the cloud, making email and file protection a focal point of any CMMC preparedness action plan. The two standard commercial cloud productivity platforms, Microsoft Office 365 and Google G Suite, provide email and file solutions that come with built-in security features. However, these platforms come up short of many of CMMC's requirements, so you will need to assess third-party data protection vendors to protect and control CUI and prepare for CMMC Level 3.

Email and File Protection Evaluation Criteria

The following criteria serve as a useful guide when evaluating email and file protection solutions to keep CUI protected throughout its lifecycle.

Ease of Use

Security solutions are only effective when they're adopted widely, and this is especially true for user-centric tools like email and files. To encourage widespread usage and keep your organization's CMMC posture strong, protections must be easy to use.

For email and files, ease of use means giving email senders and file owners an on-demand way to protect messages, attachments, and documents, ideally with a simple click of a button or flip of a switch.

Protections should exist within an intuitive user experience, ideally embedded within the existing email or file application's user interface (rather than requiring separate accounts, applications, or workflows). User experiences that force users to exchange keys manually cause confusion, negatively affecting usage and adoption, so key exchanges should always be transparent to end users.

End-to-End Encryption

End-to-end encryption goes beyond network-level encryption, protecting CUI within email and files down to the object level, such that only the data owner and their authorized recipients and collaborators may access the data. This is critical in cloud environments where underlying cloud vendors can access plaintext CUI, and in sharing workflows with limited control or visibility.

Appendix 1 lists several key CMMC practices in detail, but many focus on protecting CUI's confidentiality, preventing unauthorized or unintended disclosure, and ensuring information integrity. So by virtue of protecting CUI from unauthorized access, end-to-end encryption fulfills requirements for several CMMC practices at once.

Access Controls

Combining granular, persistent access controls with end-to-end encryption provides even greater assurances for CUI confidentiality and prevention of unauthorized access throughout supply chain workflows.

When sharing CUI, users should be able to disable forwarding and set expiration dates for granular control. Watermarks for files and attachments should be provided to help prevent data leaks, and persistent protection for attachments should allow data owners to maintain control even beyond the initial email. After CUI is shared, data owners should be able to revoke access immediately as partnerships and supply chains evolve.

Collaborator and Recipient Access

As a corollary to ease of use, seamless, secure access for collaborators and recipients is also an integral part of an effective CUI protection solution. Unnecessary friction within recipient experiences slows down joint development workflows and hampers innovation, frustrating supply chain partners and reducing your chances of winning defense contracts.

Recipients should be able to access protected email and files securely and easily to keep collaboration workflows productive. Don't force your partners to create new accounts and use new applications if you don't have to. Authentication should leverage existing accounts for streamlined, secure access.

Administrative Enforcement and Data Loss Prevention (DLP)

Administrators should be able to enforce end-to-end encryption and access controls automatically. On-demand end-user protections are necessary but not enough. Even the most diligent users get careless from time to time and forget to apply protections.

Your CUI protection solution should provide DLP capabilities, allowing admins to configure rules to scan email and files to detect CUI then automatically protect it before it's sent or shared. Administratively enforced protections complement end user protections to maximize the value of your security solution.

Visibility and Audit Logs

Audit and Accountability is a significant domain within CMMC with 14 separate practices, so persistent visibility into who has protected, accessed, or shared CUI throughout its lifecycle, when, where, and for how long is also key to CMMC preparedness.

As a best practice, both end users and administrators should be able to easily view granular audit trails for protected CUI throughout supply chain workflows. Audit logs of all protection, sharing, access, and control activity, as well as administrative actions, should be available for download or integration with security information and event management (SIEM) tools.

Customer-Hosted Encryption Keys

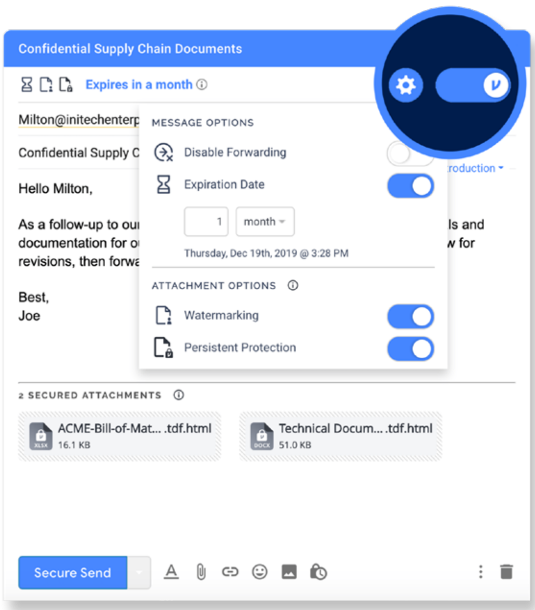
As previously discussed, storing CUI within the cloud and sharing throughout the supply chain exposes it to unauthorized access risks. Cloud vendors protect their infrastructure and networks, but not the customer CUI itself, and their personnel may obtain unauthorized access to plaintext CUI in these environments.

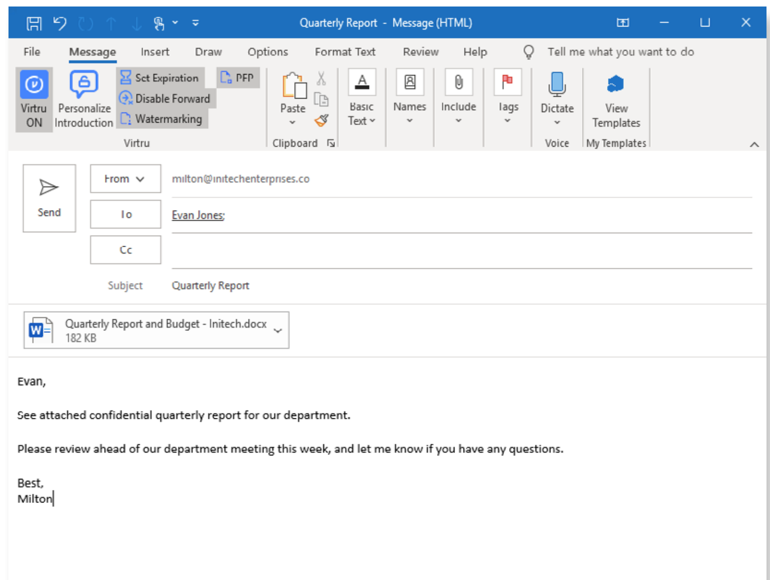
Customer-hosted keys give your organization assurances that despite these risks, you maintain ultimate control of your CUI by virtue of controlling the encryption keys protecting the CUI. Also known as "Hold Your Own Key" schemes, customer-hosted keys let you store encryption keys on-premises.

Virtru for CMMC Level 3

Virtru helps streamline your organization's preparations for CMMC Level 3 Maturity by protecting CUI from unauthorized access everywhere it's shared, with unmatched ease of use. With Virtru, CUI protection persists throughout supply chain collaboration workflows, enabling persistent enforcement and access control across all environments and applications. Virtru's data-centric protections for email and files meet a host of CMMC requirements, spanning Access Control, Audit and Accountability, Media Protection, System and Information Integrity, and more (for more details, see Appendix 1).

Solution Overview





Virtru's easy end-to-end encryption is embedded directly within Gmail and Microsoft Outlook for seamless CUI protection and control.

Unmatched Ease of Use

Virtru works seamlessly where your users already work to make CMMC readiness a breeze. Deployed as an add-in for Microsoft Outlook or a Google Chrome browser extension for Gmail and Google Drive, Virtru makes CUI protections easy for end users, giving them on-demand protections that encourage widespread adoption. Encryption and access controls are applied with a simple click of a button or flip of the switch. And unlike other end-to-end encryption solutions that require users to exchange keys manually, all Virtru key exchanges are transparent and handled securely by Virtru's hardened key management infrastructure.

End-to-End Email and File Encryption

Virtru protects messages, attachments, and files at the object-level, directly within the email or file client, to deliver end-to-end encryption. When end users encrypt CUI, Virtru generates unique symmetric encryption keys and binds them to the encrypted payload and its metadata to keep CUI protected from unauthorized disclosure or transfer, maintaining its confidentiality throughout the supply chain.

Granular, Persistent Access Controls

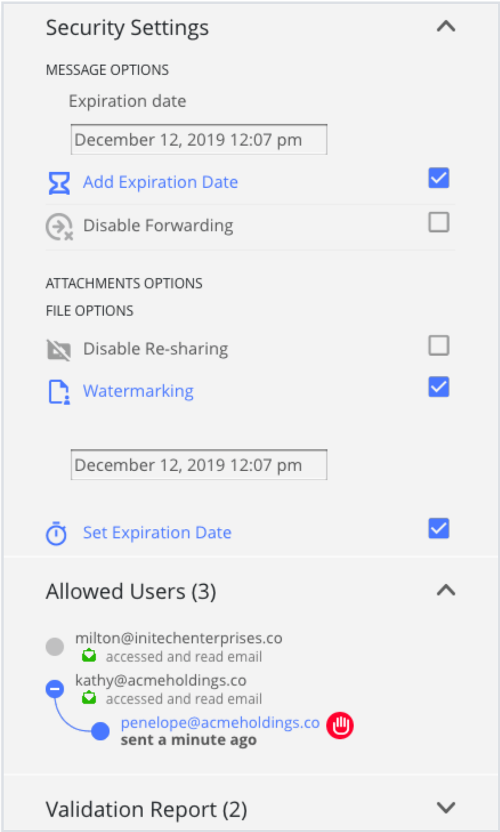
Virtru also allows end users to apply granular access controls to CUI to reinforce protections against unauthorized access. Disable forwarding and expiration help ensure CUI doesn't fall in the wrong hands as it's shared between primes, subprimes, and other mission partners. Watermarks and persistent protection can be applied to email attachments to prevent file-based leaks while facilitating sharing and collaboration where the data owner still maintains control. Access to CUI can be revoked at any time.

Seamless Sharing and Collaborator Access

With Virtru's data-centric protections and controls, contractors can share CUI confidently and seamlessly within email and file workflows. Meanwhile, recipients and collaborators get secure, easy access to CUI via the Virtru Secure Reader. While other solutions force your supply chain partners to create new passwords or accounts to access protected CUI, Virtru simply uses the email address the sender authorized when sharing the protected CUI to authenticate the recipient or collaborator. Responses sent from the Secure Reader are encrypted by default to ensure collaboration workflows keep CUI protected.

Automatic Enforcement with DLP

Virtru's end-to-end encryption and granular access controls can be enforced automatically via email DLP rules within the Virtru Dashboard. You can choose from predefined content detectors or create your own, then set rules to encrypt CUI, set expiration dates or disable forwarding, strip attachments, and much more. The Virtru Dashboard also provides a centralized portal with administrative capabilities spanning user management, protection defaults, and audit workflows.



Virtru gives end users and administrators visibility into who has accessed and shared CUI as well as comprehensive audit logs to support Audit and Accountability practices.

Persistent Visibility and Audit Reporting

Throughout supply chain collaboration workflows, Virtru allows end users and administrators to see who has accessed or shared CUI, when, where, and for how long. As supply chain collaboration evolves, this visibility helps inform access controls, adapting them to suit the context of the CUI. Audit logs of all events related to CUI, including protection, controls, sharing, access, and administrative activity, are available for export and can be integrated with SIEM tools via APIs to enable advanced forensic analysis and threat remediation workflows.

Customer Key Server

Virtru offers the Customer Key Server (CKS) to give security teams the ability to hold their own keys for stronger control over CUI stored and shared in cloud environments. The CKS rewraps the symmetric keys protecting CUI with a layer of asymmetric encryption, and the customer private key is always stored on-premises. The CKS only allows authorized personnel to access the keys, further preventing unauthorized disclosure or transfer of CUI.

The Virtru Difference

Virtru's data-centric, user-first protections give organizations a simpler, more effective method to meet CMMC requirements for CUI protection compared to alternatives.

Comparison Category	Virtru	CUI Protection Alternatives (Preveil, Microsoft GCC High)
CUI Protection and Controls	End-to-end encryption and persistent access controls protect CUI from unauthorized access during the defense contract lifecycle and throughout the supply chain. CMMC-ready CUI protections are available out-of-the-box.	Capabilities such as DLP may not be available and access controls such as revocation may be limited.
Ease of Use	Simple, on-demand protections are provided within an intuitive user experience. No new applications are required. Virtru is embedded into existing email and file applications.	Protections are not easily accessible, often buried in hidden menus or requiring administrative support. Users typically have to adapt to new apps and workflows.
Recipient and Collaborator Access	External recipients and collaborators without Virtru never have to create new accounts or passwords to access protected CUI. Simply authenticate with an existing account.	External recipients often must create a new account to access protected data, forcing collaborators to create and manage another password.
Deployment and Installation	Browser extension or add-in deploys seamlessly via managed Chrome installs or Microsoft. Simple end-user self service is also supported. Inherits groups/OUs from existing platform to streamline administration.	End users may need to download software to their desktop, in addition to a browser extension. Users may not have access to expected functionality without extensive configuration.

Comparison Category	Virtru	CUI Protection Alternatives (Preveil, Microsoft GCC High)
Audit	End users can view who has accessed CUI and revoke it, strengthening security awareness and CMMC preparedness. Administrators can download audit logs for analysis or configure the Virtru Audit Export API to integrate with SIEMs.	End users have little visibility into who has accessed CUI. Admins have access to encrypted audit logs but SIEM integrations are not always available.
Customer-Hosted Encryption Keys	Customer Key Server (CKS) lets customers hold private keys protecting all data on-premises for ultimate security. Lightweight deployments integrate easily with other key security infrastructure components.	Not supported OR requires significant administrative complexity and trade-offs with other critical security features (e.g. anti-phishing, anti-malware).
Cost	Priced per user, per year at a competitive price point, with deployment and support services included.	Priced per user, per month at a relatively higher price point. Typically requires added services costs for customization and configuration.

Keep CUI Protected Everywhere It's Shared and Unlock Innovation with Virtru

Virtru's persistent CUI protections, secure sharing workflows, and seamless user experiences give defense contractors a head start on CMMC Level 3 preparedness. But even more importantly, Virtru suports easy, secure collaboration that ensures contractors can share data with confidence throughout the supply chain, powering the development of innovative products, services, and operations that provide a competitive advantage.

If your organization is interested in learning how Virtru can jumpstart your preparations for CMMC Level 3, contact us to see how easy it is to keep CUI protected and under your control throughout the supply chain.

About Virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.

Appendix 1 - Virtru Support for Level 3, 4, and 5 CMMC Practices

The table below provides a detailed explanation of the CMMC practices from Levels 3, 4, and 5 that Virtru capabilities align with and support most directly, grouped by domain.

Note that some of these capabilities will require additional configuration to ensure they align with CMMC requirements, and many practices not listed below are already supported by services adjacent to Virtru, such as the underlying email and file platform provider or technology partners. Also note that while Virtru supports many practices within Levels 1 and 2, this appendix focuses on Levels 3, 4, and 5, aligned with the broader context of this guide regarding CUI protection.

CMMC Domain and Practice	Practice Description	Explanation of Virtru Support
Access Control AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Virtru logs the execution of all end-user and administrative actions for comprehensive audit reporting.
Access Control AC.3.022	Encrypt CUI on mobile devices and mobile computing platforms.	Virtru provides a mobile application to enable encryption of email messages and attachments containing CUI shared via mobile device.
Asset Management AM.3.036	Define procedures for the handling of CUI data.	Virtru's administratively enforced DLP allows configuration of automated procedures for protecting and controlling CUI. Administrative controls and restrictions also limit who can access CUI throughout the organization.
Audit and Accountability AU.3.048	Collect audit information (e.g. logs) into one or more central repositories.	Virtru end-user and administrator activity event logs are centralized within the Virtru platform.
Audit and Accountability AU.3.049	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Virtru administrators are authenticated and authorized before accessing audit logs to prevent potential modification or deletion.

CMMC Domain and Practice	Practice Description	Explanation of Virtru Support
Audit and Accountability AU.3.050	Limit management of audit logging functionality to a subset of privileged users.	Only Virtru super-administrators and sub-administrators that super-administrators have authorized can access audit logs.
Audit and Accountability AU.3.051	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activities.	Virtru audit logs can be exported or integrated into a SIEM tool to perform correlation, analysis, and threat remediation in the event of malicious activities.
Configuration Management CM.4.073	Employ application whitelisting and an application vetting process for systems identified by the org.	During deployment and configuration, Virtru deployment engineers review the customer's systems to ensure only trusted domains will interact with the services helping protect CUI.
Media Protection MP.3.124	Control access to media containing CUI and maintain accountability for media during transport out of controlled areas.	Virtru's end-to-end encryption protects media that often contains CUI (email messages, attachments, and files), and granular controls ensure only authorized parties can access that media.
Media Protection MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Virtru's end-to-end encryption provides a leading-edge cryptographic method for preventing unauthorized access to CUI stored on digital media throughout its lifecycle.
System and Communication Protection SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Virtru's cryptographic libraries leverage FIPS-validated modules when performing end-to-end encryption on CUI, preserving its confidentiality.

CMMC Domain and Practice	Practice Description	Explanation of Virtru Support
System and Communication Protection SC.3.181	Separate user functionality from system management functionality.	Virtru administrative workflows (e.g user management, DLP policy configuration, default protection settings) are always performed separately from all end-user functionality.
System and Communication Protection SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Virtru's end-to-end encryption and access controls ensure CUI stays protected in-transit as it's shared with supply chain collaborators, preventing disclosure to unauthorized parties.
System and Communication Protection SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Virtru's hosted key management infrastructure establishes a thorough split-knowledge architecture for managing encryption keys that protect CUI and the policies that control who can access it.
System and Communication Protection SC.3.191	Protect the confidentiality of CUI at rest.	In addition to in-transit protection, Virtru's end-to-end encryption and access controls ensure CUI is protected and confidential at rest as it's stored in email and file systems.
System and Information Integrity SC.3.219	Implement email forgery protections.	With Virtru's end-to-end encryption, email is encrypted directly within the email client, before it interacts with external components or potential bad actors. This prevents forgery or other integrity attacks since the plaintext email content is obscured with ciphertext.

Appendix 2 - Virtru Support for NIST SP 800-171 Security Requirements and DFARS 252.204-7012

The table below provides a detailed explanation of the security requirements within NIST SP 800-171 for protecting the confidentiality of CUI in nonfederal systems and organizations that Virtru capabilities align with and support most directly, grouped by security requirement family. NIST requirements also cover DFARS requirements, as paragraph (b)(2)(i) within DFARS 252.204-7012 states that "the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171."

Note that some of these capabilities will require additional configuration to ensure they align with NIST requirements, and many practices not listed below are already supported by services adjacent to Virtru, such as the underlying email and file platform provider or technology partners.

NIST Security Requirement	Requirement Description	Explanation of Virtru Support
Access Control 3.1.3	Control the flow of CUI in accordance with approved authorizations.	Virtru encrypts CUI directly within the email and file client, controlling CUI by preventing access to CUI in the clear by unauthorized parties and limiting information transfers to only authorized users.
Access Control 3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Virtru administrators are authenticated and authorized before making any privileged administrative changes. Virtru logs the execution of all end-user and administrative actions for comprehensive audit reporting.
Access Control 3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	Virtru provides a mobile application to enable encryption of email messages and attachments containing CUI shared via mobile device.

NIST Security Requirement	Requirement Description	Explanation of Virtru Support
Audit and Accountability 3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	All Virtru end-user and administrator activity and events are logged continuously and centralized within the Virtru platform.
Audit and Accountability 3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	Virtru event logs always associate system activations to a specific individual user or administrator to allow direct follow-up with that person and remediate accidental or malicious actions.
Audit and Accountability 3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Virtru audit logs can be exported or integrated into a SIEM tool to perform correlation, analysis, and threat remediation in the event of malicious activities.
Audit and Accountability 3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Virtru administrators are authenticated and authorized before accessing audit logs to prevent potential modification or deletion.
Audit and Accountability 3.3.9	Limit management of audit logging functionality to a subset of privileged users.	Only Virtru super-administrators and sub-administrators that super-administrators have authorized can access audit logs.
Configuration Management 3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	During deployment and configuration, Virtru deployment engineers review the customer's systems to ensure only trusted domains will interact with the services helping protect CUI.

NIST Security Requirement	Requirement Description	Explanation of Virtru Support
Media Protection 3.8.1	Protect (i.e. physically control and securely store) system media containing CUI, both paper and digital.	Virtru's end-to-end encryption protects media that often contains CUI (email messages, attachments, and files), and granular controls ensure only authorized parties can access that media.
Media Protection 3.8.5	Control access to media containing CUI and maintain accountability for media during transport out of controlled areas.	Virtru's access controls and audit capabilities allow owners of CUI to view who has accessed CUI throughout collaboration workflows and hold users accountable for malicious activity. Data owners have the ability to revoke access to CUI immediately.
Media Protection 3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Virtru's end-to-end encryption provides a leading-edge cryptographic method for preventing unauthorized access to CUI stored on digital media throughout its lifecycle.
System and Communications Protection 3.13.3	Separate user functionality from system management functionality.	Virtru administrative workflows (e.g user management, DLP policy configuration, default protection settings) are always performed separately from all end-user functionality.
System and Communications Protection 3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Virtru's end-to-end encryption and access controls ensure CUI stays protected in-transit as it's shared with supply chain collaborators, preventing disclosure to unauthorized parties.

NIST Security Requirement	Requirement Description	Explanation of Virtru Support
System and Communications Protection 3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Virtru's hosted key management infrastructure establishes a thorough split-knowledge architecture for managing encryption keys that protect CUI and the policies that control who can access it.
System and Communications Protection 3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Virtru's cryptographic libraries leverage FIPS-validated modules when performing end-to-end encryption on CUI, preserving its confidentiality.
System and Communication Protection 3.13.16	Protect the confidentiality of CUI at rest.	In addition to in-transit protection, Virtru's end-to-end encryption and access controls ensure CUI is protected and confidential at rest as it's stored in email and file systems.