Complying with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC)

Executive Summary

The Director of National Intelligence's annual *Worldwide Threat Assessment* report has for several years identified cyber threats as one of the most important strategic threats facing the United States. The Department of Defense (DoD) is keenly aware of the multifaceted cyber threats our nation faces and has created CMMC to better defend the vast attack surface that the Defense Industrial Base (DIB) sector presents to adversaries.

DoD is taking a supply-chain risk-management approach to improving cybersecurity. That means that all 300,000 DoD contractors will need to obtain third-party certification that they meet requirements for the CMMC maturity level appropriate to the work they wish to do for the DoD.

Current commercial email and file sharing solutions in the market are insufficient to comply with CMMC for organizations working with Controlled Unclassified Information (CUI). Better alternatives use end-to-end encryption to protect data 100% of the time.

The Department of Defense has created CMMC to better defend the vast cyberattack surface that the Defense Industrial Base sector presents to adversaries.

This paper provides a high-level overview of the new CMMC framework and its key components. It also answers the pressing question of what your company needs to do to comply with CMMC and, likewise, work with the DoD. Next, fundamental cyber security principles and how they connect with CMMC are explained. The paper's final section outlines key features of PreVeil, an affordable solution to keep your company compliant with DoD regulations.

CMMC Overview

CMMC measures an organization's ability to protect Federal Contract Information (FCI) and CUI. FCI is information not intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government. CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with federal law, regulations, and government-wide policies.

CMMC combines various cybersecurity standards already in place, and others, and maps these best practices and processes to five maturity levels ranging from basic cyber hygiene practices at Level 1 to highly advanced practices and processes at Level 5.

CMMC Model Framework

The CMMC model framework categorizes cybersecurity best practices into 17 broad *domains*, such as "Access Control" and "Systems and Communications Protection." Forty-three distinct *capabilities*, such as "control remote system access" and "control communications at system

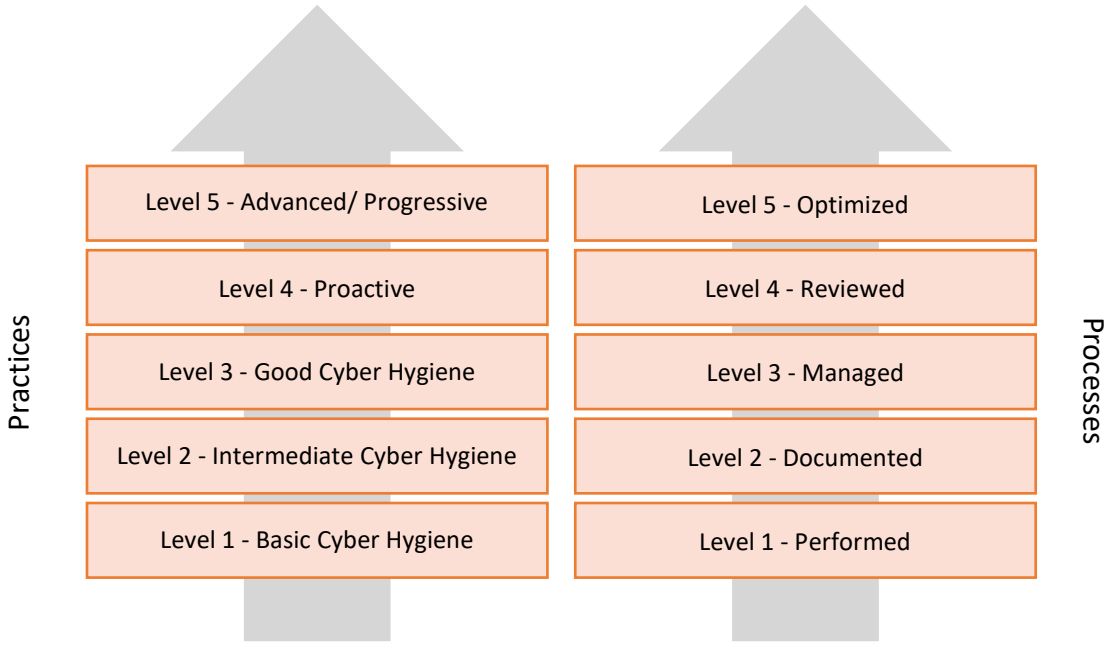
boundaries," are distributed across the 17 domains. Not all companies need to demonstrate all 43 capabilities; they apply depending on the maturity level sought.

Companies will demonstrate compliance with the required capabilities by showing adherence to a range of practices and processes. *Practices* are the technical activities required within any given capability requirement; 173 practices are mapped across the five CMMC maturity levels. *Processes* serve to measure the maturity of organizations' institutionalization of cybersecurity procedures; nine processes are mapped across the five CMMC maturity levels.

CMMC Levels

CMMC's five defined levels of cybersecurity maturity, each with a set of supporting practices and processes, are shown in Figure 1 below. Practices range from basic cyber hygiene at Level 1 to advanced and progressive cyber hygiene at Level 5. In parallel, process levels range from simply performed at Level 1 to optimized at Level 5.

Figure 1: CMMC Maturity Level Descriptions



Note that DoD contractors must meet requirements for the level they seek in both the practice and the process realms. For example, a contractor that achieves Level 3 on practice implementation and Level 2 on process institutionalization will be certified at the lower CMMC Level 2.

Companies that work with or generate CUI need to achieve CMMC Level3. The DoD explains:

> An organization assessed at Level 3 will have demonstrated good cyber hygiene and effective implementation of controls that meet the security

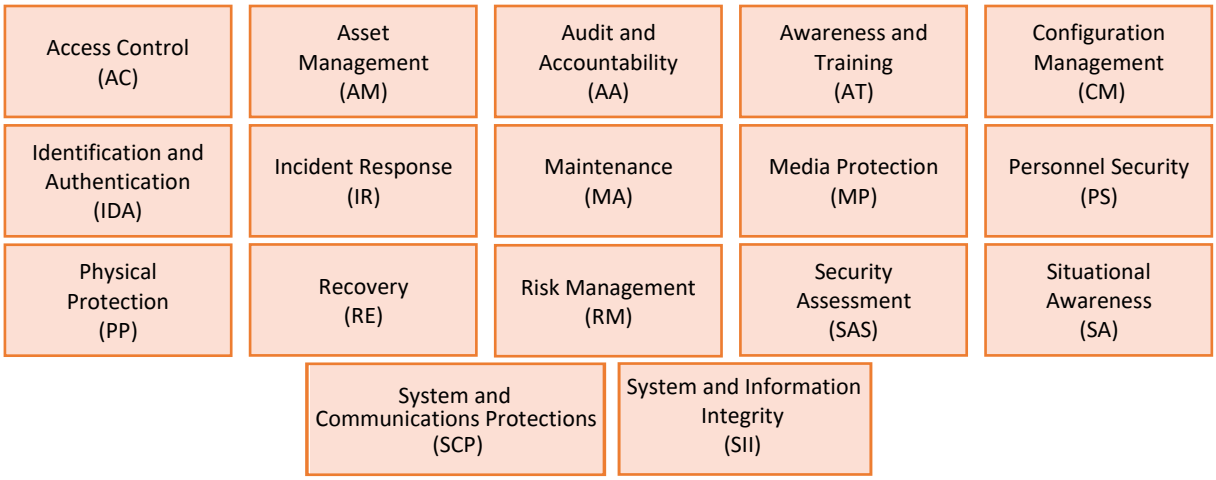
requirements of NIST SP 800-171 Rev 1[1]…Level 3 indicates a basic ability to protect and sustain an organization's assets and CUI; however, at Level 3, organizations will have challenges defending against advanced persistent threats (APTs). Note that organizations subject to DFARS Clause 252.204-7012[2] will have to meet additional requirement for Level 3, such as incident reporting.

For process maturity certification, a Level 3 organization is expected to adequately resource activities and review adherence to policy and procedures, demonstrating active management of practice implementation.[3]

CMMC Domains

The CMMC model consists of 17 domains, shown in Figure 2 below, the majority of which originated from FIPS SP 200[4] security-related areas and the NIST SP 800-171 control families.

Figure 2: CMMC Model Domains



[1] NIST SP 800-171 Rev. 1 refers to a revision of the National Institute of Standards and Technology Special Publication 800-171, entitled *Protecting CUI in Non-Federal Information Systems and Organizations*. It codifies the requirements that any non-federal computer system must follow in order to store, process or transmit CUI or provide security protection for such systems.

[2] DFARS Clause 252.204-7012 refers to a clause in a Defense Federal Acquisition Regulation Supplement entitled *Safeguarding Covered Defense Information and Cyber Incident Reporting*. It requires contractors to provide "adequate security" for covered defense information that is processed, stored or transmitted on the contractor's internal information system or network.

[3] Cybersecurity Maturity Model Certification Version 0.7, p. 3.

[4] FIPS 200 refers to the Federal Information Processing Standard Publication 200, entitled *Minimum Security Requirements for Federal Information and Information Systems*. It outlines mandatory federal standards for baseline security controls.

Again, 43 capabilities are distributed across these 17 CMMC domains, and the 173 practices associated with those capabilities are mapped across the five CMMC maturity levels.

CMMC Process Maturity

In addition to cybersecurity practices, CMMC will measure the maturity of organizations' institutionalization of cybersecurity processes. Level 1 has no maturity requirements related to institutionalization. Nine processes indicating increasingly more maturity are mapped across the remaining levels, which can be captured briefly as:

- Level 1: Performed (but no further process maturity requirements)
- Level 2: Documented
- Level 3: Managed
- Level 4: Reviewed
- Level 5: Optimized

Note that each required process applies to each domain individually. For example, the requirement that high-level management be informed of any issues within a domain requires 17 such formalized processes for doing so (given 17 domains).

Finally, adherence to CMMC practices and processes is cumulative. Once a practice or process is introduced in a level, it becomes required for all levels above that as well. Thus, for example, for an organization to achieve Level 3, all the practices and processes defined in Levels 1, 2 and 3 must be achieved. DoD Prime contractors must flow down the appropriate CMMC level requirement to their sub-contractors, which will vary depending on the nature of the subcontractors' work. For example, a prime contractor with CMMC Level 5 certification could have a subcontractor with which it shares just FCI; the DoD would require that subcontractor to achieve Level 1 certification.

What does my company need to do?

All DoD contractors will need to be CMMC certified. One of the most significant changes from previous practice is the shift from self-assessment to external assessments of cybersecurity compliance, which will be conducted by Third Party Assessment Organizations (C3PAOs). Further, whereas in the past noncompliance with DoD security regulations was acceptable as long as companies prepared POAMS (Plan of Action and Milestones) outlining plans to address deficiencies, that will no longer be the case under CMMC.[5]

Clearly, business risk is high any company that does work for the DoD needs to take action.

First, if you haven't already, familiarize yourself with CMMC and stay abreast of developments. CMMC 1.0 and its helpful, detailed appendicies were released in late January 2020 and are available on the DoD's CMMC website.

[5] Companies will still need to complete SSPs (System Security Plans), although those too will not satisfy CMMC requirements.

Next, determine the appropriate CMMC level for your company. It appears most likely that companies that handle just FCI will need to achieve Levels 1 or 2. Any company that handles CUI will need to achieve at least Level 3. Higher Levels 4 and 5 will focus on reducing the risk of advanced persistent threats (APTs) and are intended to protect CUI associated with DoD critical programs and technologies.

If your business has migrated to the cloud, standard commercial cloud services such as Microsoft Office 365 and Gmail are not CMMC compliant and so you will need to assess alternatives.

Once you determine the CMMC level you want to achieve, examine the current state of your cybersecurity and identify gaps between your organization's capabilities and the requirements for the level you seek. This gap analysis could be based on previous self-assessments, such as the NIST SP 800-171 Self-Assessment. However, a more forward-looking approach would be to consult Appendix A of the CMMC 1.0 report. That appendix includes a summary of the process requirements for each of the five CMMC levels, as well as a matrix that lists each domain's required capabilities and the corresponding practices for each level.

Note that if your business has migrated to the cloud, standard commercial cloud services such as Microsoft Office 365 and Gmail are not CMMC compliant and so you will need to assess alternatives.

As your business considers how to address its cybersecurity deficiencies, keep in mind that with the adoption of CMMC, cybersecurity will be an allowable cost. This shift recognizes the critical nature of cybersecurity and serves as an incentive for vendors to quickly comply with CMMC. Begin building budgets for what it will take to upgrade your cybersecurity to the level you need and figure out how those costs will affect your rates.

It is crucial to understand that the timetable for implementation of CMMC is rapid. The DoD is aiming to add CMMC requirements to RFPs in October 2020, starting with 15 procurements for critical DoD programs and technologies, such as those associated with nuclear and missile defense. It is expected that approximately 1,500 primes and subcontractors will be affected and, likewise, will need to be CMMC certified by Fall 2021. The roll-out will continue over a five-year period, with the expectation that all new DoD contracts will include CMMC requirements by Fall 2026. DoD will identify the required CMMC level in RFP sections L and M and use responses there as the basis of a "go/no go" decision.

CMMC: Aiming for the Fast Track

DoD is pursuing an aggressive timeline for CMMC, starting with a focus on critical programs.

- January 2020: Release of CMMC Version 1.0
- April to June 2020: Capacity building of third party assessors (C3PAOs)
- July 2020: C3PAO market place opens
- October 2020: CMMC requirements incorporated into 15 procurements for critical DoD projects, and used as the basis for "go/no-go" decisions.

As of October 2020, the DoD expects that companies seeking to work on critical DoD programs and technologies will have to be CMMC certified by a C3PAO. This could impact approximately 1,500 primes and subcontractors.

You needn't take on CMMC compliance on your own. Many consulting companies have adapted their services to address CMMC requirements and can help your company by, for example, conducting a gap analysis focused on your cybersecurity practices and/or processes. They can also help you build a roadmap for moving forward toward compliance.

Technical Cybersecurity Principles and CMMC

Cybersecurity research at leading universities has led to critical advances in applied cryptography. These new technologies, built on the fundamental security principles outlined below, will enable your company to enhance its cybersecurity and achieve the CMMC level necessary to do work for the DoD. Specific CMMC domains addressed by each security principle are noted.

New technologies will enable your company to enhance its cybersecurity and achieve the CMMC level necessary to do work for the DoD.

End-to-end encryption

End-to-end encryption ensures that data is encrypted on the sender's device and never decrypted anywhere other than on the recipient's device. This ensures that only the sender and the recipient can ever read the information being shared–and no one else. Data is never decrypted on the server, thus even if attackers successfully breach the server, all they will get is gibberish.

End-to-end encryption addresses the following CMMC domains: Access Control, Configuration Management, Media Protection, Systems & Communications Protection, and System & Informational Integrity.

Encrypted logs

All user activities should be logged in order to trace possible malicious activities. Logs themselves also should be tamper-proof and protected with end-to-end encryption so that attackers cannot glean information by viewing log entries, nor can they cover their tracks by deleting log entries.

Encrypted logs address the following CMMC domain: Audit & Accountability.

End-to-end encryption enables organizations to store sensitive information, like CUI, in the cloud because information is always completely encrypted on the server.

Cloud-based services

Cloud-based services offer significant advantages over on-premises servers, such as lower costs, better scalability, and fewer administrative and maintenance responsibilities. However, many organizations have been reluctant to trust sensitive information to the cloud. End-to-end encryption enables organizations to store sensitive information, like CUI, in the cloud because information is always completely encrypted on the server. Further, the server can never access decryption keys. No one but intended recipients can access the data, not even the cloud service provider.

Cloud-based services can help address the following CMMC domain: Maintenance & Recovery.

Key-based authentication

Passwords create a significant security risk because they are routinely phished, guessed or stolen. Compromised passwords are used for unauthorized access, escalating privileges, or impersonating a user's identity. A much better approach is to authenticate users with private keys that are stored only on the user's device. Unlike passwords, these keys cannot be guessed or stolen.

Moreover, device-based keys prevent hackers from remotely accessing user accounts. Since attackers cannot get to the keys, they cannot access data in users' accounts. If devices are lost or stolen, device management controls should allow admins to quickly disable them.

Passwords create a significant security risk because they are routinely phished, guessed or stolen. A much better approach is to authenticate users with private keys that are stored only on the user's device.

Key-based authentication can help address the CMMC domains: Identification & Access, System & Communications Protection, and Systems & Informational Integrity.

Administrative distributed trust

In most IT systems, administrators hold the proverbial keys to the kingdom, given that they most often have access to any user account in the enterprise. As such, they become a focal point of attack, and when an attacker compromises the administrator, they gain access to the entire organization's information.

A better approach is to require several people to approve an administrator's sensitive activities (such as exporting corporate data). Much like the nuclear launch keys, requiring several people to authorize critical actions can help prevent malicious activity. In essence, trust is distributed amongst approvers instead of being centralized with one admin. Distributed trust eliminates central points of attack.

Much like the nuclear launch keys, requiring several people to authorize critical actions can help prevent malicious activity.

It's also important to note that eliminating central points of attack is a fundamental means to secure systems. For example, some encryption systems centralize the storage of decryption keys in a key server. Doing so undermines the benefits of encryption because attackers can focus their efforts on penetrating the key server, which if successful would ultimately compromise all of the encrypted data.

Administrative distributed trust addresses the following CMCC domains: Access Control and Systems & Communications Protection.

Controlled access

Most email and file sharing services are open to anyone, which enables phishing, spoofing, and other kinds of attacks. When an encrypted email and file sharing service is added to complement (instead of replace) regular email and files, access can be restricted to only trusted individuals. These people form a "trusted community" that allows organizations to control the flow of CUI. Individuals outside the trusted community are blocked from sending or receiving encrypted information.

Controlled access addresses the following CMMC domains: Configuration Management, Systems & Communications Protection, and Systems & Informational Integrity.

PreVeil Product Overview

PreVeil is based on MIT computer scientists' research on cybersecurity and applied cryptography. It adheres to each of the fundamental cybersecurity principles outlined above, beginning with the gold standard of end-to-end encryption to protect email, files and data—even when networks or servers are breached, and administrators are compromised. PreVeil's encrypted Email and Drive support compliance with virtually all the CMMC mandates related to the communication and storage of CUI. (See Appendix A, *PreVeil CMMC Level 3 Compliance Matrix*, a table that lists each of the required capabilities for CMMC Level 3 and indicates which requirements PreVeil meets.)

Email

PreVeil Email lets you send and receive encrypted emails using your existing email address. It integrates with mail clients such as Outlook, Gmail, and the Apple Mail, and also works on browsers and mobile devices. When PreVeil Email is used with Outlook, Gmail, or Apple Mail, the installation process automatically creates a new set of mailboxes for your encrypted messages. Messages in these new mailboxes are encrypted and stored on PreVeil's servers. There are no changes to the mailboxes already in your mail program and no impact on the servers that store your regular, unsecure messages.

File sharing

PreVeil Drive enables end-to-end encrypted file sharing and storage. Users can access files stored on PreVeil Drive from any of their devices or share files with other users who have the appropriate access permissions through PreVeil's Trusted Communities. Unlike Box, OneDrive, Google Drive, and DropBox, which always have access to your data, only you and the people with whom you've explicitly shared files can decrypt them. PreVeil Drive also integrates seamlessly with Windows File Explorer and Mac Finder.

Elimination of passwords

Instead of relying on passwords, PreVeil authenticates users via strong cryptographic keys that are automatically created and stored on users' devices. Replacing passwords with cryptographic keys shuts down the many significant security risks that flow from phishing and password-guessing attacks, including the use of compromised passwords for unauthorized access and malicious activity. And because the keys are stored are user's devices, there is no one central point of attack for hackers to target.

Administration console

Using PreVeil's Admin Console, IT administrators can create, modify, and delete users and groups, as well as set organization-wide data and recovery policies. Device management controls let admins disable lost or stolen devices quickly. Even though all files and emails are encrypted, admins have the tools they need to manage and access their organization's data. They can view activity logs and decrypt and export user data only with permission from a PreVeil Approval Group.

Cloud-based service

Many organizations have avoided the cloud, keeping their email and file servers on premise because they don't trust the security of cloud-based solutions. PreVeil's end-to-end encryption gives organizations the best of both worlds: end-to-end encryption that is even more secure than on-premise deployments, combined with the cost, scalability and agility of the cloud.

PreVeil runs on Amazon Web Services' Gov Cloud, which provides the foundation for many of the controls required to process and store CUI. Again, end-to-end encryption ensures that no one but intended recipients—not even PreVeil or Amazon—an ever access user data.

Email and file sharing compliance

PreVeil makes it easy to comply with CMMC rules for handling CUI—in contrast to Microsoft and Google services.

Microsoft Office 365 does not meet CMMC's demands for securing email and files. One option is Microsoft's GCC High service, which is expensive per user, must be deployed across an entire organization, and requires a fork-lift upgrade to mail and file servers. Alternatively, PreVeil Email and Drive address requirements for CUI at a fraction of the cost, can be deployed only to users who handle CUI, and can be implemented with no changes to existing email and file servers.

Google's standard Gmail platform also doesn't comply with CMMC requirements for securing CUI. PreVeil supplements Gmail by adding end-to-end encryption, so neither Google nor PreVeil can access user data. The PreVeil plug-in for Gmail lets users send and receive encrypted messages all within the standard Gmail browser app.

See Appendix B, *Comparison of PreVeil vs. Alternatives,* for a comparison of PreVeil and Microsoft GCC High.

Ease of use

PreVeil is easy for end users to adopt because it works with the tools they already use. Email can be integrated with Outlook, Gmail, or Apple Mail clients. File sharing works like DropBox and is integrated with the Windows File Explorer and Mac Finder.

Cost effectiveness

PreVeil's email and file sharing service is a fraction of the cost of alternatives. Moreover, PreVeil need be deployed only to users handling CUI, whereas alternatives require deployment across an entire organization. Finally, PreVeil does not impact existing mail and file servers, making configuration and deployment simple and inexpensive.

Conclusion

The new CMMC framework will better arm the DoD in its efforts to defend against cyberattacks that threaten U.S. advantages in the military, technological and commercial realms. CMMC's implementation is on the fast track, and whether your company can continue to work with the DoD will be determined by whether it can achieve the appropriate CMMC maturity level for the contract you seek. In short, as of October 2020, CMMC certification will serve as the basis of a "go/no-go" decision for DoD contracts, beginning with those related to critical DoD programs and technologies.

All DoD contractors, regardless of size, will need to comply with CMMC requirements. To help them do so, PreVeil leverages a fundamentally better security paradigm. But better security isn't enough: if security is difficult to use, it won't be used. To be effective, security must be as frictionless as possible. PreVeil was created with this principle in mind so that your security objectives will be met. It integrates seamlessly with the email and file sharing tools you and your employees already use.

With CMMC upon us, the good news is that PreVeil's encrypted Email and Drive offerings support compliance with virtually all of the CMMC mandates related to the communication and storage of CUI.

PreVeil's principles: Grounded in the reality of today's security environment

- Uncompromising end-to-end encryption—data is never decrypted in the cloud
- Elimination of central points of attack—trust is distributed amongst the admin team
- No more passwords—impossible-to-crack cryptographic keys automatically created instead
- Secure activity logs—attackers can neither glean information nor cover their tracks
- Ease of use—effective security must be as frictionless as possible

To learn more about PreVeil, visit us at preveil.com/contact.

Appendix A:
PreVeil CMMC Level 3 Compliance Matrix

Appendix A Summary: PreVeil to CMMC Level 3 Mapping

CMMC Domain	Supports Compliance	Alternative Approach Supports Compliance (*)	Partially Complies - Additional Controls/ Processes Necessary (*)	Does Not Apply- Out of Scope	Total
Access Control (AC)	15		2	5	22
Asset Management (AM)				1	1
Audit and Accountability (AA)	9		1	1	11
Awareness and Training (AT)				3	3
Configuration Management (CM)	5	4			9
Identification and Authentication (IA)	4	6	1		11
Incident Response (IR)			1	6	7
Maintenance (MA)	2		1	3	6
Media Protection (MP)	5			3	8
Personnel Security (PS)	2				2
Physical Protection (PE)	6				6
Recovery (RE)	2		1		3
Risk Management (RM)				6	6
Security Assessment (CA)			4	1	5
Situational Awareness (SA)				1	1
System and Communications Protection (SC)	12		1	6	19
System and Information Integrity (SI)	3		1	6	10
Total	**65**	**10**	**13**	**42**	**130**

*See detailed mapping in Appendix A for explanation.

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
AC.1.001	Access Control (AC)	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	**Yes Supports Compliance**	PreVeil account required to access system. Private, device-based key authentication cryptographically enforces access rights. Trusted Community feature eliminates any spoofing or accidental communication into or out of the system. Device Management provides for control over active devices. Organization-specified Admin roles and Approval Groups required for invasive Admin actions.	3.1.1
AC.1.002	Access Control (AC)	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	**Yes Supports Compliance**	PreVeil can be deployed for a subset of organization users that need the highest level of security. File/Folder permissions are enforced cryptographically. Admin Console only accessible by specified Admins. All system actions are logged. Shared Folders with encrypted contents can be restricted to user groups on a need-to-know basis.	3.1.2
AC.1.003	Access Control (AC)	Verify and control/limit connections to and use of external information systems.	**Yes Supports Compliance**	Access to PreVeil is limited to authorized users determined by the organization. Additionally users can be added/deleted as needed by Administrators. Through a white-listing process, Trusted Communities further limits who can access the PreVeil service for an organization.	3.1.20
AC.1.004	Access Control (AC)	Control information posted or processed on publicly accessible information systems.	**Does Not Apply Out of Scope**		3.1.22
AC.2.005	Access Control (AC)	Provide privacy and security notices consistent with applicable CUI rules.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil is developing additional functionality for CUI privacy and security notices and plans to have this embedded in the offering by mid 2020. In the meantime, this mandate can be addressed outside of PreVeil.	3.1.9
AC.2.006	Access Control (AC)	Limit use of organizational portable storage devices on external information systems.	**Does Not Apply Out of Scope**		3.1.21
AC.2.007	Access Control (AC)	Employ the principle of least privilege, including for specific security functions and privileged accounts.	**Yes Supports Compliance**	Only Administrators can access Admin functions and only a cryptographic controlled Approval Group of Administrators can perform system actions that would delete or decrypt enterprise data.	3.1.5

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
AC.2.008	Access Control (AC)	Use non-privileged accounts or roles when accessing nonsecurity functions.	**Yes Supports Compliance**	Users only have a single secure account in their organization with appropriate privileges. Administrative Approval Groups protect against inappropriate access or deletion by an individual Administrator. Standard non-encrypted email and file storage/sharing can still be seamlessly utilized for communication and storage of data that is not CUI.	3.1.6
AC.2.009	Access Control (AC)	Limit unsuccessful logon attempts.	**Yes Supports Compliance**	There is no log-in for PreVeil so it inherently limits unsuccessful longon attempts. Multiple attempts at log-in by attackers are not possible. Only devices that have the user's private key can access the system. If a user does not have an authorized device in their possession and proper access to that device, they cannot even view the CUI. Remote access by an unauthorized 3rd party is virtually impossible.	3.1.8
AC.2.010	Access Control (AC)	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	**Partially Complies Additional Controls/Processes Necessary**	This mandate can be addressed outside of PreVeil via device level timeouts after a period of inactivity. PreVeil sessions can be locked remotely as required by users or Administrators.	3.1.10
AC.2.011	Access Control (AC)	Authorize wireless access prior to allowing such connections.	**Does Not Apply Out of Scope**		3.1.16
AC.2.013	Access Control (AC)	Monitor and control remote access sessions.	**Yes Supports Compliance**	Administrators can control remote sessions via device management from the AdmAll PreVeil sessions, local and remote, are controlled via end-to-end encryption. Additionally, administrators can manage and control all active devices as well as PreVeil web access sessions via device management from the Admin Console.in Console. End-to-end encryption controls access to remote access sessions.	3.1.12
AC.2.015	Access Control (AC)	Route remote access via managed access control points.	**Does Not Apply Out of Scope**		3.1.14
AC.2.016	Access Control (AC)	Control the flow of CUI in accordance with approved authorizations.	**Yes Supports Compliance**	End to end encryption with device based keys provides tools for control of CUI at the user and device level. Only those granted access can view the information. End to end encryption provides complete security of data at the server level whether on-premise or in the cloud. Trusted Community feature can limit access to CUI.	3.1.3

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
AC.3.017	Access Control (AC)	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	**Yes Supports Compliance**	Only Administrators can access Admin functions and only a cryptographically controlled Approval Group of Administrators can perform system actions that would delete or decrypt enterprise data.	3.1.4
AC.3.018	Access Control (AC)	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	**Yes Supports Compliance**	Users only have a single account with appropriate privileges. Administrative Approval Groups protect against inappropriate access or deletion. Shared Folders permit sensitive content to be shared only with users on a need to know basis. All system actions are logged (logs are encrypted and hash-chained to prevent tampering).	3.1.7
AC.3.019	Access Control (AC)	Terminate (automatically) a user session after a defined condition.	**Does Not Apply Out of Scope**	Note that PreVeil sessions can be terminated or locked remotely as required by Administrators in specific situations.	3.1.11
AC.3.012	Access Control (AC)	Protect wireless access using authentication and encryption.	**Yes Supports Compliance**	All PreVeil users are authenticated cryptographically prior to access services. All information is end-to-end encrypted, whether transmitted over wireline or wireless. PreVeil's unique encryption model allows all the benefits of end-to-end encryption for phones and tablets as well as laptops and desktops.	3.1.17
AC.3.020	Access Control (AC)	Control connection of mobile devices.	**Yes Supports Compliance**	Use of mobile devices can be restricted by Administrators on a user by user basis. Device adds can be managed. Access to PreVeil on any device can be locked by Administrators.	3.1.18
AC.3.014	Access Control (AC)	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	**Yes Supports Compliance**	PreVeil end-to-end encryption protects the confidentiality of all remote access sessions.	3.1.13
AC.3.021	Access Control (AC)	Authorize remote execution of privileged commands and remote access to security-relevant information.	**Yes Supports Compliance**	PreVeil's security model employs cryptographic controls for Approval Group Authorizations for privileged commands including Data Export, Deleting Users and Assigning Admins.	3.1.15
AC.3.022	Access Control (AC)	Encrypt CUI on mobile devices and mobile computing platforms.	**Yes Supports Compliance**	During standard operation, PreVeil does not store data on mobile devices. it is accessed in view mode and is erased from the device when the document or application is closed. Additionally, PreVeil provides for biometric protections to restrict access to the PreVeil mobile application.	3.1.19

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
AM.3.036	Asset Management (AM)	Define procedures for the handling of CUI data.	**Does Not Apply Out of Scope**		CMMC
AU.2.041	Audit and Accountability (AU)	Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	**Yes Supports Compliance**	PreVeil end-to-end encryption enforces secure authentication/identification. System actions of Users and Admins are logged in a tamperproof manner and all logs are retained indefinitely. Identity and authentication for all Users and Admins are established cryptographically via user-specific and device-specific private keys.	3.3.2
AU.2.042	Audit and Accountability (AU)	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	**Yes Supports Compliance**	Admins can view user logs. Logs cannot be deleted or modified	3.3.1
AU.2.043	Audit and Accountability (AU)	Provide system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	**Yes Supports Compliance**	All Administrative and user logs of activities show server-side time stamp.	3.3.7
AU.2.044	Audit and Accountability (AU)	Review audit logs.	**Yes Supports Compliance**	Logs are generated on the server and are not editable by Administrators or users. Logs are cryptographically protected from modification or deletion.	CMMC
AU.3.045	Audit and Accountability (AU)	Review and update audited events.	**Yes Supports Compliance**	Admins can view user logs. Logs cannot be deleted or modified.	3.3.3
AU.3.046	Audit and Accountability (AU)	Alert in the event of an audit process failure.	**Does Not Apply Out of Scope**		3.3.4
AU.3.048	Audit and Accountability (AU)	Collect audit information (e.g. logs) into one or more central repositories.	**Yes Supports Compliance**	User and Admin activity is logged and cryptographically protected against tampering. Logs can be exported to a central repository.	CMMC
AU.3.049	Audit and Accountability (AU)	Protect audit information and audit tools from unauthorized access, modification, and deletion.	**Yes Supports Compliance**	Logs are generated on the server and are not editable by Administrators or users. Logs are cryptographically protected from modification or deletion.	3.3.8
AU.3.050	Audit and Accountability (AU)	Limit management of audit logging functionality to a subset of privileged users.	**Yes Supports Compliance**	PreVeil Admin logs (organization-wide) only accessible to admins. Administrative Approval Group feature eliminates single point of failure on invasive administrative actions. User logs only available to that specific user. Logs are tamperproof and cannot be modified or deleted.	3.3.9

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
AU.3.051	Audit and Accountability (AU)	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	**Partially Complies Additional Controls/Processes Necessary**	Note that PreVeil is implementing a feature to permit export of system logs (via an Approval Group) for further analysis. A 3rd party tool is used for the analysis.	3.3.5
AU.3.052	Audit and Accountability (AU)	Provide audit reduction and report generation to support on-demand analysis and reporting.	**Yes Supports Compliance**	Administrative logs capture all system activity and can be filtered by multiple parameters to support on-demand analysis.	3.3.6
AT.2.056	Awareness and Training (AT)	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	**Does Not Apply Out of Scope**		3.2.1
AT.2.057	Awareness and Training (AT)	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	**Does Not Apply Out of Scope**		3.2.2
AT.3.058	Awareness and Training (AT)	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	**Does Not Apply Out of Scope**		3.2.3
CM.2.061	Configuration Management (CM)	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	**Does Not Apply Out of Scope**		3.4.1
CM.2.062	Configuration Management (CM)	Employ the principle of least functionality by configuring organizational system to provide only essential capabilities.	**Yes Supports Compliance**	Only authorized users on authorized devices can access the secure data in PreVeil. Permissions are enforced cryptographically. Only authorized Admins can perform Administrative functions. Only formal Approval Groups can authorize specific invasive system actions.	3.4.6

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
CM.2.063	Configuration Management (CM)	Control and monitor user-installed software.	**Yes Supports Compliance**	Administrators can run a report that shows all PreVeil users in the PreVeil Organization, all devices enabled and the version of the PreVeil software on the devices. Administrators can lock any devices or delete accounts remotely if dictated by policy.	3.4.9
CM.2.064	Configuration Management (CM)	Establish and enforce security configuration settings for information technology products employed in organizational information systems.	**Yes Supports Compliance**	PreVeil's Administrative Approval Groups support enforcement of policies associated with access to and management of the data in the PreVeil system. PreVeil logs all administrative actions in a tamperproof manner.	3.4.2
CM.2.065	Configuration Management (CM)	Track, review, approve/disapprove, and log changes to organizational systems.	**Yes Supports Compliance**	PreVeil's Administrative Approval Groups support enforcement of policies associated with access to and management of the data in the PreVeil system. PreVeil logs all administrative actions in a tamperproof manner.	3.4.3
CM.2.066	Configuration Management (CM)	Analyze the security impact of changes prior to implementation.	**Does Not Apply Out of Scope**		3.4.4
CM.3.067	Configuration Management (CM)	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the organizational system.	**Yes Supports Compliance**	PreVeil's Administrative Approval Groups support enforcement of policies associated with access to and management of the data in the PreVeil system. PreVeil logs all administrative actions in a tamperproof manner.	3.4.5
CM.3.068	Configuration Management (CM)	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	**Does Not Apply Out of Scope**		3.4.7
CM.3.069	Configuration Management (CM)	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	**Does Not Apply Out of Scope**		3.4.8
IA.1.076	Identification and Authentication (IDA)	Identify information system users, processes acting on behalf of users, or devices.	**Yes Supports Compliance**	Cryptographically enforced user and Device management via Admin Console. Identity and authentication is established cryptographically via user private keys and device-specific private keys.	3.5.1
IA.1.077	Identification and Authentication (IDA)	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	**Yes Supports Compliance**	PreVeil end-to-end encryption validates that only authorized users on authorized devices can access the secure data in PreVeil. Identity and authentication is established cryptographically via user private keys and device-specific private keys.	3.5.2

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
IA.2.078	Identification and Authentication (IDA)	Enforce a minimum password complexity and change of characters when new passwords are created.	**Alternative Approach Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication is established cryptographically via user private keys and device-specific private keys. PreVeil eliminates the need for any additional passwords or encryption certificate management.	3.5.7
IA.2.079	Identification and Authentication (IDA)	Prohibit password reuse for a specified number of generations.	**Alternative Approach Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication is established cryptographically via user private keys and device-specific private keys. PreVeil eliminates the need for any additional passwords or encryption certificate management.	3.5.8
IA.2.080	Identification and Authentication (IDA)	Allow temporary password use for system logons with an immediate change to a permanent password.	**Alternative Approach Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication is established cryptographically via user private keys and device-specific private keys. PreVeil eliminates the need for any additional passwords or encryption certificate management.	3.5.9
IA.2.081	Identification and Authentication (IDA)	Store and transmit only cryptographically-protected passwords.	**Alternative Approach Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication is established cryptographically via user private keys and device-specific private keys. PreVeil eliminates the need for any additional passwords or encryption certificate management.	3.5.10
IA.2.082	Identification and Authentication (IDA)	Obscure feedback of authentication information.	**Alternative Approach Supports Compliance**	PreVeil doesn't rely upon passwords for identify verification. Identity and authentication is established cryptographically via user private keys and device-specific private keys.	3.5.11
IA.3.083	Identification and Authentication (IDA)	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	**Alternative Approach Supports Compliance**	You must have an authorized device to access PreVeil. In addition to the device passwords required to log into an laptop or device, PreVeil requires a second factor (your cryptographic user and device private keys) to authenticate to the PreVeil service. Identity and authentication is established cryptographically via user private keys and device-specific private keys. Additionally, on mobile devices, PreVeil supports biometric authentication for access to encrypted content.	3.5.3

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
IA.3.084	Identification and Authentication (IDA)	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	**Yes Supports Compliance**	PreVeil's leverages cryptographic authentication via private user and device keys. Please see the PreVeil encryption architectural whitepaper for additional detail.	3.5.4
IA.3.085	Identification and Authentication (IDA)	Prevent reuse of identifiers for a defined period.	**Yes Supports Compliance**	Identity and authentication is not confirmed with passwords. Instead, PreVeil uses established cryptographically via user private keys and device-specific private keys. PreVeil device keys rotate every 24 hours and are not re-used.	3.5.5
IA.3.086	Identification and Authentication (IDA)	Disable identifiers after a defined period of inactivity.	**Partially Complies Additional Controls/Processes Necessary**	This is a future capability for PreVeil but can be addressed in the near term via existing device timeout functionality.	3.5.6
IR.2.092	Incident Response (IR)	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil can be an important part of an Incident Response plan as it provides an out-of-band, secure and reliable communications and information storage tool.	3.6.1
IR.2.093	Incident Response (IR)	Detect and report events	**Does Not Apply Out of Scope**		CIS Controls v7.1 19.4
IR.2.094	Incident Response (IR)	Analyze and triage events to support event resolution and incident declaration	**Does Not Apply Out of Scope**		CERT RMM v1.2 IMC:SG2.SP4
IR.2.096	Incident Response (IR)	Develop and implement responses to declared incidents according to pre-define procedures	**Does Not Apply Out of Scope**		CIS Controls v7.1 19.1
IR.2.097	Incident Response (IR)	Perform root cause analysis on incidents to determin underlying causes.	**Does Not Apply Out of Scope**		CERT RMM v1.2 IMC:SG2.SP1
IR.3.098	Incident Response (IR)	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	**Does Not Apply Out of Scope**		3.6.2
IR.3.099	Incident Response (IR)	Test the organizational incident response capability.	**Does Not Apply Out of Scope**		3.6.3
MA.2.111	Maintenance (MA)	Perform maintenance on organizational systems.	**Yes Supports Compliance**	PreVeil handles maintenance and performs regular system updates, patching, and enhancements to its software and the infrastructure it maintains. If a customer elects to host the storage on-premise, the customer is responsible for infrastructure maintenance.	3.7.1

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
MA.2.112	Maintenance (MA)	Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	**Yes Supports Compliance**	PreVeil handles maintenance and performs regular system updates, patching, and enhancements to its software and the infrastructure it maintains. PreVeil is SOC-2 certified and uses many tools, controls and processes to properly conduct this maintenance. If customer elects to host the storage on-prem, customer is responsible for system maintenance.	3.7.2
MA.2.113	Maintenance (MA)	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	**Does Not Apply Out of Scope**		3.7.5
MA.2.114	Maintenance (MA)	Supervise the maintenance activities of personnel without required access authorization.	**Does Not Apply Out of Scope**		3.7.6
MA.3.115	Maintenance (MA)	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption.	3.7.3
MA.3.116	Maintenance (MA)	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	**Does Not Apply Out of Scope**		3.7.4
MP.1.118	Media Protection (MP)	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption.	3.8.3

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
MP.2.119	Media Protection (MP)	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.8.1
MP.2.120	Media Protection (MP)	Limit access to CUI on system media to authorized users.	**Yes Supports Compliance**	PreVeil end-to-end encryption enforces authentication/identification. All access and actions are logged. AWS meets control requirements for limiting access to system infrastructure.	3.8.2
MP.2.121	Media Protection (MP)	Control the use of removable media on system components.	**Does Not Apply Out of Scope**		3.8.7
MP.3.122	Media Protection (MP)	Mark media with necessary CUI markings and distribution limitations.	**Does Not Apply Out of Scope**		3.8.4
MP.3.123	Media Protection (MP)	Prohibit the use of portable storage devices when such devices have no identifiable owner.	**Does Not Apply Out of Scope**		3.8.8
MP.3.124	Media Protection (MP)	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption.	3.8.5
MP.3.125	Media Protection (MP)	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	**Yes Supports Compliance**	All PreVeil data is protected with end-to-end encryption at all times between user devices.	3.8.6

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
PS.2.127	Personnel Security (PS)	Screen individuals prior to authorizing access to organizational systems containing CUI.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.9.1
PS.2.128	Personnel Security (PS)	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	**Yes Supports Compliance**	Preveil Administrative controls provide for account deletion and device locking associated with personnel actions such as terminations and transfers.	3.9.2
PE.1.131	Physical Protection (PP)	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.10.1
PE.1.132	Physical Protection (PP)	Escort visitors and monitor visitor activity.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.10.3
PE.1.133	Physical Protection (PP)	Maintain audit logs of physical access.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.10.4

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
PE.1.134	Physical Protection (PP)	Control and manage physical access devices.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.10.5
PE.2.135	Physical Protection (PP)	Protect and monitor the physical facility and support infrastructure for organizational systems.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS meets the required FedRAMP/NIST mandates and provides very effective protection and monitoring of facilities for security. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. AWS provides effective protection and monitoring of facilities for security.	3.10.2
PE.3.136	Physical Protection (PP)	Enforce safeguarding measures for CUI at alternate work sites .	**Yes Supports Compliance**	PreVeil restricts access to sensitive data to the devices of authorized users. Administrators can limit users from adding other devices to their account. However, Administrators can enable remote access of encrypted communication by authorized users on additional devices on as needed basis.	3.10.6
RE.2.137	Recovery (RE)	Regularly perform and test data back-ups.	**Yes Supports Compliance**	PreVeil employs Amazon AWS US East-West systems for FedRAMP Moderate impact level and AWS GovCloud (US) for FedRAMP High impact level encrypted data storage. AWS provides complete and comprehensive data back-ups that are stored off-site. All PreVeil back-ups are fully encrypted end-to-end.	CIS Controls v7.1 10.1, 10.3
RE.2.138	Recovery (RE)	Protect the confidentiality of backup CUI at storage locations.	**Yes Supports Compliance**	All primary storage and back-ups consist of end-to-end encrypted content which can only be decrypted and accessed by authorized users in the organization. At no time are the decryption keys stored centrally at a backup location.	3.8.9
RE.3.139	Recovery (RE)	Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.	**Partially Complies Additional Controls/Processes Necessary**	All primary storage and back-ups consist of end-to-end encrypted content which can only be decrypted and accessed by authorized users in the organization. At no time are the decryption keys stored centrally at a backup location. Company however needs to provide the back-up policies.	CIS Controls v7.1 10.1, 10.2, and 10.5

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
RM.2.141	Risk Assessment (RM)	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	**Does Not Apply Out of Scope**		3.11.1
RM.2.142	Risk Assessment (RM)	Scan for vulnerabilities in theorganizational system and applications periodically and when new vulnerabilities affecting the system and applicationsare identified.	**Does Not Apply Out of Scope**		3.11.2
RM.2.143	Risk Assessment (RM)	Remediate vulnerabilities in accordance with risk assessments.	**Does Not Apply Out of Scope**		3.11.3
RM.3.144	Risk Management (RM)	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	**Does Not Apply Out of Scope**		NIST CSF v1.1 ID.RA-5 & CERT RMM v1.2 RISK:SG3 and SG4.SP3
RM.3.146	Risk Management (RM)	Develop and implement risk mitigation plans.	**Does Not Apply Out of Scope**		NIST CSF v1.1 ID.RA-6 ,ID.RM-1
RM.3.147	Risk Management (RM)	Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	**Does Not Apply Out of Scope**		CMMC
CA.2.157	Security Assessment (CA)	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil is SOC-2 certified and periodically assesses system security controls.	3.12.4
CA.2.158	Security Assessment (CA)	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil is SOC-2 certified and periodically assesses system security controls.	3.12.1

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
CA.2.159	Security Assessment (CA)	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil is SOC-2 certified and periodically assesses system security controls.	3.12.2
CA.3.161	Security Assessment (CA)	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil is SOC-2 certified and periodically assesses system security controls.	3.12.3
CA.3.162	Security Assessment (CA)	Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.	**Does Not Apply Out of Scope**		CMMC
SA.3.169	Situational Awareness (SA)	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	**Does Not Apply Out of Scope**		CMMC
SC.1.175	System and Communications Protection (SCP)	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	**Yes Supports Compliance**	PreVeil can facilitate the cross-organization boundary - everything is end-to-end encrypted. The Trusted Community feature permits an additional level of control and protection by limited communication and sharing to a white-listed group of PreVeil users. Monitoring would take place at the network level using existing policies/tools	3.13.1
SC.1.176	System and Communications Protection (SCP)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	**Does Not Apply Out of Scope**		3.13.5
SC.2.178	System and Communications Protection (SCP)	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	**Does Not Apply Out of Scope**		3.13.12
SC.2.179	System and Communications Protection (SCP)	Use encrypted sessions for the management of network devices	**Does Not Apply Out of Scope**		CMMC

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
SC.3.177	System and Communications Protection (SCP)	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	**Yes Supports Compliance***	*PreVeil's service uses approved FIPS 140-2 compliant cryptographic algorithms. PreVeil's cryptographic module is currently undergoing FIPS 140-2 validation in the NIST CMVP labs. For additional information regarding PreVeil's cryptographic algorithms, please see the detailed encryption architecture white paper.	3.13.11
SC.3.180	System and Communications Protection (SCP)	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	**Yes Supports Compliance**	PreVeil employs architectural designs, software development techniques, and systems engineering principles that are SOC-2 certified and promote effective information security. PreVeil has prepared a detailed architecture document that describes the structure of the platform and how it maximizes security.	3.13.2
SC.3.181	System and Communications Protection (SCP)	Separate user functionality from system management functionality.	**Yes Supports Compliance**	PreVeil incorporates strict cryptographic controls and an approval group process for setting up Admin accounts. The Admin accounts are distinct from user accounts and Admin capabilities cannot be accessed from User accounts.	3.13.3
SC.3.182	System and Communications Protection (SCP)	Prevent unauthorized and unintended information transfer via shared system resources.	**Yes Supports Compliance**	Only authorized users on authorized devices can access the secure data in PreVeil. Permissions are enforced cryptographically. PreVeil encrypted data is stored in a parallel secure network separate from standard unencrypted organization data.	3.13.4
SC.3.183	System and Communications Protection (SCP)	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	**Yes Supports Compliance**	With the Trusted Community feature enabled, only PreVeil system members in the organization and any white-listed 3rd parties can access or share information within that walled garden. All other communication attempts either into or out of that walled garden are not permitted.	3.13.6
SC.3.184	System and Communications Protection (SCP)	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e. split tunneling)	**Yes Supports Compliance**	With PreVeil, identity and authentication is established cryptographically via user private keys and device-specific private keys. Each system user is intrinsically related to specific devices and each device connection is always direct to the secure PreVeil cloud application and encrypted data storage network.	3.13.7

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
SC.3.185	System and Communications Protection (SCP)	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	**Yes Supports Compliance**	With PreVeil, all files and communications are encrypted prior to be transmitted, and remain end-to-end encrypted until they reach the authorized recipients' devices, at which point the information is decrypted. End to end encryption is a more powerful security mechanism than encryption in transit and encryption at rest which allow for central points of attack.	3.13.8
SC.3.186	System and Communications Protection (SCP)	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	**Partially Complies Additional Controls/Processes Necessary**	PreVeil supports device and network level controls regarding termination of network connections in these situations.	3.13.9
SC.3.187	System and Communications Protection (SCP)	Establish and manage cryptographic keys for cryptography employed in organizational systems.	**Yes Supports Compliance**	Encryption key management is handled automatically behind the scenes by PreVeil. Please see the PreVeil encryption architecture white paper for detailed information regarding PreVeil's key management architecture.	3.13.10
SC.3.188	System and Communications Protection (SCP)	Control and monitor the use of mobile code.	**Does Not Apply Out of Scope**		3.13.13
SC.3.189	System and Communications Protection (SCP)	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	**Does Not Apply Out of Scope**		3.13.14
SC.3.190	System and Communications Protection (SCP)	Protect the authenticity of communications sessions.	**Yes Supports Compliance**	PreVeil leverages private user and device keys to ensure cryptographic identity and authentication of users accessing the PreVeil service. All messages, file changes, etc are cryptographically signed using the user's private key. For additional information, please see PreVeil's encryption architecture white paper.	3.13.15
SC.3.191	System and Communications Protection (SCP)	Protect the confidentiality of CUI at rest.	**Yes Supports Compliance**	All files, communications, and data in the PreVeil system are protected with end-to-end encryption. This means that CUI at rest is always encrypted at rest, in transit, and while is use on the server. The keys to decrypt it are never stored centrally. For additional information, please see PreVeil's encryption architecture white paper.	3.13.16
SC.3.192	System and Communications Protection (SCP)	Implement Domain Name System (DNS) filtering services.	**Yes Supports Compliance**	PreVeil's Trusted communities feature allows only trusted domains to communicate with one another. As a result, all malicious or unapproved domains are blocked from communication.	CMMC

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
SC.3.193	System and Communications Protection (SCP)	Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g. forums, LinkedIn, Facebook, Twitter).	**Does Not Apply Out of Scope**		CMMC
SI.1.210	System and Information Integrity	Identify, report, and correct information and information system flaws in a timely manner.	**Does Not Apply Out of Scope**		3.14.1
SI.1.211	System and Information Integrity	Provide protection from malicious code at appropriate locations within organizational information systems.	**Does Not Apply Out of Scope**		3.14.2
SI.1.212	System and Information Integrity	Update malicious code protection mechanisms when new releases are available.	**Does Not Apply Out of Scope**		3.14.4
SI.1.213	System and Information Integrity	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	**Does Not Apply Out of Scope**		3.14.5
SI.2.214	System and Information Integrity	Monitor information system security alerts and advisories and take action in response.	**Does Not Apply Out of Scope**		3.14.3
SI.2.216	System and Information Integrity	Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	**Does Not Apply Out of Scope**		3.14.6
SI.2.217	System and Information Integrity	Identify unauthorized use of organizational systems.	**Yes Supports Compliance**	All logins and use of the PreVeil service are digitally signed and logged cryptographically. In the event an attacker compromises a user's account and is able to gain unauthorized use of the system, this activity would be logged and enable administrators to identify, respond to, and analyze the incident.	3.14.7
SI.3.218	System and Information Integrity (SI)	Employ spam protection mechanisms at information system access entry and exit points.	**Yes Supports Compliance**	PreVeil email can be configured with Trusted Communities of whitelisted email addresses and domains to effectively block spam.	CMMC
SI.3.219	System and Information Integrity (SI)	Implement email forgery protections.	**Yes Supports Compliance**	PreVeil identifies all senders and recipients through the use of asymmetric cryptography. All emails and files are protected by end-to-end encryption at all times.	CMMC

This appendix maps how PreVeil supports CMMC Level 3 compliance. Please note that some practices are dependent on enterprise policies aligned with the PreVeil information system functionality. This document must not be included as-is into a System Security Plan. You are responsible for determining which practices are applicable to you, and for developing and maintaining your own System Security Plan. PreVeil has no responsibility or liability if you choose to include any or all of the practices set forth in this document in your System Security Plan.

Appendix A: PreVeil Email and Drive as a secured enterprise information system for managing U.S. Government CUI

CMMC Practice	CMMC Domain	CMMC Practice Description	CMMC Practice Compliance Support	Explanation of Compliance with PreVeil	NIST 800-171 or Source
SI.3.220	System and Informational Integrity (SII)	Utilize sandboxing to detect or block potentially malicious email.	**Partially Complies Additional Controls/Processes Necessary**	While PreVeil email does not use sandboxing, PreVeil email can be configured with Trusted Communities of whitelisted email addresses and domains to block potentially malicious mail.	CM• CIS Controls v7.1 7.10 MC

Appendix B:
PreVeil vs. Alternatives

Appendix B: PreVeil vs. Alternatives

The Department of Defense has specific requirements when organizations work with CUI. Most commercial cloud services don't meet these requirements when email or files containing CUI are stored or processed in the cloud. Microsoft Office 365's email and SharePoint services, for example, are not DoD compliant for CUI. Microsoft offers a special service, called Microsoft GCC High for CUI. Similarly, Box's cloud file storage is not compliant for CUI; Box also requires a special service to manage CUI, called Box for Government.

PreVeil compares favorably to both Microsoft GCC High and Box for Government. It is significantly less expensive than the alternatives, and it provides email and file storage and sharing. It is also much more cost effective to deploy for email than Microsoft GCC High, as PreVeil may be used by only those in the organization dealing with CUI, whereas Microsoft GCC High much be purchased for the entire organization. Further, the Microsoft GCC High Exchange server must replace the existing email server, which requires special planning and configuration, whereas PreVeil augments the existing email environment and has no effect on the regular mail server.

PreVeil provides far better security than either Microsoft GCC High or Box for Government:

- PreVeil uses end-to-end encryption so that only senders and recipients of email and files can see the data; the PreVeil server operates on encrypted data and can never access the decryption keys. Conversely, both Microsoft GCC High and Box for Government offer optional encryption via a centralized key server, whereby client information is encrypted/decrypted at the server using keys stored on another server. This scheme is subject to central points of attack. All an attacker needs to do is penetrate one of the servers to mount a successful attack. If the key server is penetrated, then all keys on the system—and hence all information for the organization—is compromised. If the data server is penetrated, the attacker will have access to all plaintext data as it enters and leaves the server. PreVeil's end-to-end encryption eliminates the central points of attack inherent in key servers.

- PreVeil authenticates users via secret keys automatically created and stored on users' devices. The other systems use passwords, which are vulnerable to phishing and password guessing attacks.

- PreVeil's Approval Groups require administrators to receive authorization from a predetermined list of approvers before an invasive activity (such as exporting corporate data) can be performed. This process makes it very difficult to compromise an administrator.

- PreVeil's Trusted Communities allow an organization to whitelist trusted external entities. No one else is allowed to send or receive encrypted email or files to the organization, which is very effective for managing CUI.

Table 1: PreVeil vs. Alternatives

	PreVeil	Microsoft GCC High	Box For Government
Product	Email & Files	Email & Files	Files Only
Security			
Encryption	End-To-End Encryption	Optional key server (central point of attack)	Optional key server (central point of attack)
Authentication	Key-Based Authentication	Passwords	Passwords
Admin Vulnerability	Admin Approval Groups	Admin vulnerability	Admin vulnerability
Whitelisting	Trusted Communities	None—open to untrusted phishing/spoofing	Limited to domain-based whitelisting
Email Deployment	No impact to existing email server Only users with CUI need deploy	Rip and replace email server Typically, must be deployed to 100% of the organization	N/A
Drive Deployment	No impact to existing file servers Only users with CUI need to deploy	Rip and replace file server Typically, must be deployed to 100% of the organization	Requires centralized key server that must be provisioned, managed and protected
Cost	$30/user/month	$$$$	$$$$

About PreVeil

PreVeil makes encryption usable for everyday business. PreVeil's encrypted email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. PreVeil Drive works like DropBox for file sharing, but with far better security. All messages and documents are encrypted end-to-end, which means that no one other than intended recipients can read or scan them—not even PreVeil. PreVeil is designed for both small teams and large enterprises. Visit www.preveil.com to learn more.

Additional copies of this paper can be downloaded at **preveil.com/cmmc-whitepaper**