PREVEIL

Complying with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC 2.0)

Table of Contents

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 cybersecurity risks our nation faces, and in 2019 introduced the Cybersecurity Maturity Model Certification (CMMC) framework to defend the vast attack surface of the Defense Industrial Base (DIB).

CMMC is designed to unify standards for the implementation of cybersecurity practices throughout the DIB. One of DoD's top goals for CMMC is to better protect Controlled Unclassified Information (CUI), a prime target for cybercriminals and our nation's adversaries.

The CMMC program in its original form was widely criticized for its complexity and the anticipated costs of achieving certification. In response, the DoD undertook an extensive review of the program, and in late 2021 introduced CMMC 2.0, a streamlined version of the original model. While the CMMC framework has indeed been simplified, the DoD is not taking pressure off organizations to improve their cybersecurity levels.

CMMC 2.0 lowers the number of CMMC levels from five to three. The new CMMC 2.0 levels are: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert). CMMC 2.0 also will permit some defense contractors to self-attest their cybersecurity compliance, as opposed to all having to undergo third-party reviews as was mandated by CMMC 1.0. Further, unlike the original framework, CMMC 2.0 will allow time-limited use of Plans of Actions and Milestones (POAMs) that can be submitted in lieu of meeting certain non-critical security controls. Waivers of certification, too, will be permitted in very limited circumstances. CMMC 2.0 also differs from CMMC 1.0 in that cybersecurity maturity processes, while still required, will not be reviewed by auditors.

Importantly, DoD also has dropped the 20 security controls it had added to the CMMC 1.0 model. This means that the security controls for the new CMMC Level 2 will be in complete alignment with the 110 security controls of NIST SP 800-171. The new Level 2 certification will indicate that an organization is able to securely store and share Controlled Unclassified Information (CUI)—a matter of high priority for the DoD and the focus of this paper.

Note that any organization that handles CUI also is subject to DFARS 252.204-7012. That clause invokes not just its own (c)-(g) requirements for cyber incident reporting and the NIST SP 800-171 security controls, but also the FedRAMP Baseline Moderate or Equivalent standard for organizations that use cloud services. Additionally, NIST SP 800-171 invokes FIPS 140-2, which specifies cryptographic modules to be used for end-to-end encryption. In short, while the new Level 2 security controls will mirror NIST SP 800-171's security controls, organizations will need to meet cybersecurity requirements beyond NIST SP 800-171 to achieve the new CMMC Level 2.

CMMC 2.0 will go through the federal rulemaking process before becoming law, a process that DoD anticipates will take anywhere from nine to 24 months. In the meantime, however, no organization should wait to improve its cybersecurity levels. The CMMC initiative is one part of a larger effort of renewed scrutiny and enforcement of cybersecurity regulations by the DoD, the Department of Justice (DoJ), and the Executive Branch. All are driven by the imperative to protect our nation's CUI.

The Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)—the DoD's ultimate authority on compliance—has announced plans to increase the size of its audit staff in response to the pressing need to improve security in the Defense Industrial Base. For its part, the Department of Justice has launched a new Cyber-Fraud Initiative to hold contractors accountable for their cybersecurity and is encouraging whistleblowers to come forward with claims.

Perhaps the most compelling reason for contractors to move now to improve their cybersecurity is that NIST SP 800-171 is currently the law of the land. That's been true since 2017. Notably, while DoD has changed its CMMC framework, it also has stepped up enforcement of NIST SP 800-171. As of late 2020, contactors are required to report their NIST SP 800-171 self-assessment scores to DoD's SPRS Supplier Performance Risk System (SPRS) and, when CMMC 2.0 is implemented, SPRS scores will need to be signed off by a company executive who will be held accountable for the validity of the score.

Clearly, compliance with NIST SP 800-171 now is the path to Level 2 certification later, when CMMC 2.0 becomes law. Your organization will need to achieve excellent self-assessment scores, because even though POAMs will be allowed under CMMC 2.0, they won't be allowed for many of the highest weighted NIST SP 800-171 controls, which are also the hardest to achieve. And unlike in the past, POAMs will be tightly time-limited under the CMMC 2.0 model.

The key to achieving the new CMMC Level 2 certification is to implement technology solutions in conjunction with appropriate policies and procedures to ensure the security of CUI. But most widely-deployed commercial systems used to store and share CUI—such as Microsoft 365 Commercial or Gmail—do not comply with all CMMC Level 2 requirements, a point that Microsoft readily acknowledges. Organizations using such solutions will need to adopt new platforms to improve their cybersecurity, achieve the new CMMC Level 2, and win DoD contracts. This brief is written to help your organization meet those challenges.

To increase your understanding and help you start to move forward, the paper offers brief explanations of fundamental cybersecurity principles and how they connect with CMMC, beginning with Zero Trust and end-to-end encryption. Building upon that base, the paper includes a practical guide outlining what your company needs to do to achieve the new CMMC Level 2.

The paper's final section outlines key features of PreVeil, a state-of-the-art encrypted file sharing and email platform that offers uncompromised security for storing and sharing CUI. PreVeil is easy to deploy and use, making military-grade cybersecurity widely accessible and affordable.

PreVeil understands the challenges that small to mid-size contractors and organizations with both commercial and defense business, as well as universities, must overcome to achieve CMMC Level 2. Its solutions will simplify your compliance journey and make it more affordable.

The paper briefly describes an actual case study of how a small defense contractor prepared for a rigorous DIBCAC audit by deploying PreVeil as an overlay to its existing O365 Commercial system for all its users handling CUI. Deployment was an easy process that laid the foundation for compliance with NIST SP 800-171's most important controls, that is, the ones that protect CUI. DIBCAC auditors certified that the contractor met 109 of the 110 NIST SP 800-171 controls. Remarkably, this near-perfect score of 109 placed the defense contractor alongside the nation's top prime contractors for cybersecurity. Without PreVeil's advanced security and compliance features to protect CUI, the contractor's NIST SP 800-171 score would have been significantly lower. With PreVeil, if CMMC 2.0 had been in effect, the contractor would have been deemed to have met the new Level 2 requirements (with a POAM for the just the one remaining control).

The brief concludes with detailed and helpful appendices. Appendix A, for example, presents a comprehensive table that lists each of NIST SP 800-171's 110 controls, as required for the new CMMC Level 2, and indicates which requirements PreVeil helps to meet and how it does so.

Finally, note that earlier versions of this paper have been downloaded more than 1,500 times by defense contractors. It is our hope that this completely updated version—reflecting the latest information available as of its release in December 2021—serves to help your organization, too, as you work to better protect your data resources and CUI, and win defense contracts.

CMMC 2.0 Overview

From the start, CMMC was designed to strengthen and unify standards for the implementation of cybersecurity controls throughout the DIB. DoD also expects that the mandate to meet CMMC requirements will help quicken the pace at which defense contractors improve their cybersecurity.

CMMC focuses on protection of both 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.

From CMMC 1.0 to CMMC 2.0

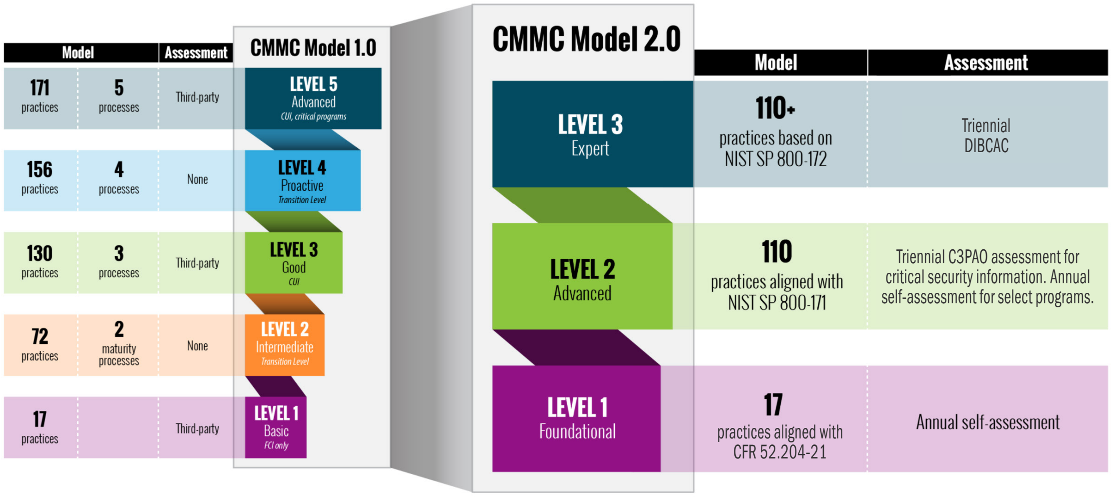
The DoD introduced its CMMC initiative in mid-2019 and released CMMC 1.0 in early 2020. At that point, DoD embarked on an ambitious plan to have every one of the hundreds of thousands of companies doing work for the DoD certified by outside assessors at their appropriate CMMC level—all within five years.

While the need for better cybersecurity throughout the DIB remained unquestioned, the impracticality of the planned rollout quickly became clear. When the Interim DFARS Rule 2019-D041, Clause 7021, which established CMMC 1.0, was released in September 2020 and became effective just two months later, DoD was inundated with hundreds of public comments. Many of those comments were from small to mid-size defense contractors (SMBs) expressing concerns about the complexity of the CMMC framework and the costs of compliance and third-party certification.

Congressional hearings and an eight-month long DoD internal review ensued, and in November 2021 DoD released its much-streamlined CMMC 2.0. The revised program reflects key DoD goals: first, to reduce costs, particularly for SMBs, and second, to clarify and align cybersecurity requirements with other federal requirements.

Figure 1 illustrates changes to the CMMC program announced in November 2021.

Figure 1: From CMMC 1.0 to CMMC 2.0



Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial DIBCAC
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial C3PAO assessment for critical security information. Annual self-assessment for select programs.
LEVEL 1 Foundational	17 practices aligned with CFR 52.204-21	Annual self-assessment

CMMC 2.0 has just three levels

CMMC 2.0 drops the number of CMMC levels from five to three by eliminating the old levels 2 and 4, which were originally developed as transition levels. The new CMMC 2.0 levels are based on the type of information DIB companies are working with:

- Level 1 (Foundational) is for companies working with FCI only; that is, information that requires protection but is not critical to national security. It is comparable to the old CMMC Level 1.
- Level 2 (Advanced) is for companies working with CUI. It is comparable to the old CMMC Level 3.
- Level 3 (Expert) is for companies working with CUI on DoD's highest priority programs. It is comparable to the old CMMC Level 5.

CMMC 2.0 Level 2 (Advanced) security controls will mirror NIST SP 800-171

CMMC 2.0 eliminates all practices that were unique to CMMC, and instead aligns with the security controls developed by the National Institute of Technology and Standards (NIST) to protect CUI. Accordingly, the 20 requirements in the old CMMC Level 3 that DoD had imposed were dropped, meaning that the new Level 2 (Advanced) security controls are in complete alignment with NIST SP 800-171. DoD is still determining the specific security controls that will be required for the Level 3 (Expert), but has indicated that those will be based on NIST SP 800-171's 110 controls plus a subset of NIST SP 800-172 controls.

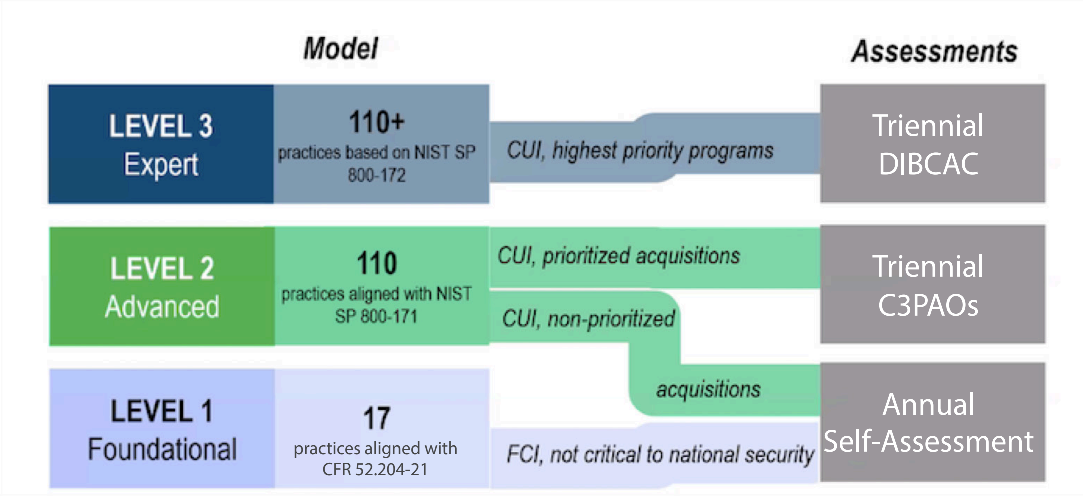
Going forward, DoD is committed to working with NIST to add new requirements as the need arises, rather than doing so on its own. One of the benefits of this approach is that the CMMC program will be easier for other federal agencies to adopt if it doesn't include DoD-specific requirements.

NIST SP 800-171 maturity process requirements will not be audited under CMMC 2.0. However, NIST SP 800-171's several appendices will still be in effect. That includes Appendix E, which provides mature processes and procedure descriptions for each control, and which Non-Federal Organizations (known as NFOs or, for these purposes, defense contractors) are routinely expected to satisfy. Auditors won't check specifically for those policies and procedures, but if a contractor doesn't have them in place, it will be difficult to implement their corresponding NIST SP 800-171 controls.

CMMC 2.0 will permit self-assessments for some DIB companies

Unlike CMMC 1.0, which required all DoD contractors to undergo third-party assessments for CMMC certification, CMMC 2.0 assessment requirements will be based on the type of information DIB companies are working with, as illustrated in Figure 2.

Figure 2: CMMC 2.0 model and assessments based on information being handled


Model
Assessments
LEVEL 3
Expert
110+
practices based on NIST SP 800-172
CUI, highest priority programs
Triennial
DIBCAC
LEVEL 2
Advanced
110
practices aligned with NIST SP 800-171
CUI, prioritized acquisitions
Triennial
C3PAOs
CUI, non-prioritized
acquisitions
LEVEL 1
Foundational
17
practices aligned with CFR 52.204-21
FCI, not critical to national security
Annual
Self-Assessment

At Level 1, defense contractors handling FCI will be required to perform annual self-assessments, as will a subset of Level 2 contractors that, while handling CUI, are working on projects that do not involve sensitive national security information (i.e., non-prioritized acquisitions). These contractors' self-assessments will need to be accompanied by an annual attestation from a senior company official that the company is meeting Level 2 cybersecurity requirements.

Level 2 defense contractors handling CUI that is critical to national security (i.e., prioritized acquisitions) will be required to undergo third-party assessments once every three years. Those assessments will be conducted only by accredited C3PAOs (CMMC Third Party Assessment Organizations). Once the new CMMC 2.0 Assessment Guide is released, the CMMC-AB (CMMC Accreditation Body) will resume training C3PAOs and CMMC Assessors, as well as CMMC consultants. Accredited C3PAOs will be listed on the CMMC-AB Marketplace. Contractors will be fully responsible for obtaining and coordinating the needed assessment and certification.

After completion of the CMMC assessment, the C3PAO will provide an assessment report to the DoD. Again, security controls for Level 2 certification align completely with NIST SP 800-171's security controls. Note that self-assessment of NIST SP 800-171 compliance has been required since 2017 for contractors subject to DFARS 252.204-7012, and as of November 2020, scores must be reported to the DoD's SPRS (Supplier Performance Risk System), as described in more detail on page 16 below.

As of December 2021, the DoD was still working on details of the bifurcation of Level 2 in terms of required assessments. DoD officials have made clear, though, that they do not plan to create a different class of CUI. Examples of contracts provided by DoD to illustrate the Level 2 path to self-assessment are designing military uniforms or boots, both of which involve CUI but not sensitive national security information. Examples of Level 2 work that would lead to triennial C3PAO assessments are developing parts for a weapons system, or for a command and control communications system.

All Level 3 contractors—who by definition are working on the most critical defense programs—will be required to undergo triennial assessments done by audit teams from the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), the DoD's ultimate authority on compliance.

CMMC 2.0 will allow POAMs in limited circumstances

The DoD will allow companies to be awarded defense contracts under CMMC 2.0 with a POAM in place for security controls they have not yet met at the time of the award. This is a significant change from CMMC 1.0, which did not allow POAMs and instead made CMMC certification the basis of go/no-go decisions for contract awards.

However, according to senior DoD officials, POAMs will not be permitted for a subset of the highest-weighted security requirements—which also are the hardest requirements to meet. The DoD's current self-assessment methodology for NIST SP 800-171 gives each of the 110 controls a weight of 1, 3 or 5 points. Although the DoD has not yet released information along these lines, many CMMC experts outside the DoD expect that the "highest-weighted security requirements" are the controls that are assigned 5 points. Note that 44 of the 110 controls currently are weighted at 5 points each.

Further, DoD is also planning to establish a minimum SPRS score that must be achieved when POAMs are used to support attainment of the new CMMC levels, and POAMs will be time-bound, with limits strictly enforced. DoD has not yet made a final decision regarding those time limits, but has indicated it is considering 180 days. While also unknown, many CMMC experts expect that the 180-day POAM clock will start upon award of a contract, either by DoD to a prime or by a contractor to a subcontractor.

CMMC 2.0 will allow waivers in limited circumstances

To increase flexibility of the CMMC program and to retain the ability to move rapidly when needed, the DoD will allow waivers under CMMC 2.0. Waivers were not permitted under CMMC 1.0. Waivers will be very limited and permitted only for select mission-critical contracts. DoD program officers will need to submit a justification package that includes a risk mitigation plan and a specific timeline by which CMMC requirements will be met. Waiver requests will require senior DoD leadership approval. Waivers will apply to the entire CMMC requirement, not to individual cybersecurity controls. Additional details regarding waivers will be determined during the rulemaking process, described below.

CMMC 2.0 rulemaking and timeline

The DoD intends to strengthen the basis of the CMMC program by removing ambiguities stemming from previous reliance on the Interim DFARS Rule to implement CMMC 1.0. For CMMC 2.0, the DoD will pursue rulemaking both in Part 32 of the Code of Federal Regulations (CFR) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR. Codifying CMMC 2.0 through this federal rulemaking process will provide the clarity needed to effectively measure and enforce cybersecurity compliance throughout the DIB.

DoD anticipates that the rulemaking process will take anywhere from nine to 24 months. While these rulemaking efforts are ongoing, DoD is suspending all CMMC pilot efforts and mandatory CMMC certification. Further, DoD will not approve inclusion of a CMMC requirement in any DoD solicitation until the rulemaking process is complete. In the meantime, to encourage contractors to continue to focus on improving their cybersecurity, the DoD is exploring whether to provide incentives for contractors to voluntarily attain their needed CMMC level prior to completion of the rulemaking process.

In any case, the DoD strongly encourages defense contractors to continue to enhance their cybersecurity posture while rulemaking is underway. In fact, DoD recently has stepped up enforcement of NIST SP 800-171, which has been in effect since 2017. The DoD's and the

Department of Justice's efforts underway now to enforce adherence to current federal cybersecurity standards are described in more detail below (see page 13 below.).

CMMC-AB's role in CMMC 2.0

Upon release of CMMC 2.0, the DoD signaled its intent to continue to work with the CMMC-AB as its training partner and assessor for CMMC 2.0 Level 2 certification.

The CMMC-AB's Certified CMMC Professional (CCP) training is ongoing. Once DoD releases the new CMMC 2.0 Assessment Guide, which essentially will "de-scope" the program, the CMMC-AB will revise its training accordingly. The CMMC-AB also plans to offer free "delta training" to anyone who has already gone through its training and certification, so that those individuals will be better positioned for the newly-revised exams to come.

Modern Cybersecurity Principles and CMMC 2.0

This section is offered as a brief primer on modern cybersecurity principles and how they connect to NIST SP 800-171's security controls. The aim is to increase your understanding of what DoD is expecting of your organization in terms of protecting CUI—the fundamental purpose of CMMC. From this knowledge base, you will be well positioned to undertake the steps outlined in the section that follows, which presents a practical guide to achieving the new CMMC Level 2.

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

In recent years, cybersecurity research at leading universities has led to critical innovations in applied cryptography. These new technologies are based on best practices advanced by the National Security Agency (NSA)—the federal agency responsible for the nation's cybersecurity—and other key fundamental security principles outlined below. The new technologies will enable your company to enhance its cybersecurity and help it achieve the CMMC level necessary to do work for the DoD.

Specific NIST SP 800-171 control families addressed by each cybersecurity principle are noted. Recall that security controls for the new CMMC 2.0 Level 2 will mirror NIST SP 800-171's security controls.

Zero Trust

The NSA's February 2021 memorandum, *Embracing a Zero Trust Security Model*, describes a Zero Trust model as one that "eliminates trust in any one element, node, or service" and "assumes that a breach is inevitable or likely has already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity." The NSA explains that the Zero Trust approach is in contrast to "Traditional perimeter-based network defenses with multiple layers of disjointed security technologies [which] have proven themselves to be unable to meet the cybersecurity needs due to the current threat environment."[1] The NSA memorandum urges the entirety of the DoD and the DIB to adopt the Zero Trust security model.[2]

The Zero Trust security model, according to the NSA, is designed to secure the entire breadth of computing services, data resources, and network locations across enterprises. It's a mindset that spans every one NIST SP 800-171's 14 control families.

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 steal data from the server, it will be only encrypted gibberish.

End-to-end encryption addresses the following NIST SP 800-171 control families: Access Control, Configuration Management, Media Protection, Systems & Communications Protection, and System & Informational Integrity.

Encrypted logs

All user and admin activities should be logged in order to constantly monitor for and trace possible malicious activities. Logs themselves also should be tamper-proof and protected with end-to-end encryption to maintain their integrity and to prevent attackers from gleaning sensitive information or covering their tracks by deleting log entries.

Encrypted logs address the following NIST 800-171 control family: Audit & Accountability.

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

Cloud-based services

Cloud-based services offer significant advantages over on-premises servers, such as lower costs, less risk, better scalability, fewer administrative and maintenance responsibilities, and faster routes to compliance with cybersecurity regulations. 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 such information is always encrypted on the cloud server. Further, the server can never access decryption keys. No

[1] See: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[2] Note that while at this point it is still possible to comply with CMMC 2.0 and NIST SP 800-171 using legacy security systems, a better path to compliance is achievable through modern Zero Trust systems. To learn more about how Zero Trust creates fundamentally better cybersecurity, see PreVeil's brief, *Zero Trust: A better way to enhance cybersecurity and achieve compliance*.

one but the intended recipients can access the data, not even the cloud service provider.

Cloud-based services can help address the following NIST SP 800-171 control families: Maintenance, Media Protection, and Physical Protection.

Key-based authentication

Passwords create a significant security risk because they are routinely 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 cryptographic keys that are stored only on the user's device. Unlike passwords, these keys cannot be guessed or stolen.

> ***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.***

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 the devices are lost or stolen, device management controls allow admins to quickly disable them.

Key-based authentication can help address the following NIST SP 800-171 control families: Identification & Authentication, System & Communications Protection, and Systems & Informational Integrity.

Administrative distributed trust and eliminating central points of attack

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 central 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 codes, 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 administrator. Distributed trust eliminates central points of attack.

> ***Much like the nuclear launch codes, 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 NIST SP 800-171 control families: 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 NIST SP 800-171 control families: Configuration Management, Systems & Communications Protection, and Systems & Informational Integrity.

What does my organization need to do?

Now is the time to take action to improve your organization's cybersecurity. One of the most emphatic points made by the DoD upon the release of CMMC 2.0 is that no organization should wait until the new framework becomes law. Indeed, NIST SP 800-171 is currently in effect, and has been since 2017.

Understand, too, that DIBCAC audits will continue while the rulemaking process for CMMC 2.0 runs its course. In fact, DIBCAC has announced plans to increase the size of its audit staff in response to the pressing need to improve security in the DIB. Just like the IRS can audit any taxpayer, the DIBCAC can select any defense contractor for a NIST SP 800-171 audit. If your organization is chosen for a DIBCAC audit, being able to show that you're implementing adequate data protections is critical. One of your best defenses will be if you can demonstrate that your organization is on a path toward achieving a good NIST SP 800-171 score (more on this below).

The Department of Justice (DoJ) also has raised the stakes for compliance with the launch of its Civil Cyber-Fraud Initiative, with the aim of holding contractors accountable for their cybersecurity. DoJ is utilizing the power of the False Claims Act to help enforce cybersecurity compliance and is encouraging whistleblowers to come forward. A new DoJ task force will focus on investigating reports of contractors choosing to withhold reports of breaches or that falsify claims of self-assessment scores. The consequences of withholding information or submitting false scores are severe. None of these activities is slowing down while CMMC 2.0 works its way through the rulemaking process.

Here are the first steps your organization needs to take now toward achieving CMMC Level 2 certification:

Familiarize Yourself with the CMMC 2.0 Framework

With this paper you're already off to an excellent start on familiarizing yourself with the CMMC 2.0 framework. Continue to stay abreast of developments by regularly checking the DoD's CMMC website, which has been completely overhauled with the introduction of CMMC 2.0, and the CMMC-AB website. We recommend that these two official sites serve as your primary sources for all things CMMC.

Determine the CMMC Level Your Organization Needs to Achieve

Your defense contract will specify which CMMC level your organization will need to achieve. As described above, the new CMMC levels are based on the type of information your organization works with. Organizations that handle just FCI will need to achieve Level 1 (Foundational). Any organization that handles CUI will need to achieve at least Level 2 (Advanced).

To help your organization's cybersecurity planning process, the following DoD guidance will help you determine which level you will need to achieve when CMMC 2.0 is implemented and, if that's Level 2, whether you should expect to undergo third-party assessments or conduct self-assessments:

If applicable, review your current DoD contracts to determine if your organization is already handling CUI and to gain insight as to whether DoD could consider the work you do to be critical to national security and, therefore, a "prioritized acquisition." If that's the case, then you most likely will be required to achieve CMMC Level 2 and undergo a C3PAO assessment once every three years. DoD examples of prioritized acquisitions include contracts for developing parts for a weapons system, or for a command and control communications system.

On the other hand, if your organization handles CUI but works on defense projects that do not involve sensitive national security information, then DoD is likely to consider your contract to be a "non-prioritized acquisition," in which case you will need to achieve CMMC Level 2 and conduct annual self-assessments of CMMC compliance. DoD examples of non-prioritized acquisitions include contracts for the design of military uniforms or boots.

Regardless of this distinction, DIBCAC is advising organizations to prepare for the new CMMC Level 2 as if they will need to undergo third-party assessments. The primary reason for this approach is simply that the mindset for a self-assessment should not be any different than if you were preparing for an external audit. In either scenario, the bar is set at the same level and the same cybersecurity regulations apply.

The DoD estimates that the approximately 220,000 organizations in the Defense Industrial Base will breakdown into the CMMC 2.0 levels as follows:

Level 1 (Foundational) ~ 140,000 organizations
Level 2 (Advanced) ~ 80,000 organizations*
Level 3 (Expert) ~ 500 organizations

***DoD also has estimated that half of the 80,000 organizations at Level 2 will be permitted to self-assess, while the remaining 40,000 at that level will need to undergo third-party assessments.**

See Figure 2 above for more information on the bifurcation of assessment requirements for the new CMMC Level 2.

The new CMMC Level 3 (Expert) is for defense contractors and university researchers that work with CUI on DoD's highest priority programs. Cybersecurity requirements for these companies have not yet been finalized by the DoD.

Scope your compliance boundary

Any defense contractor or university researcher hoping to achieve the new CMMC Level 2 will need to meet NIST SP 800-171's 110 security controls. The question is, how can an organization determine the scope of its compliance project, that is, figure out which of its users, systems, devices and processes are subject to NIST SP 800-171? We know that this standard focuses on the protection of CUI. Therefore, organizations that work with CUI need to determine who in their organization accesses CUI; which devices process CUI; which organizational processes are related to the protection of CUI; and, importantly, how these users, systems and devices can be segregated into an enclave separate from the non-CUI part of your organization. With regard to the latter, the good news is that the DoD's latest guidance on the subject, *CMMC Assessment Scope: Level 2, Version 2.0* released in December 2021, makes clear that CUI enclaves will be acceptable in the new scoping regime.

That said, if 100% of your organization's work is on DoD contracts and many of them involve CUI, then it makes sense to include your entire organization in scope for NIST SP 800-171 compliance. On the other hand, if only a portion of your organization handles CUI, then it makes sense to narrow the scope of the security requirements as much as is reasonable.

A self-assessment or a third-party assessor using the DoD's Assessment Methodology will require documentation and evidence that NIST SP 800-171's requirements are being met within the scope of the compliance boundary that you determine fits your organization's profile. It stands to reason that a narrower scope means a simpler, faster assessment process.

Gap Analysis: Conduct a NIST SP 800-171 Self-Assessment

Once you determine the CMMC 2.0 level you need to achieve and the scope of your compliance boundary, the next step is to examine the current state of your cybersecurity and identify gaps between your organization's capabilities and the requirements for the CMMC level you seek. You may need to work with an outside consultant to complete this gap analysis.

If your organization is aiming for the new CMMC Level 2, the obvious place to begin your gap analysis is with NIST SP 800-171, given that the new Level 2 security controls will mirror NIST SP 800-171's security controls. And while CMMC 2.0 won't be effective until the federal rulemaking process is complete, DoD has already stepped up enforcement of NIST SP 800-171. Specifically, while DFARS 252.204-7012 has required implementation of NIST SP 800-171 controls since late 2017, DoD has until recently permitted self-attestation of compliance. The Interim DFARS Rule changed that in late 2020, and now contractors are required to report the results of their NIST SP

800-171 self-assessments to the DoD. That new requirement remains in effect despite the changes being made to the CMMC framework.

The Interim DFARS Rule aimed at stepping up compliance with NIST SP 800-171—and still in effect—stipulates that:

- Contractors must create a System Security Plan (SSP) as a prerequisite for all further considerations for DoD work.
- DoD's NIST SP 800-171 Assessment Methodology must be followed and all contractors who handle CUI must perform at least a Basic level self-assessment. Scoring starts at a maximum of 110, based on the 110 NIST 800-171 controls. Points will be subtracted for each control not yet implemented.
- Self-assessment scores will range from -203 to +110, a spread of 313 points.
- Self-assessment scores must be filed in the DoD's SPRS system by the time of contract award, and your security program must be maintained for the duration of the contract.
- If their self-assessment score falls below 110, contractors are required to create a POAM and indicate to the DoD by what date the security gaps will be remediated and a score of 110 will be achieved. Recall, however, that while POAMs will be allowed under CMMC 2.0, their use will be limited on a number of levels, and so it is important to address security gaps with the appropriate technology or policies in a timely fashion.

The significance of the NIST SP 800-171 self-assessment and resulting SPRS score is twofold. First, it demonstrates your organization's cybersecurity posture and is an important determinant of your position vis-à-vis competitors when seeking to be part of a defense contract. The Interim DFARS Rule doesn't specify minimum self-assessment scores that must be achieved, unlike CMMC 2.0, which will require minimum scores when implemented. But the DoD will do risk-based assessments to help determine which companies it will award contracts to. If a company has a low self-assessment score, it stands to reason that the DoD will consider that company to be a higher security risk than an alternative supplier with a better score. Likewise, primes will consider self-assessment scores when evaluating possible subcontractors with which to work, and it is reasonable to expect that subcontractors with higher scores are more likely to win the work.[3]

Second and more important, there is no path to CMMC 2.0 Level 2 certification without compliance with NIST SP 800-171, and there is no indication that its foundational controls are changing. In this environment, your organization's best course of action is to focus on complying with NIST SP 800-171. Doing so now will put your organization on a smooth path to achieving the new Level 2 when that time comes.[4]

[3] To learn more about increasing your NIST 800-171 self-assessment score, see PreVeil's briefs, *DFARS Self-Assessment: How to Raise Your NIST 800-171 Score* and *Case Study: How a Defense Contractor Using PreVeil Achieved a Near-Perfect NIST 800-171 Score in DIBCAC Audit*.

[4] DoD plans to provide guidance with respect to Standard Acceptance Agreements between CMMC 2.0 Level 2 (Advanced) and the NIST SP 800-171 DoD Assessment Methodology for the high assessment or confidence level. See DoD's CMMC 2.0 FAQ sidebar here. DoD notes that any such equivalencies or acceptance standards, if established, will be implemented as part of the rulemaking process.

Finally, note too that in another effort to increase enforcement of federal cybersecurity regulations, CMMC 2.0 will require that SPRS scores be signed off by a company or university executive, who will be held accountable for the validity of the score. Currently, any employee can sign off on the NIST SP 800-171 self-assessment score; that most often falls to IT staff. This new CMMC 2.0 approach is akin to the responsibility corporate leaders in the financial realm had to take on when the Sarbanes-Oxley Act was adopted nearly 20 years ago in response to a string of highly visible financial scandals. Given how effective Sarbanes-Oxley has been in improving the accuracy of financial reporting, that model is now being followed by the DoD.

Identify Partners to Get the Help You Need

You needn't take on NIST SP 800-171 compliance and CMMC certification on your own. Many cybersecurity companies have devoted extensive time and resources to gain a deep understanding of the CMMC framework and have adapted their services to help organizations in the DIB—many of which lack the necessary internal security expertise to achieve CMMC Level 2. They can assist your organization by, for example, helping you conduct a self-assessment and gap analysis, and with completion of your required SSP.

Perhaps most important, outside partners can help your company create a smooth path to NIST SP 800-171 compliance and attainment of CMMC Level 2.

Assess Alternatives to Commercial Cloud Services

If your organization has migrated to the cloud, standard commercial cloud services such as Microsoft 365 Commercial are not CMMC compliant and so you will need to assess alternatives. To comply with the new CMMC Level 2 requirements and other federal regulations that your organization may need to meet, cloud service providers should meet DFARS 252.204-7012 (c)-(g), be certified as FedRAMP Baseline Moderate or Equivalent,[5] and use a FIPS 140-2[6] validated cryptographic module for encryption. Note that as part of the CMMC 2.0 rulemaking process, the DoD is aiming to develop Standard Acceptance Agreements between CMMC Level 2 and FedRAMP requirements for commercial cloud service offerings.[7] Standard Acceptance Agreements between two cybersecurity standards means that compliance with one of the standards can be considered equivalent to compliance with the other standard in the agreement.

Project and Plan for Costs

CMMC 2.0 costs are projected to be significantly lower relative to CMMC 1.0 as a result of plans to streamline requirements at all levels, increase oversight of the third-party assessment ecosystem,

[5] FedRAMP is the US General Services Administration's (GSA's) Federal Risk and Authorization Management Program, which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[6] FIPS 140-2 refers to NIST's Federal Information Processing Standard 140-2 publication, entitled *Security Requirements for Cryptographic Modules*. It specifies the security requirements for cryptographic modules, and provides four increasing, qualitative levels intended to cover a wide range of potential applications and environments.

[7] See DoD's CMMC 2.0 FAQ sidebar here. DoD notes that any such equivalencies or acceptance standards, if established, will be implemented as part of the rulemaking process.

and allow contractors at the new Level 1, as well as and some at Level 2, to perform self-assessments rather than undergo third-party assessments.

That said, the Interim DFARS Rule published in September 2020 had this to say about costs: "Contractors pursuing…[the old CMMC] Level 3 Certification should have already implemented the 110 existing NIST SP 800-171 security requirements. Therefore, the estimated engineering costs per small entity is associated with implementation of 23 new requirements (20 CMMC practices and 3 CMMC processes)."[8]

That is to say, the DoD is assuming that defense contractors that have been handling CUI already are in compliance with NIST SP 800-171, and therefore any additional costs for achieving CMMC Level 2 certification should be minimal. It's unknown whether DoD will continue to take this approach to costs under CMMC 2.0. As part of the rulemaking process, DoD will publish a comprehensive cost analysis associated with each CMMC 2.0 level.

PreVeil Product Overview

PreVeil's file sharing and email platform adheres to each of the fundamental cybersecurity principles outlined above, beginning with Zero Trust and the gold standard of end-to-end encryption. PreVeil's encrypted Drive and Email support compliance with virtually all the new CMMC Level 2 mandates related to the communication and storage of CUI. In contrast, most widely-deployed commercial systems used to store and share CUI do not comply with the Level 2 requirements. Organizations using those standard commercial solutions will need to adopt new platforms to improve their cybersecurity, achieve CMMC Level 2, and win DoD contracts.

This section describes PreVeil Drive and Email, and how PreVeil can help your organization achieve NIST SP 800-171 compliance and, when the time comes, CMMC Level 2 certification—a straightforward step given that the new Level 2 security controls will mirror NIST SP 800-171's security controls.

For more details, Appendix A, available at the end of this paper, presents a comprehensive table that lists each of NIST SP 800-171's 110 controls—as required for the new CMMC Level 2—and indicates which requirements PreVeil helps to meet and how it does so.

File sharing and storage

PreVeil Drive 🔗 enables end-to-end encrypted file sharing and storage and integrates seamlessly with Windows File Explorer and Mac Finder. Users can enable granular visibility and control with file sharing permissions such as edit, read only, and view only, and can access files stored on PreVeil Drive from any of their devices. With PreVeil's Trusted Communities feature, organizations can limit communications and file sharing to only those users who are listed as having trusted addresses and domains, and appropriate access permissions.

[8] See the Federal Register, *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)*, September 29, 2020, p. 61,514.

Importantly, 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.

Email

PreVeil Email lets you send and receive end-to-end encrypted emails using your existing email address. PreVeil users can securely share CUI within an organization, with outside partners, and with government agencies—including the DoD.

PreVeil integrates with mail clients such as Outlook, Gmail, and 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. Users keep their regular email address, which keeps it simple.

Compliance attributes

PreVeil supports compliance with virtually all the CMMC Level 2 requirements for storing and sharing CUI. These requirements include standards beyond NIST SP 800-171's security controls, which PreVeil also addresses. PreVeil's key compliance attributes include:

- Meets FedRAMP Baseline Moderate or Equivalent
- Encrypts and stores data on FedRAMP High AWS GovCloud
- Meets DFARS 252.204-7012 (c)-(g), which stipulates requirements for cyber incident reporting
- Meets ITAR 120.54 via end-to-end encryption wherein the cloud service provider has no access to keys, and the FIPS 140-2 validated cryptographic module is used[9]

TO HELP YOU LEARN MORE about the fast-changing landscape of compliance and its ramifications for defense companies, PreVeil has several resources to offer.

***Zero Trust: A Better Way to Enhance Cybersecurity and Achieve Compliance*, for example, was written to help defense companies better understand Zero Trust principles. The paper describes how a Zero Trust mindset and architecture creates fundamentally better cybersecurity and, likewise, helps contractors comply with DoD regulations and win defense contracts.**

See Appendix C for a complete list of PreVeil resources.

Most widely-deployed commercial systems used to store and share CUI do not comply with the new CMMC Level 2 requirements. That includes Microsoft 365 Commercial. Instead, Microsoft offers GCC High, a comprehensive solution for large organizations striving for CMMC compliance.

[9] See PreVeil blog, *Ensuring FIPS 140-2 Compliance: Caveat Emptor*, to learn more.

However, GCC High is a complex system to deploy and configure. It most often needs to be deployed across your entire organization, and requires that existing file and mail servers be ripped and replaced. As a result, GCC High is disruptive and time consuming to install, and expensive per user. While that approach may be viable for the largest primes that work exclusively for the DoD, the complexity and costs of GCC High are suboptimal for small to mid-size companies and universities. For those organizations, PreVeil offers compelling advantages, namely, military-grade security that addresses requirements for protecting CUI at a fraction of the cost of GCC High.

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

Google's standard Gmail platform also doesn't comply with CMMC Level 3 requirements for securing CUI. PreVeil supplements Gmail by adding end-to-end encryption, so that 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, while allowing them to keep their regular email address.

Case Study: PreVeil helps your company comply with NIST SP 800-171

PreVeil can help your organization comply with NIST SP 800-171, as illustrated by this actual case study:

In early 2021, a team of seven DIBCAC auditors undertook a rigorous audit of a small defense contractor with less than 100 employees. DIBCAC—the DoD's ultimate authority on compliance—conducted the random audit using DoD's NIST SP 800-171 Basic Assessment Framework. In preparation for the DIBCAC audit and upon the recommendation of its cybersecurity consultant, the contractor deployed PreVeil to all its users handling CUI, a rapid and easy process. The contractors then simply dragged and dropped sensitive data and CUI into folders in their PreVeil Drive and began using PreVeil's secure message system for sensitive communications, knowing that all communication between PreVeil users is automatically encrypted. This simple deployment laid the foundation for NIST SP 800-171 compliance.

The contractor achieved a near-perfect DIBCAC audit score by meeting 109 of the 110 controls and created a POAM for the one control that was not immediately achieved. Remarkably, this near-perfect NIST SP 800-171 score placed the defense contractor alongside the nation's top prime contractors for cybersecurity. The score is especially notable in light of the fact that a recent DIBCAC review of its assessments conducted during FY 2019 and FY 2020 found that just 22% of assessed companies satisfactorily demonstrated that they met all 110 NIST SP 800-171 controls.

Without PreVeil's advanced security and compliance features to protect CUI, the contractor's NIST SP 800-171 score would have been significantly lower. With PreVeil, if CMMC 2.0 had been in effect, the contractor would have been deemed to have met the new Level 2 requirements (with a POAM for the just the one remaining control) because PreVeil also complies with the CMMC Level 2 requirements that go beyond NIST SP 800-171.

The additional CMMC 2.0 requirements beyond NIST SP 800-171 flow from the fact that any organization that handles CUI is subject to DFARS 252.204-7012. That clause invokes not just its own (c)-(g) requirements for cyber incident reporting and the NIST SP 800-171 security controls, but also the FedRAMP Baseline Moderate or Equivalent standard for organizations that use cloud services. Additionally, NIST SP 800-171 invokes FIPS 140-2, which specifies cryptographic modules to be used for end-to-end encryption. PreVeil meets all of these requirements, unlike Microsoft 365 Commercial.

PreVeil also helped support DIBCo's audit process, as the DIBCAC audit team independently reached out to PreVeil to seek further clarification on specific security aspects of its end-to-end encrypted email and file sharing system. PreVeil responded quickly and provided documents to the audit team, including a detailed security architecture describing how its system encrypts and decrypts data, as well as how it supports compliance with NIST SP 800-171.

To learn more, see PreVeil's *Case Study: How a Defense Contractor using PreVeil Achieved a Near-Perfect NIST SP 800-171 Score in DIBCAC Audit*. And for a deep dive into DoD's NIST SP 800-171 Assessment Methodology, including how the scoring works, the weights given to each of the 110 controls, what your company needs to do to improve its self-assessment score, and more, see PreVeil's brief, *DFARS Self-Assessment: Improving Cybersecurity and Raising Your Score*.

Links to these papers and several additional relevant resources are provided in Appendix C.

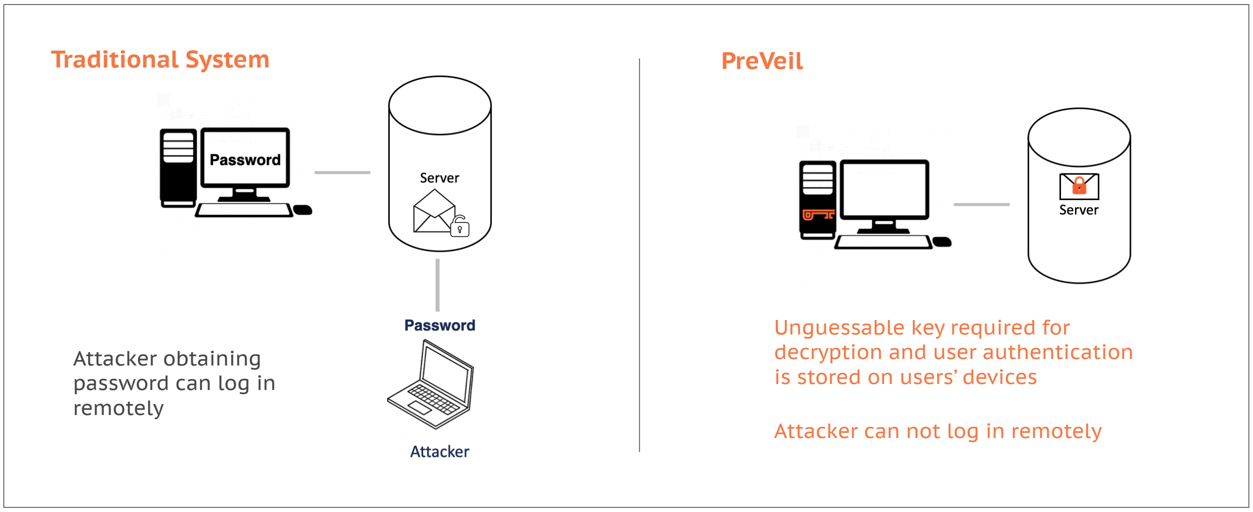
PreVeil Security and Compliance Features

PreVeil's state-of-the art security features can help your organization raise its cybersecurity levels, comply with NIST SP 800-171 requirements, and achieve the new CMMC Level 2, as described below.

Elimination of passwords

Instead of relying on passwords, PreVeil authenticates users via unguessable cryptographic keys that are automatically generated and stored on users' devices. Unlike passwords, it is mathematically impossible to guess these 256-bit keys by brute force techniques or by even the most sophisticated password cracking efforts. Replacing passwords with cryptographic keys also shuts down the many significant security risks that flow from phishing and spoofing attacks, including the use of compromised passwords for unauthorized access and malicious activity. And because the keys are stored on users' devices and nowhere else—including servers—there is no one central point of attack for hackers to target, as shown in Figure 3 below.

Figure 3: PreVeil eliminates password vulnerabilities with keys


Traditional System
Password
Server
Password
Attacker obtaining password can log in remotely
Attacker
PreVeil
Server
Unguessable key required for decryption and user authentication is stored on users' devices
Attacker can not log in remotely

Administrative console

Using PreVeil's Administrative 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.

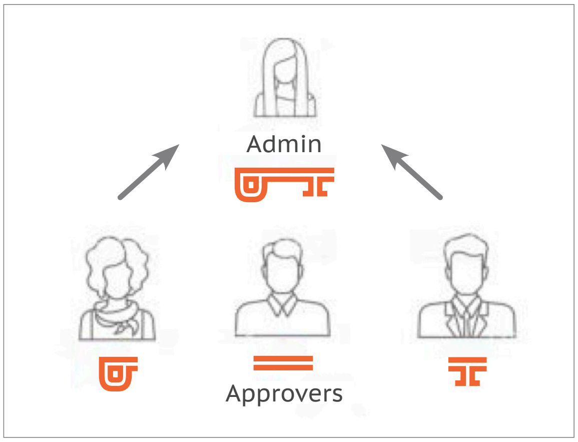
Approval Groups

With PreVeil, data stays secure even if an admin is compromised. That's accomplished by PreVeil's Approval Group feature, grounded in the principle of least privilege. Admins have to get approval from a pre-designated group of people within your business before accessing other users' information, as shown in Figure 4 below. Approval is a critical but seamless process.

Logging and continuous monitoring

PreVeil automatically logs all actions using cryptographic techniques similar to those used in blockchains to ensure that log entries are tamper proof and cannot be deleted. The logs allow visibility throughout the network and its devices, enabling constant monitoring and assessment of the security status of organizations' data. PreVeil's logging system also raises alerts in critical situations, such as when data is accessed from a new device, cryptographic keys are transferred, or a request for privileges is submitted.

Figure 4: PreVeil Approval Groups: Admin access only with complete key



Cloud-based service

Many organizations have avoided the cloud, keeping their file and email 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' FedRAMP High 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—can ever access user data.

Readily accessible data backups

PreVeil constantly backs up, encrypts, and retains every version of all your data and files, and so can readily recover them in the event of a ransomware attack. This is done via an append-only technique, which makes previously saved versions of documents immutable; that is, they are unchangeable. PreVeil also replicates your organization's encrypted data and files from Amazon Gov Cloud to another, geographically-distant area of the country, so that it can be recovered even in the event of a large-scale disaster. See PreVeil's brief, *Cybersecurity and Ransomware Protection*, for a more detailed explanation of how this works.

PreVeil Benefits

PreVeil understands the challenges that small to mid-size contractors must overcome to achieve CMMC Level 2. For organizations with limited cybersecurity expertise and compliance resources, the benefits of using PreVeil's secure platform include its ease of use and deployment, low cost, and a three-step roadmap to CMMC Level 2 certification, as described below.

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. Users keep their regular email address, which keeps it simple. File sharing works like DropBox and is integrated with the Windows File Explorer and Mac Finder.

Cost effectiveness

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

PreVeil's three-step roadmap to CMMC Level 2 certification

PreVeil offers a unique three-step solution to smooth your company's path to CMMC certification and make it more affordable.

Step One: Adopt a cloud platform to secure, store and share CUI. PreVeil Drive and Email are built on a modern Zero Trust security model, one strongly recommended by the NSA. Organizations can easily add PreVeil to their existing IT environments, dramatically reducing the time and expense required to achieve compliance.

PreVeil's platform delivers end-to-end encryption, ease of deployment and use, and compliance related to the protection of CUI.

Step Two: Take advantage of PreVeil's Security System Plan (SSP) template. An SSP is a prerequisite for any DoD work. To help defense contractors get this essential task done, PreVeil provides an SSP template to companies that deploy its platform. The SSP template is based on the 110 NIST SP 800-171 controls—which CMMC Level 2's security controls will mirror—and has been filled in to reflect PreVeil's capabilities and the requirements it meets.

The SSP template was created by PreVeil partners with extensive experience working with companies to complete their SSPs. The comprehensive template will give your organization a considerable head start on its SSP—otherwise a daunting, time-consuming, and costly task. In short, the PreVeil template dramatically accelerates your path to CMMC compliance.

Step Three: Leverage PreVeil's partner community. While PreVeil Drive and Email support compliance with virtually all of NIST and CMMC 2.0 mandates related to the storage and communication of CUI, other mandates will need to be addressed too. To facilitate that, PreVeil has partnered with hundreds of organizations and individuals certified by the CMMC-AB, with expert knowledge of DFARS, NIST, CMMC and PreVeil, as illustrated in Figure 5 below. Coordinated access to this specialized partner community will smooth your organization's path to compliance, saving time, minimizing your risks, and reducing costs.[10]

Figure 5: PreVeil's partner community: An indispensable resource

[10] To learn more about PreVeil's three-step solution to CMMC 2.0 Level 2 (Advanced) certification, see *Securing the Defense Supply Chain: Helping Your Subcontractors Comply with DFARS, NIST and CMMC*.

Conclusion

CMMC's cybersecurity standards will better arm the DoD in its efforts to defend against cyberattacks that threaten U.S. advantages in the military, technological and commercial realms. But it's clear that the DoD cannot wait for CMMC 2.0 to be implemented to improve cybersecurity in the Defense Industrial Base. While the new CMMC 2.0 framework works its way through the federal rulemaking process, enforcement of federal cybersecurity regulations governing defense contractors and universities doing DoD research has stepped up.

A key target for enforcement is NIST SP 800-171, which stipulates security controls necessary to protect CUI—a matter of high priority for the DoD. NIST SP 800-171 is currently the law of the land for defense contractors and researchers that handle CUI, and has been since 2017. Upon implementation, the new CMMC Level 2 security controls will completely align with NIST SP 800-171's 110 security controls. Clearly, focusing on your organization's compliance with NIST SP 800-171 now will smooth its path to the new Level 2 when CMMC 2.0 becomes law.

PreVeil leverages a fundamentally better security paradigm to help defense companies and universities comply with NIST SP 800-171—and with the additional requirements that must be met to achieve CMMC Level 2 when that time comes.

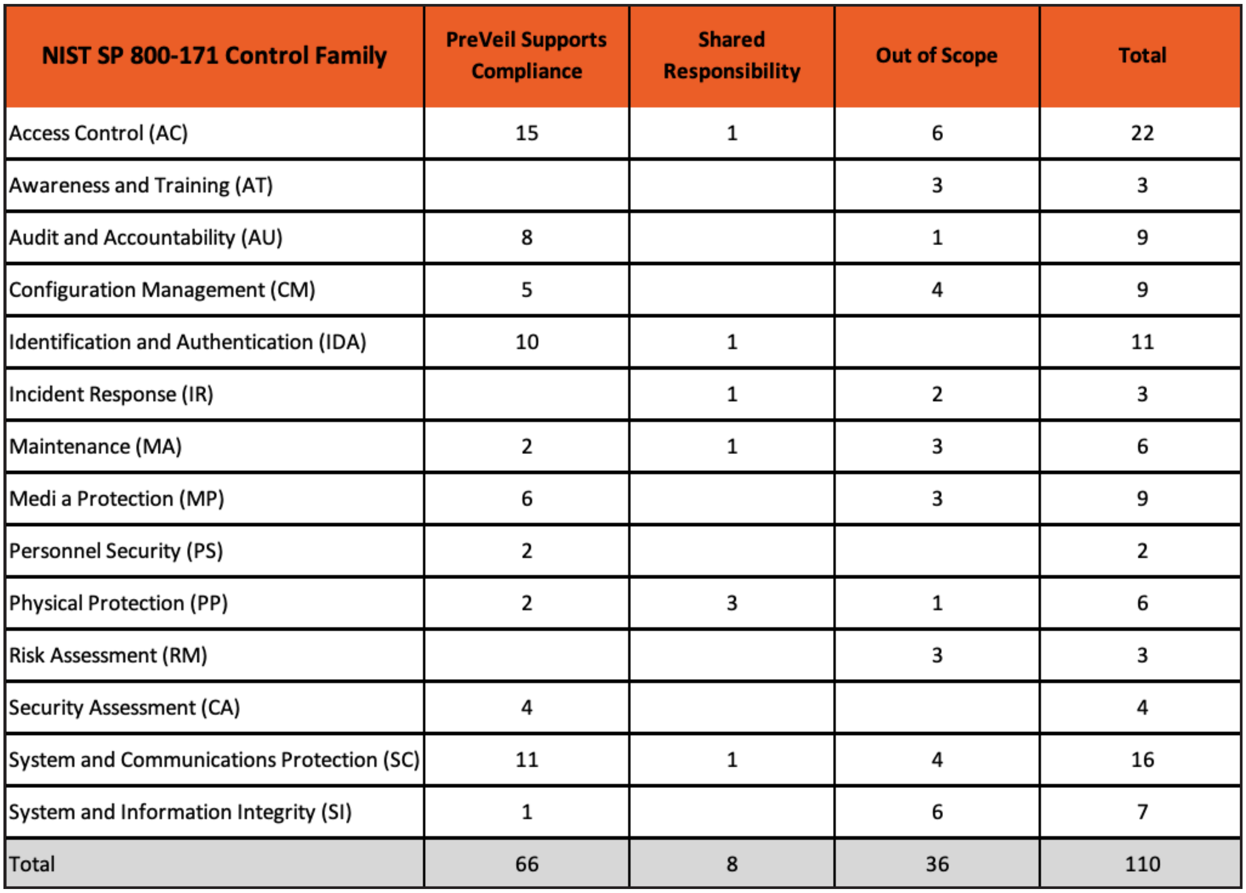
But better security isn't enough: if security is difficult to use, it won't be used. To be effective, security must be as frictionless as possible. PreVeil was created with this principle in mind so that your security objectives will be met. It integrates seamlessly with the file sharing and email tools you and your employees already use, making world class security simple to deploy and easy to use.

To learn more about how PreVeil's state-of-the-art encrypted Drive and Email platforms can help your organization improve its cybersecurity and achieve NIST SP 800-171 compliance and the new CMMC Level 2 more affordably, please access the compliance resources listed in Appendix C and contact us at preveil.com/contact or (857) 353-6480.

PREVEIL'S PRINCIPLES: GROUNDED IN THE REALITY OF TODAY'S SECURITY ENVIRONMENT

- **ZERO TRUST—never trust, always verify explicitly, and assume a breach**
- **END-TO-END ENCRYPTION—data is decrypted only on users' devices and never 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**

Appendix A: PreVeil Drive and Secure Messaging—NIST SP 800-171 Compliance Matrix Summary



NIST SP 800-171 Control Family	PreVeil Supports Compliance	Shared Responsibility	Out of Scope	Total
Access Control (AC)	15	1	6	22
Awareness and Training (AT)			3	3
Audit and Accountability (AU)	8		1	9
Configuration Management (CM)	5		4	9
Identification and Authentication (IDA)	10	1		11
Incident Response (IR)		1	2	3
Maintenance (MA)	2	1	3	6
Medi a Protection (MP)	6		3	9
Personnel Security (PS)	2			2
Physical Protection (PP)	2	3	1	6
Risk Assessment (RM)			3	3
Security Assessment (CA)	4			4
System and Communications Protection (SC)	11	1	4	16
System and Information Integrity (SI)	1		6	7
Total	66	8	36	110

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.1.1	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.2	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.3	Access Control (AC)	Control the flow of CUI in accordance with approved authorizations.	**Yes** **Supports Compliance**	End-to-end encryption with device-based keys provide tools for control of CUI at the user and device level. Only those granted access by organization administrators can view the information. End to end encryption provides complete security of data at the server level whether on-premise or in the cloud. PreVeil's Trusted Community feature can also limit access to CUI. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.4	Access Control (AC)	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	**Yes** **Supports Compliance**	Only Administrators can access Administrative functions and only a cryptographic controlled Approval Group of Administrators can change high-risk system configuration settings or delete or decrypt enterprise data general user access to only what is necessary based on the user's business need. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.5	Access Control (AC)	Employ the principle of least privilege, including for specific security functions and privileged accounts.	**Yes** **Supports Compliance**	Only Administrators can access Administrative functions and only a cryptographic controlled Approval Group of Administrators can change high-risk system configuration settings or delete or decrypt enterprise data general user access to only what is necessary based on the user's business need. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.6	Access Control (AC)	Use non-privileged accounts or roles when accessing nonsecure 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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.7	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 required to do their basic job functions. Administrative Approval Groups protect against inappropriate use of privileged and security functions. 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). PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.1.8	Access Control (AC)	Limit unsuccessful logon attempts.	**Yes Supports Compliance**	Access to the PreVeil system is granted via public/private user and device keys and not user name/password logon. Multiple attempts at logon 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 access the CUI stored on PreVeil. Individual users, in addition to administrators, may remotely revoke keys or disable devices registered to an account in the event of loss or compromise. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.9	Access Control (AC)	Provide privacy and security notices consistent with applicable CUI rules.	**Yes Supports Compliance**	PreVeil desktop application includes a click-through message to PreVeil users notifying them about potential CUI on device in use.
3.1.10	Access Control (AC)	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	**Shared Responsibility**	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.
3.1.11	Access Control (AC)	Terminate (automatically) a user session after a defined condition.	**Enabled Outside of PreVeil**	
3.1.12	Access Control (AC)	Monitor and control remote access sessions.	**Yes Supports Compliance**	Administrators can control remote sessions via device management from the Admin Console. All PreVeil sessions, local and remote, are controlled via approved 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. End-to-end encryption controls access to remote access sessions. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.13	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.
3.1.14	Access Control (AC)	Route remote access via managed access control points.	**Enabled Outside of PreVeil**	
3.1.15	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 remotely executed Approval Group authorizations for privileged commands including Data Export, Deleting Users and Assigning Admins. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.16	Access Control (AC)	Authorize wireless access prior to allowing such connections.	**Enabled Outside of PreVeil**	
3.1.17	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.1.18	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 additions can be managed. Access to PreVeil on any device can be locked by Administrators. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.1.19	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. PreVeil supports compliance with this Practice only when CUI is stored locally on devices using PreVeil. Any additional device or container that contains CUI must also use FIPS-validated encryption, following guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper storage and use of CUI on mobile devices.
3.1.20	Access Control (AC)	Verify and control/limit connections to and use of external information systems.	**Enabled Outside of PreVeil**	
3.1.21	Access Control (AC)	Limit use of organizational portable storage devices on external information systems.	**Enabled Outside of PreVeil**	
3.1.22	Access Control (AC)	Control information posted or processed on publicly accessible information systems.	**Enabled Outside of PreVeil**	
3.2.1	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.	**Enabled Outside of PreVeil**	
3.2.2	Awareness and Training (AT)	Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	**Enabled Outside of PreVeil**	
3.2.3	Awareness and Training (AT)	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	**Enabled Outside of PreVeil**	
3.3.1	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**	Administrators can view user logs. Logs cannot be deleted or modified. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.3.2	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 Administrators 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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.3.3	Audit and Accountability (AU)	Review and update audited events.	**Yes Supports Compliance**	Admins can view user logs. Logs cannot be deleted or modified. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.3.4	Audit and Accountability (AU)	Alert in the event of an audit process failure.	**Enabled Outside of PreVeil**	
3.3.5	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.	**Yes Supports Compliance**	PreVeil enables the export of system logs (via an Approval Group) to provides this analysis.
3.3.6	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.3.7	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.3.8	Audit and Accountability (AU)	Protect audit information and audit tools from unauthorized access, modification, and deletion.	Yes Supports Compliance	User and Administrator activity is logged and cryptographically protected against tampering. Logs can be exported to a central repository. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.3.9	Audit and Accountability (AU)	Limit management of audit logging functionality to a subset of privileged users.	Yes Supports Compliance	PreVeil Administrative logs (organization-wide) are only accessible to administrators. The Administrative Approval Group feature eliminates single point of failure on invasive administrative actions. User logs are only available to that specific user. Logs are tamperproof and cannot be modified or deleted. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.4.1	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.	Enabled Outside of PreVeil	
3.4.2	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 configuration, access to and management of the data in the PreVeil system. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies
3.4.3	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.4.4	Configuration Management (CM)	Analyze the security impact of changes prior to implementation.	Enabled Outside of PreVeil	
3.4.5	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.4.6	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 Administrators can perform administrative functions. Only formal Approval Groups can authorize specific invasive system actions. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.4.7	Configuration Management (CM)	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.	Enabled Outside of PreVeil	
3.4.8	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.	Enabled Outside of PreVeil	
3.4.9	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.5.1	Identification and Authentication (IDA)	Identify information system users, processes acting on behalf of users, or devices.	Yes Supports Compliance	Identity and authentication is established cryptographically via user and device-specific private keys, which are managed and enforced via the Admin Console. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.5.2	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's end-to-end encryption ensures that only authorized and authenticated users on authorized devices can access the secure data in PreVeil. Identity and authentication is established cryptographically via user and device-specific private keys. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.5.3	Identification and Authentication (IDA)	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	**Yes Supports Compliance**	You must have an authorized device to access PreVeil. In addition to the device passwords required to log into a laptop or device, PreVeil requires a second factor (your cryptographic user and device private keys) to authenticate to the PreVeil service. Identity and authentication are established cryptographically via user private keys and device-specific private keys. Additionally, on mobile devices, PreVeil supports biometric authentication for access to encrypted content.
3.5.4	Identification and Authentication (IDA)	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	**Yes Supports Compliance**	PreVeil leverages device-to-device cryptographic authentication via intrinsically linked user and device keys to eliminate the potential for a man-in-the-middle attack. PreVeil supports compliance with this practice when combined with additional policies, procedures, and/or technologies.
3.5.5	Identification and Authentication (IDA)	Prevent reuse of identifiers for a defined period.	**Yes Supports Compliance**	PreVeil leverages device-to-device cryptographic authentication via intrinsically linked user and device keys to eliminate the potential for a man-in-the-middle attack. PreVeil supports compliance with this practice when combined with additional policies, procedures, and/or technologies.
3.5.6	Identification and Authentication (IDA)	Disable identifiers after a defined period of inactivity.	**Shared Responsibility**	The PreVeil system supports disabling of inactive user account identifiers and related accounts as required by policy.
3.5.7	Identification and Authentication (IDA)	Enforce a minimum password complexity and change of characters when new passwords are created.	**Yes Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication are 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	Identification and Authentication (IDA)	Prohibit password reuse for a specified number of generations.	**Yes Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication are 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	Identification and Authentication (IDA)	Allow temporary password use for system logons with an immediate change to a permanent password.	**Yes Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication are 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	Identification and Authentication (IDA)	Store and transmit only cryptographically-protected passwords.	**Yes Supports Compliance**	PreVeil's security model eliminates passwords for identify verification. Identity and authentication are established cryptographically via user private keys and device-specific private keys. PreVeil eliminates the need for any additional passwords or encryption certificate management.
3.5.11	Identification and Authentication (IDA)	Obscure feedback of authentication information.	**Yes 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.
3.6.1	Incident Response (IR)	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	**Shared Responsibility**	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.
3.6.2	Incident Response (IR)	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	**Enabled Outside of PreVeil**	
3.6.3	Incident Response (IR)	Test the organizational incident response capability.	**Enabled Outside of PreVeil**	

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.7.1	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.7.2	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. If a customer elects to host the storage on-premise, the customer is responsible for infrastructure maintenance. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.7.3	Maintenance (MA)	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	**Shared Responsibility**	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.
3.7.4	Maintenance (MA)	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	**Enabled Outside of PreVeil**	
3.7.5	Maintenance (MA)	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	**Enabled Outside of PreVeil**	
3.7.6	Maintenance (MA)	Supervise the maintenance activities of personnel without required access authorization.	**Enabled Outside of PreVeil**	
3.8.1	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 for proper media sanitization. PreVeil supports compliance with this Practice only when FCI is stored solely on PreVeil. Any additional device or service that contains FCI must also follow the guidelines put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper sanitization of FCI.
3.8.2	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 system access and actions are logged (logs are encrypted and hash-chained to prevent tampering). AWS meets control requirements for limiting physical access to system infrastructure. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper access control of CUI.
3.8.3	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 for proper media sanitization. PreVeil supports compliance with this Practice only when FCI is stored solely on PreVeil. Any additional device or service that contains FCI must also follow the guidelines put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper sanitization of FCI.
3.8.4	Media Protection (MP)	Mark media with necessary CUI markings and distribution limitations.	**Enabled Outside of PreVeil**	

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.8.5	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 for physical control and provides secure protection and monitoring of facilities. PreVeil supports compliance with this Practice only when CUI is digitally stored or transported solely on PreVeil. Any additional device, service, or location that stores or transports CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper controlled access to CUI.
3.8.6	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. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI, hardcopy or digital, must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper protection of CUI.
3.8.7	Media Protection (MP)	Control the use of removable media on system components.	**Enabled Outside of PreVeil**	
3.8.8	Media Protection (MP)	Prohibit the use of portable storage devices when such devices have no identifiable owner.	**Enabled Outside of PreVeil**	
3.8.9	Media Protection (MP)	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. PreVeil supports compliance with this Practice only when CUI is stored solely on devices using PreVeil. Any additional device or container that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper confidentiality of CUI backup.
3.9.1	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 secure protection and monitoring of facilities. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper personnel security.
3.9.2	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. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper personnel security.
3.10.1	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 secure protection and monitoring of facilities. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper personnel security.

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.10.2	Physical Protection (PP)	Protect and monitor the physical facility and support infrastructure for organizational systems.	**Shared Responsibility**	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 secure protection and monitoring of facilities. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper personnel security.
3.10.3	Physical Protection (PP)	Escort visitors and monitor visitor activity.	**Shared Responsibility**	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 secure protection and monitoring of facilities. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper personnel security.
3.10.4	Physical Protection (PP)	Maintain audit logs of physical access.	**Shared Responsibility**	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 secure protection and monitoring of facilities. With PreVeil, CUI, ITAR and EAR data is protected at all times with end-to-end encryption. PreVeil supports compliance with this Practice only when CUI is digitally stored solely on PreVeil. Any additional device, service, or location that contains CUI must also follow guidance put forth in CMMC Appendix B. We recommend implementing policies and/or procedures to outline proper personnel security.
3.10.5	Physical Protection (PP)	Control and manage physical access devices.	**Enabled Outside of PreVeil**	
3.10.6	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.11.1	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.	**Enabled Outside of PreVeil**	
3.11.2	Risk Assessment (RM)	Scan for vulnerabilities in the organizational system and applications periodically and when new vulnerabilities affecting the system and applications are identified.	**Enabled Outside of PreVeil**	
3.11.3	Risk Assessment (RM)	Remediate vulnerabilities in accordance with risk assessments.	**Enabled Outside of PreVeil**	
3.12.1	Security Assessment (CA)	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	**Yes Supports Compliance**	PreVeil is SOC-2 certified and periodically assesses system security controls.
3.12.2	Security Assessment (CA)	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	**Yes Supports Compliance**	PreVeil is SOC-2 certified and periodically assesses system security controls.

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.12.3	Security Assessment (CA)	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	**Yes Supports Compliance**	PreVeil is SOC-2 certified and periodically assesses system security controls.
3.12.4	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.	**Yes Supports Compliance**	PreVeil is SOC-2 certified and periodically assesses system security controls.
3.13.1	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.2	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.3	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.4	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.5	System and Communications Protection (SCP)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	**Enabled Outside of PreVeil**	
3.13.6	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.7	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.

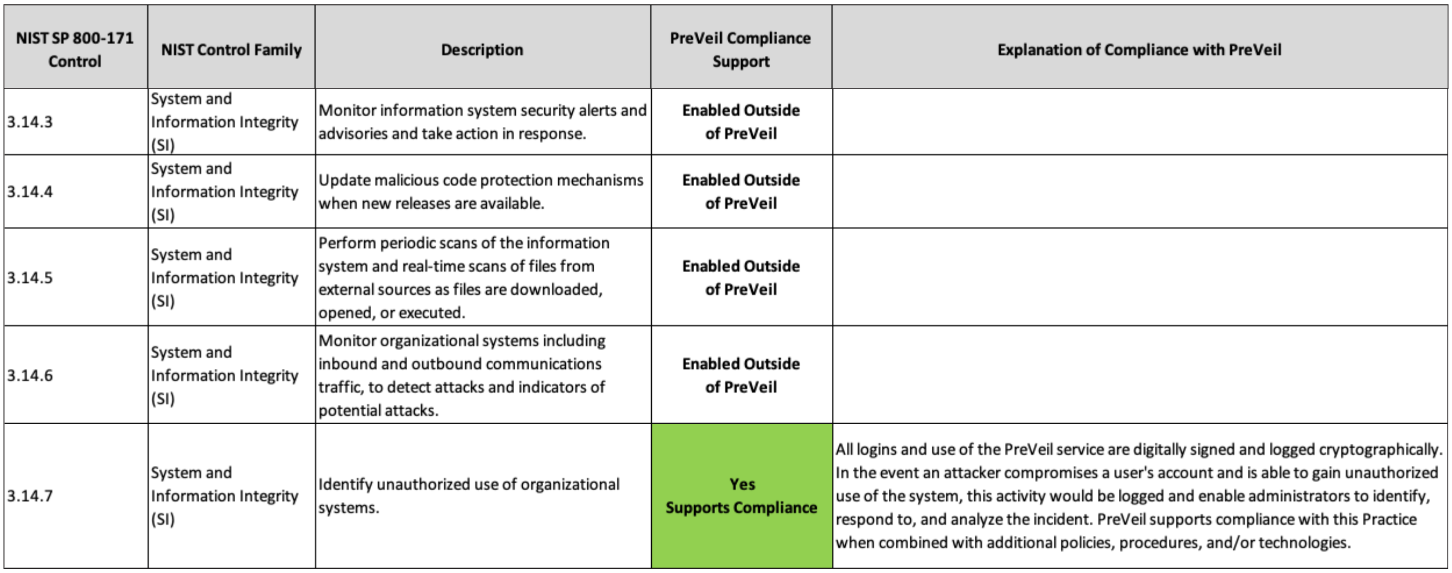
Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix

NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.13.8	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 transmission, and remain encrypted end-to-end until the data reaches 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. *PreVeil 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. PreVeil supports compliance with this Practice only when CUI is stored solely on devices using PreVeil. Any additional systems or devices that contain CUI must follow guidance put forth in CMMC Appendix B.
3.13.9	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.	**Shared Responsibility**	PreVeil supports device and network level controls regarding termination of network connections in these situations.
3.13.10	System and Communications Protection (SCP)	Establish and manage cryptographic keys for cryptography employed in organizational systems.	**Yes Supports Compliance**	PreVeil protects cryptographic key confidentiality and authenticity through decentralized key management that is transparent to the user and is further described in the PreVeil encryption architecture white paper. PreVeil supports compliance with this Practice only when CUI is stored solely on devices using PreVeil. Any additional systems or devices that contain CUI must follow guidance put forth in CMMC Appendix B.
3.13.11	System and Communications Protection (SCP)	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	**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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.12	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.	**Enabled Outside of PreVeil**	
3.13.13	System and Communications Protection (SCP)	Control and monitor the use of mobile code.	**Enabled Outside of PreVeil**	
3.13.14	System and Communications Protection (SCP)	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	**Enabled Outside of PreVeil**	
3.13.15	System and Communications Protection (SCP)	Protect the authenticity of communications sessions.	**Yes Supports Compliance**	PreVeil leverages device-to-device cryptographic authentication via intrinsically linked user and device keys. All user actions are cryptographically signed with the user's private key. For additional information, please see PreVeil's encryption architecture white paper. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.
3.13.16	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 in use on the server. The keys to decrypt data are never stored centrally. For additional information, please see PreVeil's encryption architecture white paper. PreVeil supports compliance with this Practice only when CUI is stored solely on devices using PreVeil. Any additional systems or devices that contain CUI must follow guidance put forth in CMMC Appendix B.
3.14.1	System and Information Integrity (SI)	Identify, report, and correct information and information system flaws in a timely manner.	**Enabled Outside of PreVeil**	
3.14.2	System and Information Integrity (SI)	Provide protection from malicious code at appropriate locations within organizational information systems.	**Enabled Outside of PreVeil**	

Note: This NIST SP 800-171/CMMC 2.0 Level 2 controls mapping document contains detail only on controls that PreVeil helps to support. Please note that many controls are dependent on enterprise policies aligned with the PreVeil information system functionality. This document should not be included as-is into a System Security Plan. You are responsible for determining which controls 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 sample controls set forth in this document in your System Security Plan.

Appendix A: PreVeil Drive and Secure Messaging–NIST SP 800-171 Compliance Matrix



NIST SP 800-171 Control	NIST Control Family	Description	PreVeil Compliance Support	Explanation of Compliance with PreVeil
3.14.3	System and Information Integrity (SI)	Monitor information system security alerts and advisories and take action in response.	**Enabled Outside of PreVeil**	
3.14.4	System and Information Integrity (SI)	Update malicious code protection mechanisms when new releases are available.	**Enabled Outside of PreVeil**	
3.14.5	System and Information Integrity (SI)	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	**Enabled Outside of PreVeil**	
3.14.6	System and Information Integrity (SI)	Monitor organizational systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	**Enabled Outside of PreVeil**	
3.14.7	System and Information Integrity (SI)	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. PreVeil supports compliance with this Practice when combined with additional policies, procedures, and/or technologies.

Appendix B: PreVeil vs. Alternatives

The Department of Defense requires organizations that store or share CUI to meet the requirements for CMMC 2.0 Level 2 (Advanced) or Level 3 (Expert). Most commercial cloud services don't meet these requirements when files or emails containing CUI are stored or processed in the cloud. Microsoft 365 Commercial and SharePoint services, for example, are not DoD compliant for handling CUI.

The leading options for cloud-based platforms that comply with virtually all the new CMMC Level 2 requirements related to the storage and sharing of CUI are Microsoft's GCC High and PreVeil. Note that neither option by itself will take your company all the way to CMMC Level 2; in both cases, you will need to address additional security mandates beyond those pertaining to CUI.

Microsoft GCC High is a comprehensive solution for large organizations striving for CMMC compliance. However, GCC High is a complex system to deploy and configure. It most often needs to be deployed across your entire organization, and requires that existing file and email services be ripped and replaced. As a result, GCC High is disruptive and time consuming to install and expensive per user.

Microsoft readily acknowledges the difficulties of migrating users to its GCC High platform. A Microsoft blog post put it this way: "This pain and frustration [of migrating users] is further exasperated [sic] if the users are located in a Commercial Cloud. You can only imagine the baggage associated with a migration from Commercial. It often includes the re-homing of device and software registrations, MDM [Mobile Device Management] enrollments, encryption technologies, etc."

Nevertheless, GCC High is a viable option for the largest primes that work exclusively for the DoD.

PreVeil, on the other hand, offers compelling advantages for small to mid-size companies and organizations with both commercial and defense business, as well as universities. PreVeil is easy to deploy. It complements Microsoft 365 Commercial as a simple overlay, with no impact on an organization's regular file or email servers. And because it needs to be deployed only to users that handle CUI, it's far more cost effective than Microsoft GCC High—which most often must be purchased for the entire organization. Further, the obligatory switch to Microsoft GCC High Exchange servers is a complex undertaking that requires special planning and configuration.

Another cloud-based option for protecting CUI is Box for Government, which PreVeil also compares favorably to, as shown in the table below.

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

- PreVeil is grounded in modern Zero Trust security principles and the gold standard of end-to-end encryption. Microsoft GCC High and Box for Government, on the other hand, rely on legacy, perimeter-based approaches to security. The NSA explains in a February 2021 memorandum that the Zero Trust model contrasts with "Traditional perimeter-based network defenses with multiple layers of disjointed security technologies [which] have proven themselves to be unable to meet the cybersecurity needs due to the current threat environment." Indeed, the NSA urges the entirety of the DoD and the DIB to adopt the Zero Trust security model.[11]

- PreVeil uses end-to-end encryption so that only senders and recipients of files and emails can see the data; PreVeil servers operates on encrypted data and can never access the decryption keys. Conversely, both Microsoft GCC High and Box for Government offer optional enhanced 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, and renders successful penetration of data servers useless.
- 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 extremely difficult to compromise an administrator.
- PreVeil's Trusted Communities allow an organization to create a list of trusted external entities. No one else is allowed to send or receive encrypted email or files to the organization, which is extremely effective for managing CUI.

	PreVeil	Microsoft GCC High	Box For Government
PRODUCT	Email & Files	Email & Files	Files Only
SECURITY			
Zero Trust	Built on Zero Trust principles	Relies on legacy perimeter defenses	Relies on legacy perimeter defenses
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
Trusted Lists	Trusted Communities	None—open to untrusted phishing/spoofing	Limited to domain- based listing
DRIVE	No impact to existing file servers	Rip and replace file server and domain	Requires centralized key server that must be provisioned, managed and protected
Deployment	Only users with CUI need deploy	Typically, must be deployed to 100% of the organization	
EMAIL	No impact to existing file servers	Rip and replace email server and domain	N/A
Deployment	Only users with CUI need deploy	Typically, must be deployed to 100% of the organization	
COST	$30/user/month	$$$$	$$$$

[11] Note that while at this point it is still possible to comply with CMMC and NIST SP 800-171 using legacy security systems, a better path to compliance is achievable through modern Zero Trust systems. To learn more about how Zero Trust creates fundamentally better cybersecurity, see PreVeil's brief, *Zero Trust: A better way to enhance cybersecurity and achieve compliance*.

Appendix C: PreVeil CMMC, DFARS, NIST and ITAR compliance resources

- *Zero Trust: A Better Way to Enhance Cybersecurity and Achieve Compliance.* Simply put, the NSA's principles for a Zero Trust security model are to never trust, always verify explicitly, and to assume a breach. A Zero Trust mindset creates fundamentally better cybersecurity. This brief was written to help defense companies better understand Zero Trust principles, comply with DoD regulations, and win defense contracts.
- *DFARS Self-Assessment: Improving Cybersecurity and Raising your NIST SP 800-171 Score.* The Interim DFARS Rule mandates that NIST SP 800-171 self-assessment scores be reported to the DoD, and it stands to reason that higher scores will win more contracts. This brief shows how PreVeil can help raise your self-assessment score by nearly 40 points.
- *Case Study: How a Defense Contractor using PreVeil Achieved a Near-Perfect NIST SP 800-171 Score in DIBCAC Audit.* A defense contractor using PreVeil underwent a rigorous DIBCAC audit and met 109 of the 110 NIST SP 800-171 controls, placing them alongside the nation's top prime contractors for cybersecurity.
- *Getting Started with NIST SP 800-171 Compliance in Higher Education.* The US Department of Education, following the lead of DoD, is ramping up enforcement of NIST SP 800-171 requirements to protect federal student aid data. This brief outlines steps for universities to take now to achieve compliance.
- *Securing the defense supply chain: Helping your subcontractors comply with DFARS, NIST and CMMC.* The Interim DFARS Rule released in December 2020 has placed responsibility for subcontractors' compliance with DFARS, NIST and CMMC squarely on the shoulders of their contractors. This brief helps contractors accelerate their subcontractors' compliance efforts.
- *PreVeil's End-to-End Encryption Enables ITAR Compliance.* New State Department guidelines exempt ITAR-restricted data from federal regulations when that data is secured using end-to-end encryption that meets standards specified in FIPS Publication 140-2. This brief explains the new guidelines and how PreVeil meets them.
- *Cybersecurity and Ransomware Protection.* Ransomware attacks are increasing at an alarming pace. PreVeil provides affordable military-grade cybersecurity to protect organizations' critical data—and readily recover it in the event of a ransomware attack—so that you don't have to pay a ransom. This brief describes how PreVeil makes that happen and keeps your business running smoothly.

To access additional briefs, please visit PreVeil's resources page.

About PreVeil

PreVeil was built from the ground up to implement Zero Trust principles and to make military-grade security accessible for everyday business. Its state-of-the-art encrypted Drive and Email platforms can help your organization improve its cybersecurity and achieve the new CMMC Level 2 certification. PreVeil Drive works like DropBox for file sharing and collaboration, but with far better security. PreVeil Email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. All documents and messages 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 to help 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

PREVEIL

Dec. 2021 v9.0