PREVEIL

# Complying with the Department of Defense's Cybersecurity Maturity Model Certification

# 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 response created 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.

CMMC has three compliance levels: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert). Defense contractors aiming to achieve Level 1 will be permitted to self-attest their cybersecurity compliance, as will some limited number of contractors certified at Level 2. All others will need to undergo independent third-party reviews.

Organizations that handle CUI will need to achieve at least Level 2. Level 2's security controls will be in complete alignment with the 110 security controls of NIST SP 800-171, and Level 2 certification will indicate that an organization is able to securely store, process and transmit CUI—a 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 clauses 7012, 7019 and 7020. DFARS 7012 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 CMMC Level 2.

The CMMC initiative is 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 increased its audit staff size in response to the pressing need to improve security in the Defense Industrial Base. For its part, the Department of Justice has launched a robust 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 steers the CMMC program through the federal rulemaking process, it is also stepping up

enforcement of NIST SP 800-171. Since late 2020, DFARS 7019 has required contactors to report their NIST SP 800-171 self-assessment scores to DoD's SPRS Supplier Performance Risk System (SPRS). And when CMMC is implemented, those 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. Your organization will need to achieve excellent self-assessment scores, because even though POA&Ms will be allowed under CMMC, they won't be allowed for the highest weighted NIST SP 800-171 controls, which are also some of the hardest to achieve. And unlike in the past, POA&Ms will be tightly time-limited under the CMMC model.

The key to achieving CMMC Level 2 certification is to implement technology solutions in conjunction with appropriate policies and procedures to ensure the security of CUI. CUI is most frequently exchanged via file sharing and email. But most widely-deployed commercial systems used to store, process and transmit CUI—such as Microsoft 365 Commercial or Gmail—do not comply with all CMMC Level 2 requirements, a point that Microsoft readily acknowledges. (See Appendix C for more details.) Organizations using such solutions will need to adopt new platforms to improve their cybersecurity, achieve 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, we offer brief explanations of fundamental cybersecurity principles and how they connect with CMMC, beginning with end-to-end encryption. Building upon that base, the paper includes a practical guide outlining what your company needs to do to achieve 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, processing and transmitting 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. PreVeil simplifies your compliance journey and makes it more affordable. Its comprehensive compliance documentation package and the Governance, Risk and Compliance (GRC) tool it offers will save your organization an enormous amount of time and effort along the way. And PreVeil's partner community of C3PAOs, Certified CMMC Assessors, Registered Practioners, MSPs (Managed Service Providers), and other consultants and organizations certified by the Cyber AB—all with expert knowledge of DFARS, NIST, CMMC and PreVeil—will streamline your journey to CMMC Level 2 certification.

In short, if you are unfamiliar with what it takes to be DoD compliant, PreVeil can support your organization's compliance journey every step of the way, from deployment of its platform to compliance documentation and GRC assessment, to its partner community and audit responses as needed.

The brief concludes with detailed and helpful appendices. For example, Appendix A presents a comprehensive matrix that lists each CMMC Level 2 practice and corresponding NIST SP 800- 171 security control and objectives, and indicates which requirements PreVeil helps to meet. Appendix B presents an actual case study of how a small defense contractor using PreVeil achieved the highest possible score of 110 out of 110 on a NIST SP 800-171 DIBCAC audit.

Finally, note that earlier versions of this paper have been downloaded more than 2,000 times by defense contractors. It is our hope that this completely updated version—reflecting the latest information available as of its release in June 2023—serves to help your organization, too, as you work to better protect your data resources and CUI, and win defense contracts.

# CMMC 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.

## CMMC compliance levels

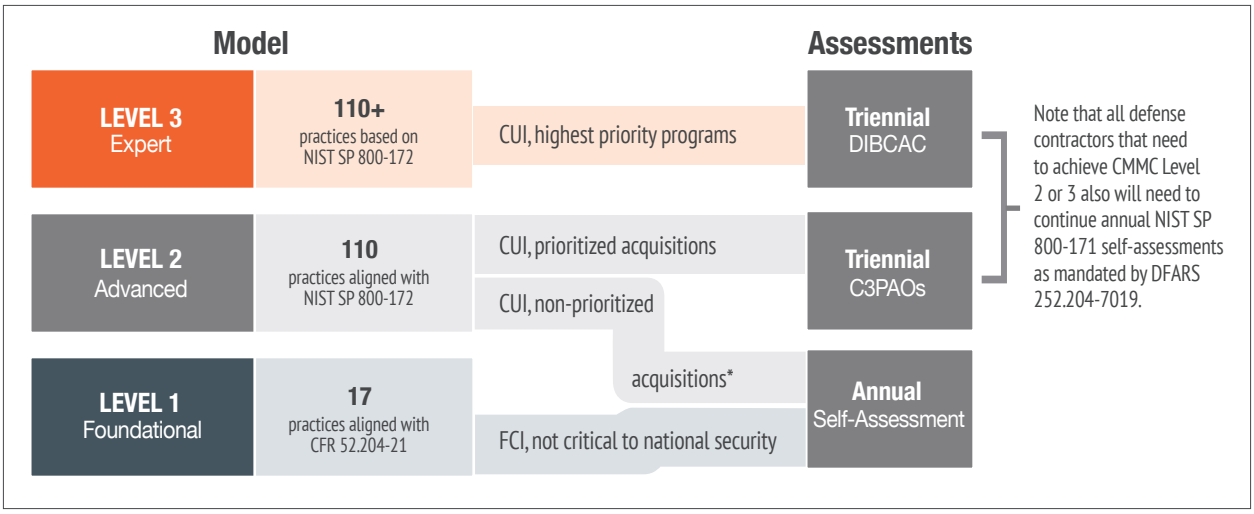
CMMC has three compliance levels, based on the type of information DIB organizations are working with:

- Level 1 (Foundational) is for organizations working with FCI only
- Level 2 (Advanced) is for organizations working with CUI
- Level 3 (Expert) is for organizations working with CUI on DoD's highest priority programs

## CMMC assessment requirements

CMMC assessment requirements will be based on the type of information DIB organizations are working with, as illustrated in Figure 1.

**Figure 1: CMMC model and assessments based on information being handled**




Source: DoD Chief Information Officer website.

* DoD CISO David McKeown reported during a February 2022 DoD CISO Special Session Town Hall that after conducting an analysis of the work of the DIB contractors that will need CMMC Level 2 certification, the DoD determined that it expects to require all defense contractors at Level 2 to undergo outside assessments conducted by Cyber AB certified C3PAOs. That is, Level 2 may not be bifurcated as illustrated in this figure and described below. If and when this decision is formally announced, this paper will be updated to reflect this change.

At Level 1, defense contractors handling FCI will be required to perform annual self-assessments. At Level 2, a very small subset of contractors also will be required to perform annual self-assessments. The subset includes contractors that, while handling CUI, are working on projects that do not involve sensitive national security information, i.e., non-prioritized acquisitions. (See note under Figure 1 above, however, for more information.) 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 need to be conducted by accredited C3PAOs (CMMC Third Party Assessment Organizations). After completion of the CMMC assessment, the C3PAO will provide an assessment report to the DoD.

Forty-two accredited C3PAOs were listed on the Cyber AB (formerly the CMMC-AB) Marketplace in June 2023. Ideally, the pace of accreditation of these critical components of the CMMC ecosystem will accelerate. Contractors will be fully responsible for obtaining and coordinating their needed assessment and certification.

As of June 2023, 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 offered 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 Level 2 (Advanced) security controls will mirror NIST SP 800-171

CMMC Level 2 (Advanced) security controls will be in complete alignment with NIST SP 800-171's 110 security controls.

Going forward, DoD is committed to working with NIST (the National Institute of Technology and Standards) 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.

## CMMC will allow POA&Ms in limited circumstances

The DoD will allow companies to be awarded defense contracts under CMMC with a POA&M in place for security controls they have not yet met at the time of the award. However, according to senior DoD officials, POA&Ms will not be permitted for the highest-weighted security requirements—which also are some of the hardest requirements to meet. The DoD's self-assessment methodology for NIST SP 800-171 gives each of the 110 controls a weight of one, three or five points. Scoring starts at the lowest possible score of -203. One, three, or five points are earned for each control met, all the way up to the maximum of +110. Negative self-assessment scores are possible, as scores can range from -203 to +110, a spread of 313 points.

DoD is also planning to establish a minimum SPRS self-assessment score that must be achieved when POA&Ms are used to support CMMC certification. The Cyber AB's draft CMMC Assessment Process (aka CAP), released in July 2022, reflects this approach, stipulating that organizations can receive a "CMMC Level 2 Conditional Certification" only if at least 80% of all CMMC Level 2 practices (i.e., 88 of the 110 NIST SP 800-171 controls) are met.

Further, POA&Ms will be time-bound, with limits strictly enforced. On this subject the Cyber AB's draft CAP states that organizations given CMMC Level 2 Conditional Certification are responsible for ensuring that all deficiencies listed in their POA&M are corrected within 180 days from the time of their "Final Findings" briefing with their C3PAO. The CAP further notes that this timeframe includes scheduling a CMMC POA&M Close-Out Assessment.

## CMMC 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. 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.

## CMMC rulemaking and timeline

The DoD is codifying CMMC through the federal rulemaking process, which will provide the authority needed to effectively measure and enforce cybersecurity compliance throughout the DIB. Several signs of momentum toward implementation of CMMC are clear. In summer 2022, for example, the Cyber AB released its draft CMMC Assessment Process (CAP). The release of the draft CAP meant that voluntary third- party assessments of organizations' compliance with NIST SP 800-171 could begin. Those assessments are being conducted now by C3PAOs in collaboration with DIBCAC auditors, and are known as Joint Surveillance Voluntary Assessments. The assessments focus on NIST SP 800-171 compliance because the CMMC framework has not yet been codified into law. Recall, however, that CMMC Level 2's security controls will be in complete alignment with NIST SP 800-171's controls—meaning that organizations undergoing voluntary assessments now are competitively positioning themselves for CMMC Level 2 certification as soon as that's possible.

As of this writing in June 2023, the clearest sign of CMMC becoming law is that it appears that DoD is aiming to release Proposed Rules within the next few months to legally establish the CMMC program. The Proposed Rules would allow for comment periods and then time would be taken for responses to those comments. Or, it's possible that a faster route could be pursued via release of an Interim Final Rule, which would convert in 60 days to a Final Rule and put CMMC into effect at that point.

***There is no correlation between the size of defense contracts and when CMMC requirements will appear in those contracts.***

It is important for contractors to understand that even though once CMMC becomes law it may be phased in over time, it does not necessarily follow that if you're a small to mid-size contractor, or have a small defense-related contract, then your organization will have more time to achieve CMMC certification. Your organization, for example, could be far down the supply chain from a contractor subject to CMMC; if that's the case, per DFARS 7020, that contractor must flow down CMMC requirements to all subcontractors throughout its supply chain, which would include your organization.

In short, there is no correlation between the size of defense contracts and when CMMC requirements will appear in those contracts. Now, while CMMC rulemaking is underway, is the time to improve your cybersecurity posture. A good place to start is to familiarize yourself with the modern cybersecurity principles described in the next section.

# Modern Cybersecurity Principles and CMMC

This section is offered as a brief primer on modern cybersecurity principles and how they connect to NIST SP 800-171's security controls. To that end, specific CMMC/NIST SP 800-171 control families addressed by each cybersecurity principle are noted.

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.

## 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 CMMC/NIST SP 800-171 control families: Access Control, Configuration Management, Media Protection, Systems & Communications Protection, and System & Informational Integrity.

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

## 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 CMMC/NIST 800-171 control family: Audit & Accountability.

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

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

## Key-based authentication instead of passwords

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.

Moreover, device-based keys prevent hackers from ever 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.

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

Key-based authentication can help address the following CMMC/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 CMMC/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. These vulnerabilities are significant: phishing attacks are the most common method used by cybercriminals to steal passwords, gain unauthorized access, and engage in malicious activities. When an encrypted email and file sharing service is added to complement (instead of replace) regular email and files, access can be restricted to only trusted individuals. These people form a "trusted community" that allows organizations to control the flow of CUI. Individuals outside the trusted community are blocked from sending or receiving encrypted information.

Controlled access addresses the following CMMC/NIST SP 800-171 control families: Configuration Management, Systems & Communications Protection, and Systems & Informational Integrity.

# How do I prepare my organization for CMMC?

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 is that no organization should wait until the new framework becomes law. Informed estimates from C3PAOs who have done this work are that it take will take typical small to medium-size organizations anywhere from 12-18 months to meet CMMC Level 2 requirements.

Understand, too, that DIBCAC audits will continue while the CMMC rulemaking process runs its course. The lowest-hanging fruit for DIBCAC is to simply check whether an organization has submitted its NIST SP 800-171 self-assessment score (aka SPRS score) as required; reports are that DIBCAC is steadily increasing such spot checks. And primes have begun to ask subcontractors not only if they have submitted an SPRS score, but also to meet a minimum required score.

Without question, any organization that doesn't have an SPRS score on file is sending a clear and problematic signal about its cybersecurity capabilities to both the DoD and contractors assessing potential subcontractors to work with.

And 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 self-assessment score (more on this below).

The Department of Justice 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. And 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 include severe penalties and steep fines. None of these activities is slowing down while CMMC 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 framework

With this paper you're already off to an excellent start on familiarizing yourself with the CMMC framework. Continue to stay abreast of developments by regularly checking the DoD's CMMC website and the Cyber AB's 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. The 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).

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," as described above (see page six). 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.

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

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

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.

All this said, the DoD currently is reviewing whether to bifurcate Level 2 assessment requirements as described here. See the note at the bottom of Figure 1 (on page six) for more information along these lines. But in any case, DIBCAC is advising organizations to prepare for CMMC Level 2 as if they will need to undergo third-party assessments. That's simply because 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.

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 and 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 guidance on the subject, CMMC Assessment Scope: Level 2, Version 2.0, makes clear that CUI enclaves will be acceptable in the new scoping regime.

If 100% of your organization's work is on DoD contracts and many of them involve CUI, then your best approach is to include your entire organization in scope for NIST SP 800-171 compliance. But 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.

## Adopt a platform to secure CUI

Meeting the 110 security controls of NIST SP 800-171—developed specifically to protect CUI—is a fundamental requirement for achieving CMMC Level 2 certification. The most heavily weighted of those 110 controls, at 5 points, are the ones that relate directly to securing CUI. Adopting a platform that allows your organization to securely store, process and transmit CUI is key to preparing for your required NIST SP 800-171 self-assessment. It makes sense to adopt the platform before the self-assessment so that your organization can achieve a better outcome and save time and money in the long run.

## Assess Cloud Service Provider options

If your organization has migrated to the cloud, standard commercial cloud services such as Microsoft 365 Commercial for storing, processing and transmitting CUI are not CMMC compliant. Remember that file sharing and email is how CUI is most frequently transmitted. If you are using a Microsoft platform, you will need to assess alternatives and confirm that they meet CMMC Level 2 requirements.

Specifically, cloud service providers (CSPs) should:

- Meet DFARS 252.204-7012 (c)-(g). Briefly, those requirements are:
  c) cyber incident reporting to the DoD Cyber Crimes Center (DC3)
  d) malicious software, if discovered, to be submitted to DC3
  e) media preservation and protection for 90 days
  f) provide DC3 access to additional information if requested
  g) assist DoD with cyber incident damage assessment if requested

Organizations should confirm and ask their CSP for documentation that it meets these requirements.

- Meet FedRAMP Moderate Baseline or Equivalency standards, or higher. FedRAMP stands for the Federal Risk and Authorization Management Program, and "Moderate Baseline" is an official certification within the FedRAMP program.[1] This means that contractors need to confirm that their CSP is either FedRAMP Baseline Moderate or that it can demonstrate Equivalency.

The Cyber AB's draft CMMC Assessment Process (CAP) specifies two criteria for the demonstration of Equivalency:

1) The OSC [Organization Seeking Certification] or the External Cloud Service Provider has provided a body of evidence documenting how the External Cloud Service Provider's security controls are equivalent to those provided by the FedRAMP Moderate Baseline standard; and

2) Said body of evidence has been attested to by an independent, credible, professional source.

Don't simply accept a CSP's self-attestation of Equivalency; instead ask for documented evidence that it meets the two CAP criteria above.

- If your CSP provides data encryption for CUI, a FIPS 140-2 validated cryptographic module must be used for that encryption.[2] Be sure to ask your CSP for its FIPS 140-2 certification as well.

Finally, it is important to know that responsibility for choosing a CMMC-compliant CSP rests squarely on the shoulders of defense contractors: The Cyber AB's CAP states that "Ultimately, the OSC [Organization Seeking Certification] is solely responsible for their relationship with any External Cloud Service Providers and how those cloud services…are meeting the requirements for CMMC certification."

1 FedRAMP is a General Services Administration (GSA) program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services

2 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.

## Identify partners to get the help you need

You needn't take on NIST SP 800-171 compliance and CMMC certification on your own. It's understandable that many organizations lack the necessary internal security expertise to achieve CMMC Level 2. And so, in the end, it may most efficient to bring in outside help at any point where you are uncertain or stuck. 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. They can assist you, for example, by helping with development of your SSP, updating and documenting policies and procedures, and conducting your required self-assessment, as well as with preparation for your outside assessment for CMMC Level 2 by a C3PAO and follow up as needed.

Most important, outside partners can help you save time and money by creating a smooth path to NIST SP 800-171 compliance and attainment of CMMC Level 2.

## Conduct a NIST SP 800-171 self-assessment

If your organization handles CUI, then you have a DFARS 7012 clause in your contract. DFARS 7012 obligates contractors to implement the 110 controls specified in NIST SP 800-171. But DFARS 7012 permits contractors to self-assess their cybersecurity levels and so compliance throughout the DIB has been weak. To ramp up compliance, in 2020 DoD released two new DFARS Interim Rule clauses—7019 and 7020. In 2022, these clauses were cemented into Final Rules. (See related sidebar.)

The first task you'll need to tackle is development of a System Security Plan (SSP) as required by NIST SP 800-171. Your SSP details the policies and procedures your organization has in place to comply with NIST SP 800-171's 110 security controls. The SSP serves as a foundational document for a NIST SP 800-171 self-assessment and is a prerequisite for consideration for any DoD contract.

### DFARS 7012, 7019 and 7020: The Basics

Any defense contractor that handles CUI has a DFARS 7012 clause in its contract.

**DFARS 7012 requires contractors to:**

Implement NIST SP 800-171, written to protect CUI

Comply with DFARS 7012 (c)-(g) on cyber incident reporting

Confirm their Cloud Service Provider (CSP) is at least FedRAMP Baseline Moderate or Equivalent

FedRAMP

Use FIPS 140-2 validated modules when data is encrypted

Flow down all these requirements to subcontractors

After you've developed your SSP, DFARS 7019 requires your organization to:

- Conduct an NIST SP 800-171 self-assessment according to the DoD's Assessment Methodology. All contractors that handle CUI must perform at least a Basic level self-assessment, as described in the methodology.
    - DoD methodology assigns each of the 110 NIST SP 800-171 controls a weight of one, three, or five points. Scoring starts at the lowest possible score of -203. One, three, or five points are earned for each control met, all the way up to the maximum of +110. Negative self-assessment scores are possible, as scores can range from -203 to +110, a spread of 313 points. The DoD requires that scores be reported at this summary level, rather than broken down by each NIST SP 800-171 control.
    - To assess whether a control has been met, the DoD methodology specifies objectives associated with each control. There are 320 objectives distributed across the 110 NIST SP 800-171 security controls. Every objective associated with a control must be met for that control to be satisfied. See Figure 2 on page 22 below for more details on how this works.
- Submit your self-assessment scores to the DoD's SPRS by the time of contract award. The self-assessment must have been completed within the last three years, and be maintained for the duration of the contract. This DoD document, SPRS Access for NIST SP 800-171, offers step-by-step instructions for submitting scores via the DoD's Procurement Integrated Enterprise Environment (PIEE).
- If your organization's self-assessment score falls below 110, you are required to create a POA&M for security controls not met, and indicate by what date those security gaps will be remediated and a score of 110 will be achieved.

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

**DFARS clauses 7019 and 7020 require defense contractors that handle CUI to also:**

Conduct a NIST SP 800-171 self-assessment according to DoD Assessment Methodology and submit the score to the DoD's Supplier Performance Risk System (SPRS)


Create a Plan of Actions & Milestones (POA&M) for the NIST SP 800-171 controls not yet met

Cooperate fully with DoD auditors should they choose to conduct a review of contractor's compliance


Flow down all these requirements to subcontractors

Contractors that meet these DFARS requirements are in an excellent position to achieve CMMC Level 2 because Level 2's security requirements will mirror NIST SP 800-171's controls.

to be part of a defense contract. DFARS 7019 doesn't specify minimum self-assessment scores that must be achieved, unlike CMMC, 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]

Lack of an SPRS score altogether is a breach of DFARS 7019 contractural requirements and severely jeopardizes your organization's eligibility to keep existing DoD contracts and win new ones. Prime contractors already have begun to formally request SPRS scores from their subcontractors, and some have specified minimum scores required to work with them. If you're a subcontractor, know that primes are increasingly wary of the risk of working with any subcontractor not in compliance with DoD cybersecurity mandates—and will quickly turn to those that are. Indeed, DFARS 7020 also requires primes to take responsibility for the security of their supply chains. And with the SPRS score, primes now have a single, objective metric to easily compare the cyber maturity of competing subcontractors.

Second and more important, there is no path to CMMC Level 2 certification without compliance with NIST SP 800-171.[4] In this environment, your organization's best course of action is to focus on complying with that standard now.

Finally, note too that in another effort to increase enforcement of federal cybersecurity regulations, CMMC 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 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.

## CMMC Level 2 requirements beyond NIST SP 800-171

Compliance with NIST SP 800-171 is fundamental to achieving CMMC Level 2. However, organizations will need to meet cybersecurity requirements beyond NIST SP 800-171 to achieve CMMC Level 2. Any organization that handles CUI also is subject to DFARS clauses 7012, 7019 and 7020. DFARS 7012 invokes not just its own (c)-(g) requirements for cyber incident reporting and

3 To learn more about increasing your NIST 800-171 self-assessment score, see PreVeil's briefs, NIST SP 800-171 Self-Assessment: Improving Cybersecurity and Raising Your SPRS Score and Case Study: Defense contractor achieves 110/110 score in NIST SP 800-171 DoD audit.

4 In May 2023, NIST released Revision 3 of NIST SP 800-171. That started a 60-day comment period, which will be followed by responses and changes based on input received. Revision 3 isn't expected to be released for at least a year, and so organizations are best advised to focus on complying with NIST SP 800-171 as it stands today (i.e., Revision 2).

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.

## Notes regarding costs

The DoD indicated early on that the costs of achieving CMMC certification will be allowable, meaning that they could be built into organizations' bids for defense contracts. Your organization will need to incur the costs up front, though, and will recoup those costs from the DoD only if you win a contract. Note too that the DFARS Interim Rule published in September 2020 had this to say about the costs of CMMC certification at that point in the program's evolution (when the DoD had added 23 security requirements on top of NIST SP 800-171's 110 requirements): "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)."[5]

That is to say, at that point the DoD was assuming that defense contractors handling CUI were already in compliance with NIST SP 800-171, and therefore any additional, allowable "engineering" costs for achieving the new CMMC Level 2 certification would be minimal.

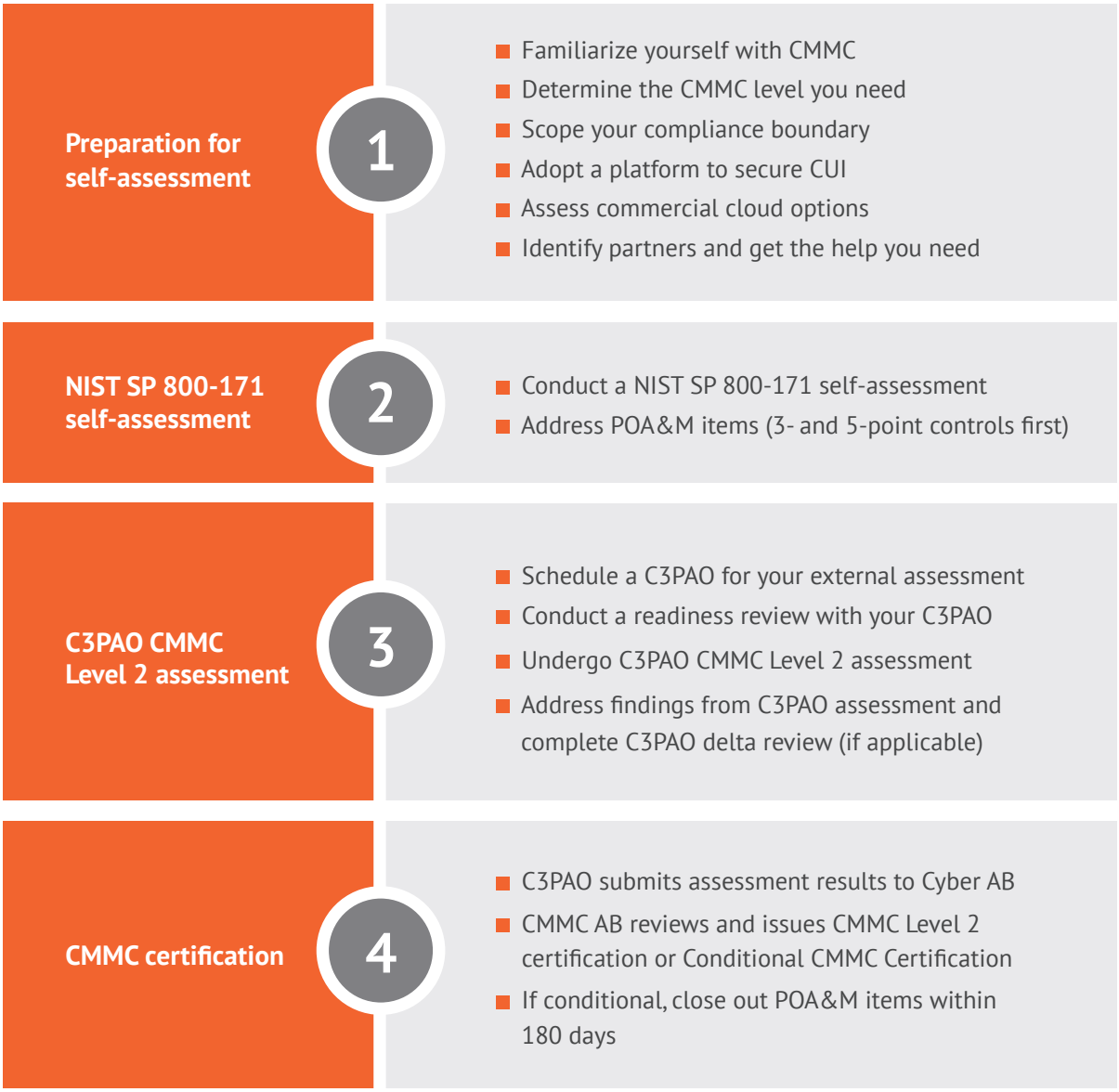
The extent to which DoD will consider the costs of CMMC certification to be allowable—including costs beyond those associated with compliance with NIST SP 800-171—is unknown at this point. As part of the rulemaking process, DoD is required to publish a comprehensive cost analysis associated with each CMMC level, which should shed more light on what organizations in the DIB should expect and plan for.

In the meantime, to help you project and plan for costs, Figure 2 summarizes the steps described above on how to prepare for CMMC, and adds more detail on moving from your NIST SP 800-171 self-assessment to CMMC Level 2 certification (see next page). As noted in the figure, costs for each step will vary widely across organizations.

All organizations—particularly small businesses that derive a small proportion of revenue from DoD contracts—should weigh their own estimated costs of CMMC Level 2 certification against the projected revenue from DoD contracts that certification will enable. Take a long-term perspective for this analysis: Upfront CMMC-related costs most likely will be significantly higher than ongoing costs, and the inability to do work for DoD over the long term could present a serious business risk for your organization. Consider, too, that technology solutions that reduce the time and costs to achieve CMMC certification are available.

5 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.

**Figure 2: Steps to CMMC Level 2 certification & note regarding costs**




***Costs associated with each step will vary across organizations.*** Variables include current cybersecurity level, scope of CUI enclave, number of employees that handle CUI, how much preparation organizations can do on their own for their C3PAO assessment, and how much outside expertise will be needed to achieve CMMC Level 2 certification.

# PreVeil Product Overview

PreVeil's file sharing and email platform adheres to each of the fundamental cybersecurity principles outlined above, beginning with he gold standard of end-to-end encryption. PreVeil's encrypted Drive and Email support compliance with virtually all the CMMC Level 2 mandates related to the communication and storage of CUI. In contrast, most widely- deployed commercial systems used to store, process and transmit 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 Level 2 security controls will mirror NIST SP 800-171's security controls.

For more details, Appendix A presents a comprehensive matrix that lists each CMMC Level 2 practice and corresponding NIST SP 800-171 security controls and objectives, and indicates which requirements PreVeil helps to meet.

## 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 listed as having trusted addresses and domains and appropriate access permissions.

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.

***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.

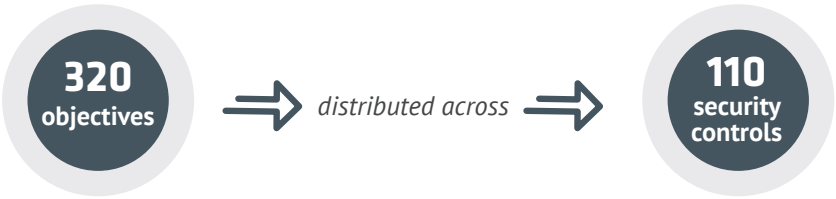
PreVeil integrates with mail clients such as Outlook, Gmail, and Apple Mail, and also works on browsers and mobile devices. When PreVeil Email is used with Outlook, Gmail, or Apple Mail, the installation process automatically creates a new set of mailboxes for your encrypted messages. Messages in these 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

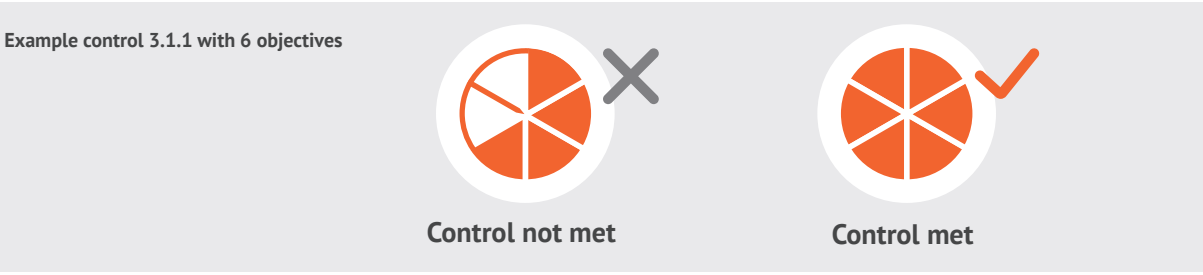
PreVeil supports compliance with virtually all CMMC Level 2 requirements for storing, processing and transmitting CUI. This includes 260 of the 320 assessment objectives specified in NIST SP 800-171A and 102 of the 110 NIST SP 800-171 security controls, as shown in Figure 3.

**Figure 3: NIST SP 800-171A assessment and how PreVeil helps**

NIST SP 800-171 assessors will review compliance with:




Each security control has anywhere from one to 15 objectives. Every *objective* associated with a *control* must be met for that control to be satisfied. For example:




**PreVeil supports**


**Including:**

***every objective*** for **37** controls

+

***shared responsibility*** for **65** controls

**Total = 102 controls**

PreVeil also supports CMMC Level 2 requirements that extend beyond NIST SP 800-171. PreVeil's additional key compliance attributes include:

- Meets FedRAMP Baseline Moderate Equivalent[6]
- Encrypts and stores data on FedRAMP High AWS GovCloud
- Meets DFARS 252.204-7012 (c)-(g), which stipulate requirements for cyber incident reporting[7]
- Meets the U.S. State Department's ITAR 120.54 standards for end-to-end encryption, wherein the cloud service provider has no access to keys, and the FIPS 140-2 validated cryptographic module is used[8]

As noted above, most widely-deployed commercial systems used to store, process and transmit CUI do not comply with these CMMC Level 2 requirements. That includes Microsoft 365 Commercial. Instead, Microsoft offers GCC High, 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 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 a burden 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.

**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 D for a complete list of PreVeil resources.**

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

6 The FedRAMP Baseline Moderate "Equivalent" category exists because only organizations that sell directly to the Federal government need to achieve FedRAMP Baseline Moderate status; cloud service providers that sell to other entities, such as defense contractors (and not directly to the government), need to achieve FedRAMP Baseline Moderate Equivalency. As the name implies, the standards are exactly the same across the two categories. See PreVeil's FedRAMP Story to learn more about how PreVeil achieved FedRAMP Baseline Moderate Equivalency.

7 See PreVeil's one-page Statement on DFARS 7012 (c)-(g), which specifies how PreVeil's information assurance compliance program meets each of the (c)-(g) requirements.

8 See PreVeil's FIPS 140-2 certificate on NIST's Computer Security Resource website here.

Google's standard Gmail platform also doesn't comply with CMMC Level 2 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.

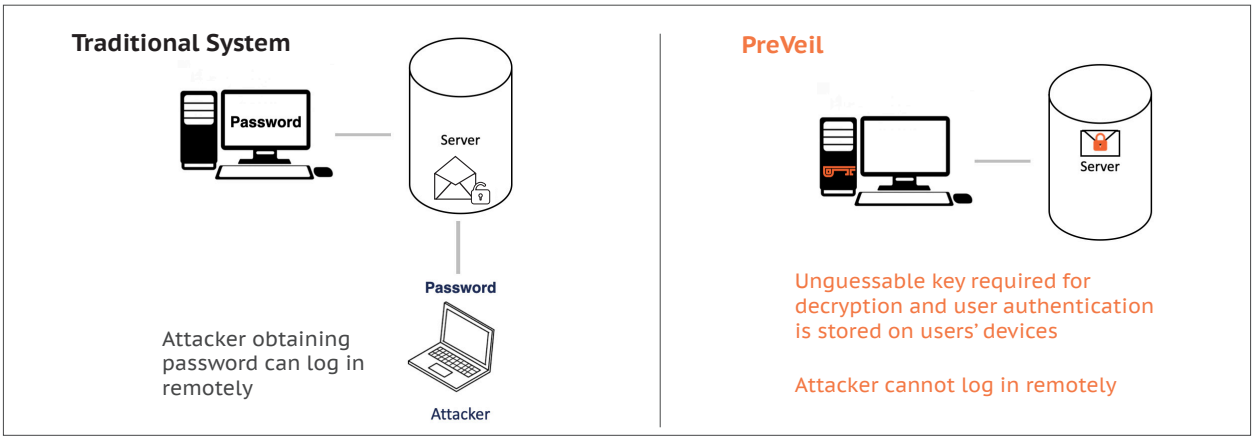
## PreVeil Security and Compliance Features

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 CMMC Level 2. Those features include:

### *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 4 below.

**Figure 4: PreVeil eliminates password vulnerabilities with keys**




### *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.

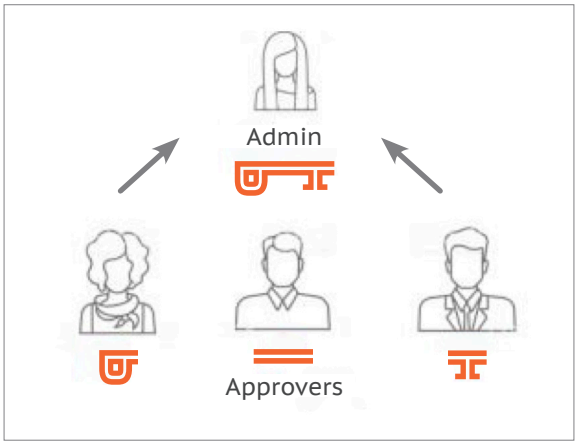
## *Approval Groups*

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 organization before accessing other users' information, as shown in Figure 5. Approval is a critical but seamless process.

## *Trusted Communities*

PreVeil Trusted Communities feature allows administrators to restrict communication to pre-approved domains and email addresses. This ensures that only members of a trusted community can exchange email and files, virtually eliminating phishing and spoofing attacks.

**Figure 5: PreVeil Approval Groups: Admin access to other users' data only with complete key**




## *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.

## *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 for storing, processing and transmitting 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. The ability to recover your information

is critical: There were more than 620 million ransomware attacks globally in 2021 and US businesses were the targets of nearly half of those attacks. Moreover, cybercriminals consider small to mid-size companies to be particularly easy targets and so focus much of their energy on them. To defend against ransomware, PreVeil saves every version of your data and files using 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 straightforward 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.

Further, the PreVeil Express platform allows individuals to create an account and take advantage of PreVeil's privacy and security without installing any software. Users simply create a free PreVeil Express account using their preferred browser, and in a matter of seconds they can send and receive secure files and email messages. PreVeil Express allows contractors to share CUI with individual partners with whom they need to communicate securely.

### *Cost effectiveness*

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

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

At this stage of the evolution of the CMMC program, the path to CMMC Level 2 certification has come into focus. PreVeil's unique three-step solution will streamline your organization's journey on that path, making it more efficient and affordable.

**Step One: Adopt a cloud platform to store, process and transmit 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 compliance documentation package and Governance, Risk and Compliance (GRC) tool.** To help defense contractors get essential documentation tasks done, PreVeil offers a comprehensive compliance documentation package to customers that deploy its platform. The package includes a System Security Plan (SSP) template that's based on NIST SP 800-171's 110 security controls—which CMMC Level 2's practices will mirror—and is prefilled to reflect PreVeil's capabilities and the security controls it supports, along with procedures relevant to those controls. To help complete the SSP, PreVeil's documentation package also includes policy templates for the CMMC Level 2/NIST SP 800-171 families, as well as templates for an internal responsibility matrix, a Customer Responsibility Matrix (CRM) specifying which controls and assessment objectives PreVeil supports, and a POA&M for showing how the controls and objectives that PreVeil doesn't support can be met.

Given the complexity of DoD compliance, PreVeil also offers its customers a GRC compliance assessment platform for keeping track of all their compliance documentation—a potentially overwhelming organizational task to undertake on your own. PreVeil's compliance templates described above flow into the GRC tool, which automatically assesses the documentation and produces several reports including, for example, which NIST SP 800-171 security controls have not yet been met, along with an accompanying POA&M report that helps you track progress toward closing your security gaps. Importantly, the platform also calculates your organization's Supplier Performance Risk System (SPRS) score, which the majority of organizations in the DIB are required to report to the DoD.

PreVeil's compliance documentation package gives your organization a considerable head start on its SSP and essential supporting documents—otherwise a daunting, time-consuming, and costly task. In combination with the GRC tool, these offerings will dramatically accelerate your journey to CMMC Level 2 compliance..

**Step Three: Leverage PreVeil's partner community.** Once you've taken the first step and deployed PreVeil Drive and Email, your organization will be well on its way toward NIST SP 800-171 compliance. And if you take advantage of PreVeil's documentation package and the GRC tool it offers, the documentation you need to demonstrate compliance will be in good order and you'll have your SPRS score too. But more remains to be accomplished: the goal is an SPRS score of 110, meaning that your organization meets the required 110 NIST SP 800-171 security controls for the protection of CUI, which mirror CMMC Level 2 controls.

Understandably, many organizations in the DIB lack the necessary in-house IT security and compliance expertise needed to achieve CMMC Level 2 on their own. Instead, for many small to

mid-size businesses, the most cost-effective approach is to hire outside consultants on a limited basis rather than keep cybersecurity and compliance experts on the payroll.

To facilitate connections to the specialized help you need, PreVeil has built a partner network of C3PAOs, Certified CMMC Assessors, Registered Practioners, MSPs (Managed Service Providers), and other consultants and organizations certified by the Cyber AB—all with expert knowledge of DFARS, NIST, CMMC and PreVeil (see Figure 6).

**Figure 6: PreVeil's partner community: An indispensable resource**


Your organization can leverage the PreVeil community by first arranging for a one-time engagement with a partner Registered Practitioner (RP) or Registered Practitioner Organization (RPO) that will steer you through upgrading your cybersecurity and the compliance documentation process. The goal of the RP/RPO engagement is to position your organization for a successful outside, third party assessment as required for CMMC Level 2 certification.

Once your organization is ready for a third-party assessment, you will need to engage a C3PAO to conduct it.[9] Note, however, that because CMMC hasn't been implemented yet, C3PAOs cannot conduct Level 2 assessments yet. They can, however, conduct Joint Surveillance Voluntary Assessments with DIBCAC as described above on page eight. In fact, the Cyber AB has indicated that such voluntary assessments will be converted into CMMC Level 2 assessments when CMMC is implemented, and the three-year clock for renewal of the assessment won't begin until then.

PreVeil offers coordinated access to its vetted and specialized partner community based on your needs. The partners' expert knowledge of PreVeil significantly streamlines your engagement because no time is spent learning how PreVeil supports compliance. This efficiency saves you money and smooths your organization's path to CMMC Level 2 certification.

In sum, if you are unfamiliar with what it takes to be DoD compliant, PreVeil can support your organization's journey to CMMC Level 2 certification every step of the way, from deployment of its DoD-compliant Drive and Email platform to compliance documentation and GRC assessment, to its partner community and audit responses as needed—all while saving you time, minimizing your risks, and reducing your costs.

9 DoD regulations require that different individuals and/or organizations serve as a defense contractor's RP/RPO and C3PAO so as to avoid the conflict of interest that would arise if they were to assess their own work.

# 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 to be implemented to improve cybersecurity in the Defense Industrial Base, and so 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, 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 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.

Moreover, PreVeil can support your organization's journey to CMMC Level 2 certification every step of the way, from deployment of its DoD-compliant Drive and Email platform to compliance documentation and GRC assessment, to audit responses as needed and more—all while saving you time, minimizing your risks, and reducing your costs.

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 CMMC Level 2 more affordably, please access the compliance resources listed in Appendix D. And if you'd like a free 15-minute consultation with our compliance team to answer your specific questions about CMMC, sign up here.

**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 Customer Responsibility Matrix (CRM)

PreVeil worked with a certified C3PAO to create its Customer Responsibility Matrix (CRM), showing how PreVeil supports the NIST 800-171/NIST 800-171A and CMMC Level 2 requirements. PreVeil supports 102 of the 110 NIST 800-171/CMMC Level 2 controls, and 260 of the 320 assessment objectives distributed across those 110 controls, as specified in NIST 800-171A.

The PreVeil CRM that follows shows how PreVeil supports these controls and assessment objectives by either allowing the customer to inherit the control or objective from PreVeil (with the assumption and understanding that the customer is ultimately responsible for its compliance documentation and evidence gathering), or by sharing the responsibility for the control or assessment objective with the customer. The PreVeil CRM also shows which assessment objectives are associated with each NIST 800-171 control.

# **PreVeil** Customer Responsibility Matrix
# Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**
The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.
PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.
**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| Access Control (AC) | AC.L1-3.1.1 | 3.1.1 | Control | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | Shared |
| Access Control (AC) | AC.L1-3.1.1(a) | 3.1.1(a) | Objective | Authorized users are identified | Shared |
| Access Control (AC) | AC.L1-3.1.1(b) | 3.1.1(b) | Objective | Processes acting on behalf of authorized users are identified | PreVeil Inherited |
| Access Control (AC) | AC.L1-3.1.1(c) | 3.1.1(c) | Objective | Devices (and other systems) authorized to connect to the system are identified | PreVeil Inherited |
| Access Control (AC) | AC.L1-3.1.1(d) | 3.1.1(d) | Objective | System access is limited to authorized users | Shared |
| Access Control (AC) | AC.L1-3.1.1(e) | 3.1.1(e) | Objective | System access is limited to processes acting on behalf of authorized users | PreVeil Inherited |
| Access Control (AC) | AC.L1-3.1.1(f) | 3.1.1(f) | Objective | System access is limited to authorized devices (including other systems) | Shared |
| Access Control (AC) | AC.L1-3.1.2 | 3.1.2 | Control | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | PreVeil Inherited |
| Access Control (AC) | AC.L1-3.1.2(a) | 3.1.2(a) | Objective | The types of transactions and functions that authorized users are permitted to execute are defined | PreVeil Inherited |
| Access Control (AC) | AC.L1-3.1.2(b) | 3.1.2(b) | Objective | System access is limited to the defined types of transactions and functions for authorized users | PreVeil Inherited |
| Access Control (AC) | AC.L1-3.1.20 | 3.1.20 | Control | Verify and control/limit connections to and use of external information systems. | Shared |
| Access Control (AC) | AC.L1-3.1.20(a) | 3.1.20(a) | Objective | Connections to external systems are identified | Shared |
| Access Control (AC) | AC.L1-3.1.20(b) | 3.1.20(b) | Objective | The use of external systems is identified | Shared |
| Access Control (AC) | AC.L1-3.1.20(c) | 3.1.20(c) | Objective | Connections to external systems are verified | Shared |
| Access Control (AC) | AC.L1-3.1.20(d) | 3.1.20(d) | Objective | The use of external systems is verified | Shared |
| Access Control (AC) | AC.L1-3.1.20(e) | 3.1.20(e) | Objective | Connections to external systems are controlled/limited | Shared |
| Access Control (AC) | AC.L1-3.1.20(f) | 3.1.20(f) | Objective | The use of external systems is controlled/limited | Shared |
| Access Control (AC) | AC.L1-3.1.22 | 3.1.22 | Control | Control information posted or processed on publicly accessible information systems. | Customer Responsibility |
| Access Control (AC) | AC.L1-3.1.22(a) | 3.1.22(a) | Objective | Individuals authorized to post or process information on publicly accessible systems are identified | Customer Responsibility |
| Access Control (AC) | AC.L1-3.1.22(b) | 3.1.22(b) | Objective | Procedures to ensure FCI is not posted or processed on publicly accessible systems are identified | Customer Responsibility |
| Access Control (AC) | AC.L1-3.1.22(c) | 3.1.22(c) | Objective | A review process is in place prior to posting of any content to publicly accessible systems | Customer Responsibility |
| Access Control (AC) | AC.L1-3.1.22(d) | 3.1.22(d) | Objective | Content on publicly accessible systems is reviewed to ensure that it does not include FCI | Customer Responsibility |
| Access Control (AC) | AC.L1-3.1.22(e) | 3.1.22(e) | Objective | Mechanisms are in place to remove and address improper posting of FCI | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.3 | 3.1.3 | Control | Control the flow of CUI in accordance with approved authorizations. | Shared |
| Access Control (AC) | AC.L2-3.1.3(a) | 3.1.3(a) | Objective | Information flow control policies are defined | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.3(b) | 3.1.3(b) | Objective | Methods and enforcement mechanisms for controlling the flow of CUI are defined | Shared |
| Access Control (AC) | AC.L2-3.1.3(c ) | 3.1.3(c ) | Objective | Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified; | Shared |
| Access Control (AC) | AC.L2-3.1.3(d) | 3.1.3(d) | Objective | Authorizations for controlling the flow of CUI are defined | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.3(e ) | 3.1.3(e ) | Objective | Approved authorizations for controlling the flow of CUI are enforced | Shared |
| Access Control (AC) | AC.L2-3.1.4 | 3.1.4 | Control | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | Shared |
| Access Control (AC) | AC.L2-3.1.4(a) | 3.1.4(a) | Objective | The duties of individuals requiring separation are defined | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.4(b) | 3.1.4(b) | Objective | Responsibilities for duties that require separation are assigned to separate individuals | Shared |
| Access Control (AC) | AC.L2-3.1.4(c) | 3.1.4(c) | Objective | Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals | Shared |
| Access Control (AC) | AC.L2-3.1.5 | 3.1.5 | Control | Employ principle of least privilege, including for specific security functions and privileged accounts. | Shared |
| Access Control (AC) | AC.L2-3.1.5(a) | 3.1.5(a) | Objective | Privileged accounts are identified | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.5(b) | 3.1.5(b) | Objective | Access to privileged accounts is authorized in accordance with the principle of least privilege | Shared |
| Access Control (AC) | AC.L2-3.1.5(c ) | 3.1.5(c ) | Objective | Security functions are identified | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.5(d) | 3.1.5(d) | Objective | Access to security functions is authorized in accordance with the principle of least privilege | Shared |
| Access Control (AC) | AC.L2-3.1.6 | 3.1.6 | Control | Use non-privileged accounts or roles when accessing nonsecurity functions. | Shared |
| Access Control (AC) | AC.L2-3.1.6(a) | 3.1.6(a) | Objective | Nonsecurity functions are identified | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.6(b) | 3.1.6(b) | Objective | Users are required to use non-privileged accounts or roles when accessing nonsecurity functions | Shared |
| Access Control (AC) | AC.L2-3.1.7 | 3.1.7 | Control | Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.7(a) | 3.1.7(a) | Objective | Privileged functions are defined | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.7(b) | 3.1.7(b) | Objective | Non-privileged users are defined | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.7(c) | 3.1.7(c) | Objective | Non-privileged users are prevented from executing privileged functions | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.7(d) | 3.1.7(d) | Objective | The execution of privileged functions is captured in audit logs | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.8 | 3.1.8 | Control | Limit unsuccessful logon attempts. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.8(a) | 3.1.8(a) | Objective | The means of limiting unsuccessful logon attempts is defined | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.8(b) | 3.1.8(b) | Objective | The defined means of limiting unsuccessful logon attempts is implemented | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.9 | 3.1.9 | Control | Provide privacy and security notices consistent with CUI rules. | Shared |
| Access Control (AC) | AC.L2-3.1.9(a) | 3.1.9(a) | Objective | Privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category | Shared |
| Access Control (AC) | AC.L2-3.1.9(b) | 3.1.9(b) | Objective | Privacy and security notices are displayed | Shared |
| Access Control (AC) | AC.L2-3.1.10 | 3.1.10 | Control | Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.10(a) | 3.1.10(a) | Objective | The period of inactivity after which the system initiates a session lock is defined | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.10(b) | 3.1.10(b) | Objective | Access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity; | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.10(c ) | 3.1.10(c ) | Objective | Previously visible information is concealed via a pattern-hiding display after the defined period of inactivity. | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.11 | 3.1.11 | Control | Terminate (automatically) user sessions after a defined condition. | Shared |
| Access Control (AC) | AC.L2-3.1.11(a) | 3.1.11(a) | Objective | Conditions requiring a user session to terminate are defined | Shared |
| Access Control (AC) | AC.L2-3.1.11(b) | 3.1.11(b) | Objective | A user session is automatically terminated after any of the defined conditions occur | Shared |
| Access Control (AC) | AC.L2-3.1.12 | 3.1.12 | Control | Monitor and control remote access sessions. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.12(a) | 3.1.12(a) | Objective | Remote access sessions are permitted | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.12(b) | 3.1.12(b) | Objective | The types of permitted remote access are identified | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.12(c ) | 3.1.12(c ) | Objective | Remote access sessions are controlled | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.12(d) | 3.1.12(d) | Objective | Remote access sessions are monitored | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.13 | 3.1.13 | Control | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.13(a) | 3.1.13(a) | Objective | Cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.13(b) | 3.1.13(b) | Objective | Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.14 | 3.1.14 | Control | Route remote access via managed access control points. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.14(a) | 3.1.14(a) | Objective | Managed access control points are identified and implemented | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.14(b) | 3.1.14(b) | Objective | Remote access is routed through managed network access control points | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.15 | 3.1.15 | Control | Authorize remote execution of privileged commands and remote access to security-relevant information. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.15(a) | 3.1.15(a) | Objective | Privileged commands authorized for remote execution are identified | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.15(b) | 3.1.15(b) | Objective | Security-relevant information authorized to be accessed remotely is identified | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.15(c ) | 3.1.15(c ) | Objective | The execution of the identified privileged commands via remote access is authorized | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.15(d) | 3.1.15(d) | Objective | Access to the identified security-relevant information via remote access is authorized | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.16 | 3.1.16 | Control | Authorize wireless access prior to allowing such connections. | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.16(a) | 3.1.16(a) | Objective | Wireless access points are identified | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.16(b) | 3.1.16(b) | Objective | Wireless access is authorized prior to allowing such connections | Customer Responsibility |

# **PreVeil** Customer Responsibility Matrix Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| Access Control (AC) | AC.L2-3.1.17 | 3.1.17 | Control | Protect wireless access using authentication and encryption. | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.17(a) | 3.1.17(a) | Objective | Wireless access to the system is protected using authentication | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.17(b) | 3.1.17(b) | Objective | Wireless access to the system is protected using encryption | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.18 | 3.1.18 | Control | Control connection of mobile devices. | Shared |
| Access Control (AC) | AC.L2-3.1.18(a) | 3.1.18(a) | Objective | Mobile devices that process, store, or transmit CUI are identified | Customer Responsibility |
| Access Control (AC) | AC.L2-3.1.18(b) | 3.1.18(b) | Objective | Mobile device connections are authorized | Shared |
| Access Control (AC) | AC.L2-3.1.18(c ) | 3.1.18(c ) | Objective | Mobile device connections are monitored and logged | Shared |
| Access Control (AC) | AC.L2-3.1.19 | 3.1.19 | Control | Encrypt CUI on mobile devices and mobile computing platforms. | Shared |
| Access Control (AC) | AC.L2-3.1.19(a) | 3.1.19(a) | Objective | Mobile devices and mobile computing platforms that process, store, or transmit CUI are identified | Shared |
| Access Control (AC) | AC.L2-3.1.19(b) | 3.1.19(b) | Objective | Encryption is employed to protect CUI on identified mobile devices and mobile computing platforms | PreVeil Inherited |
| Access Control (AC) | AC.L2-3.1.21 | 3.1.21 | Control | Limit use of portable storage devices on external systems. | Shared |
| Access Control (AC) | AC.L2-3.1.21(a) | 3.1.21(a) | Objective | The use of portable storage devices containing CUI on external systems is identified and documented | Shared |
| Access Control (AC) | AC.L2-3.1.21(b) | 3.1.21(b) | Objective | Limits on the use of portable storage devices containing CUI on external systems are defined | Shared |
| Access Control (AC) | AC.L2-3.1.21(c ) | 3.1.21(c ) | Objective | The use of portable storage devices containing CUI on external systems is limited as defined. | Shared |
| Awareness and Training (AT) | AT.L1-3.2.1 | 3.2.1 | Control | Ensure that managers, system 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. | Shared |
| Awareness and Training (AT) | AT.L1-3.2.1(a) | 3.2.1(a) | Objective | Security risks associated with organizational activities involving CUI are identified | Shared |
| Awareness and Training (AT) | AT.L1-3.2.1(b) | 3.2.1(b) | Objective | Policies, standards, and procedures related to the security of the system are identified | Customer Responsibility |
| Awareness and Training (AT) | AT.L1-3.2.1(c ) | 3.2.1(c ) | Objective | Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities | Shared |
| Awareness and Training (AT) | AT.L1-3.2.1(d) | 3.2.1(d) | Objective | Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system | Customer Responsibility |
| Awareness and Training (AT) | AT.L2-3.2.2 | 3.2.2 | Control | Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. | Shared |
| Awareness and Training (AT) | AT.L2-3.2.2(a) | 3.2.2(a) | Objective | Information security-related duties, roles, and responsibilities are defined | Shared |
| Awareness and Training (AT) | AT.L2-3.2.2(b) | 3.2.2(b) | Objective | Information security-related duties, roles, and responsibilities are assigned to designated personnel; | Customer Responsibility |
| Awareness and Training (AT) | AT.L2-3.2.2(c ) | 3.2.2(c ) | Objective | Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities | Shared |
| Awareness and Training (AT) | AT.L2-3.2.3 | 3.2.3 | Control | Provide security awareness training on recognizing and reporting potential indicators of insider threat. | Shared |
| Awareness and Training (AT) | AT.L2-3.2.3(a) | 3.2.3(a) | Objective | Potential indicators associated with insider threats are identified | Shared |
| Awareness and Training (AT) | AT.L2-3.2.3(b) | 3.2.3(b) | Objective | Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.1 | 3.3.1 | Control | Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.1(a) | 3.3.1(a) | Objective | Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.1(b) | 3.3.1(b) | Objective | The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.1(c ) | 3.3.1(c ) | Objective | Audit records are created (generated) | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.1(d) | 3.3.1(d) | Objective | Audit records, once created, contain the defined content | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.1(e ) | 3.3.1(e ) | Objective | Retention requirements for audit records are defined | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.1(f) | 3.3.1(f) | Objective | Audit records are retained as defined | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.2 | 3.3.2 | Control | Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.2(a) | 3.3.2(a) | Objective | The content of the audit records needed to support the ability to uniquely trace users to their actions is defined | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.2(b) | 3.3.2(b) | Objective | Audit records, once created, contain the defined content. | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.3 | 3.3.3 | Control | Review and update logged events. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.3(a) | 3.3.3(a) | Objective | A process for determining when to review logged events is defined | Customer Responsibility |
| Audit and Accountability (AU) | AU.L2-3.3.3(b) | 3.3.3(b) | Objective | Event types being logged are reviewed in accordance with the defined review process | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.3(c ) | 3.3.3(c ) | Objective | Event types being logged are updated based on the review. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.4 | 3.3.4 | Control | Alert in the event of an audit logging process failure. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.4(a) | 3.3.4(a) | Objective | Personnel or roles to be alerted in the event of an audit logging process failure are identified | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.4(b) | 3.3.4(b) | Objective | Types of audit logging process failures for which alert will be generated are defined | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.4(c ) | 3.3.4(c ) | Objective | Identified personnel or roles are alerted in the event of an audit logging process failure | Customer Responsibility |
| Audit and Accountability (AU) | AU.L2-3.3.5 | 3.3.5 | Control | Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.5(a) | 3.3.5(a) | Objective | Audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.5(b) | 3.3.5(b) | Objective | Defined audit record review, analysis, and reporting processes are correlated | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.6 | 3.3.6 | Control | Provide audit record reduction and report generation to support on-demand analysis and reporting. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.6(a) | 3.3.6(a) | Objective | An audit record reduction capability that supports on-demand analysis is provided | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.6(b) | 3.3.6(b) | Objective | A report generation capability that supports on-demand reporting is provided | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.7 | 3.3.7 | Control | Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.7(a) | 3.3.7(a) | Objective | Internal system clocks are used to generate time stamps for audit records | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.7(b) | 3.3.7(b) | Objective | An authoritative source with which to compare and synchronize internal system clocks is specified | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.7(c ) | 3.3.7(c ) | Objective | Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.8 | 3.3.8 | Control | Protect audit information and audit logging tools from unauthorized access, modification, and deletion. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.8(a) | 3.3.8(a) | Objective | Audit information is protected from unauthorized access | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.8(b) | 3.3.8(b) | Objective | Audit information is protected from unauthorized modification | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.8(c ) | 3.3.8(c ) | Objective | Audit information is protected from unauthorized deletion | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.8(d) | 3.3.8(d) | Objective | Audit logging tools are protected from unauthorized access | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.8(e ) | 3.3.8(e ) | Objective | Audit logging tools are protected from unauthorized modification | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.8(f) | 3.3.8(f ) | Objective | Audit logging tools are protected from unauthorized deletion | PreVeil Inherited |
| Audit and Accountability (AU) | AU.L2-3.3.9 | 3.3.9 | Control | Limit management of audit logging functionality to a subset of privileged users. | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.9(a) | 3.3.9(a) | Objective | A subset of privileged users granted access to manage audit logging functionality is defined | Shared |
| Audit and Accountability (AU) | AU.L2-3.3.9(b) | 3.3.9(b) | Objective | Management of audit logging functionality is limited to the defined subset of privileged users. | Shared |

# **PreVeil** Customer Responsibility Matrix
# Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| Configuration Management (CM) | CM.L2-3.4.1 | 3.4.1 | Control | Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | Shared |
| Configuration Management (CM) | CM.L2-3.4.1(a) | 3.4.1(a) | Objective | A baseline configuration is established | Shared |
| Configuration Management (CM) | CM.L2-3.4.1(b) | 3.4.1(b) | Objective | The baseline configuration includes hardware, software, firmware, and documentation | Shared |
| Configuration Management (CM) | CM.L2-3.4.1(c ) | 3.4.1(c ) | Objective | The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle | Shared |
| Configuration Management (CM) | CM.L2-3.4.1(d) | 3.4.1(d) | Objective | A system inventory is established | Shared |
| Configuration Management (CM) | CM.L2-3.4.1(e ) | 3.4.1(e ) | Objective | The system inventory includes hardware, software, firmware, and documentation | Shared |
| Configuration Management (CM) | CM.L2-3.4.1(f) | 3.4.1(f) | Objective | The inventory is maintained (reviewed and updated) throughout the system development life cycle | Shared |
| Configuration Management (CM) | CM.L2-3.4.2 | 3.4.2 | Control | Establish and enforce security configuration settings for information technology products employed in organizational systems. | Shared |
| Configuration Management (CM) | CM.L2-3.4.2(a) | 3.4.2(a) | Objective | Security configuration settings for information technology products employed in the system are established and included in the baseline configuration | Shared |
| Configuration Management (CM) | CM.L2-3.4.2(b) | 3.4.2(b) | Objective | Security configuration settings for information technology products employed in the system are enforced | Shared |
| Configuration Management (CM) | CM.L2-3.4.3 | 3.4.3 | Control | Track, review, approve, or disapprove, and log changes to organizational systems. | Shared |
| Configuration Management (CM) | CM.L2-3.4.3(a) | 3.4.3(a) | Objective | Changes to the system are tracked | Shared |
| Configuration Management (CM) | CM.L2-3.4.3(b) | 3.4.3(b) | Objective | Changes to the system are reviewed | Shared |
| Configuration Management (CM) | CM.L2-3.4.3(c ) | 3.4.3(c ) | Objective | Changes to the system are approved or disapproved | Shared |
| Configuration Management (CM) | CM.L2-3.4.3(d) | 3.4.3(d) | Objective | Changes to the system are logged | Shared |
| Configuration Management (CM) | CM.L2-3.4.4 | 3.4.4 | Control | Analyze the security impact of changes prior to implementation. | Shared |
| Configuration Management (CM) | CM.L2-3.4.4(a) | 3.4.4(a) | Objective | The security impact of changes to the system is analyzed prior to implementation | Shared |
| Configuration Management (CM) | CM.L2-3.4.5 | 3.4.5 | Control | Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. | Shared |
| Configuration Management (CM) | CM.L2-3.4.5(a) | 3.4.5(a) | Objective | Physical access restrictions associated with changes to the system are defined | PreVeil Inherited |
| Configuration Management (CM) | CM.L2-3.4.5(b) | 3.4.5(b) | Objective | Physical access restrictions associated with changes to the system are documented | PreVeil Inherited |
| Configuration Management (CM) | CM.L2-3.4.5(c ) | 3.4.5(c ) | Objective | Physical access restrictions associated with changes to the system are approved | PreVeil Inherited |
| Configuration Management (CM) | CM.L2-3.4.5(d) | 3.4.5(d) | Objective | Physical access restrictions associated with changes to the system are enforced | PreVeil Inherited |
| Configuration Management (CM) | CM.L2-3.4.5(e ) | 3.4.5(e ) | Objective | Logical access restrictions associated with changes to the system are defined | Shared |
| Configuration Management (CM) | CM.L2-3.4.5(f) | 3.4.5(f) | Objective | Logical access restrictions associated with changes to the system are documented | Shared |
| Configuration Management (CM) | CM.L2-3.4.5(g) | 3.4.5(g) | Objective | Logical access restrictions associated with changes to the system are approved | Shared |
| Configuration Management (CM) | CM.L2-3.4.5(h) | 3.4.5(h) | Objective | Logical access restrictions associated with changes to the system are enforced | Shared |
| Configuration Management (CM) | CM.L2-3.4.6 | 3.4.6 | Control | Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. | Shared |
| Configuration Management (CM) | CM.L2-3.4.6(a) | 3.4.6(a) | Objective | Essential system capabilities are defined based on the principle of least functionality | Shared |
| Configuration Management (CM) | CM.L2-3.4.6(b) | 3.4.6(b) | Objective | The system is configured to provide only the defined essential capabilities | PreVeil Inherited |
| Configuration Management (CM) | CM.L2-3.4.7 | 3.4.7 | Control | Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. | Shared |
| Configuration Management (CM) | CM.L2-3.4.7(a) | 3.4.7(a) | Objective | Essential programs are defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(b) | 3.4.7(b) | Objective | The use of nonessential programs is defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(c ) | 3.4.7(c ) | Objective | The use of nonessential programs is restricted, disabled, or prevented as defined | Shared |
| Configuration Management (CM) | CM.L2-3.4.7(d) | 3.4.7(d) | Objective | Essential functions are defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(e ) | 3.4.7(e ) | Objective | The use of nonessential functions is defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(f) | 3.4.7(f) | Objective | The use of nonessential functions is restricted, disabled, or prevented as defined | Shared |
| Configuration Management (CM) | CM.L2-3.4.7(g) | 3.4.7(g) | Objective | Essential ports are defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(h) | 3.4.7(h) | Objective | The use of nonessential ports is defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(i) | 3.4.7(i) | Objective | The use of nonessential ports is restricted, disabled, or prevented as defined | Shared |
| Configuration Management (CM) | CM.L2-3.4.7(j) | 3.4.7(j) | Objective | Essential protocols are defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(k) | 3.4.7(k) | Objective | The use of nonessential protocols is defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(l) | 3.4.7(l) | Objective | The use of nonessential protocols is restricted, disabled, or prevented as defined | Shared |
| Configuration Management (CM) | CM.L2-3.4.7(m) | 3.4.7(m) | Objective | Essential services are defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(n) | 3.4.7(n) | Objective | The use of nonessential services is defined | Customer Responsibility |
| Configuration Management (CM) | CM.L2-3.4.7(o) | 3.4.7(o) | Objective | The use of nonessential services is restricted, disabled, or prevented as defined | Shared |
| Configuration Management (CM) | CM.L2-3.4.8 | 3.4.8 | Control | Apply deny-by-exception (deny listing) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (allow listing) policy to allow the execution of authorized software. | Shared |
| Configuration Management (CM) | CM.L2-3.4.8(a) | 3.4.8(a) | Objective | A policy specifying whether allow-listing or deny-listing is to be implemented is specified | Shared |
| Configuration Management (CM) | CM.L2-3.4.8(b) | 3.4.8(b) | Objective | The software allowed to execute under allow-listing or denied use under deny-listing is specified | Shared |
| Configuration Management (CM) | CM.L2-3.4.8(c ) | 3.4.8(c ) | Objective | Allow-listing to allow the execution of authorized software or deny-listing to prevent the use of unauthorized software is implemented as specified | Shared |
| Configuration Management (CM) | CM.L2-3.4.9 | 3.4.9 | Control | Control and monitor user-installed software. | Shared |
| Configuration Management (CM) | CM.L2-3.4.9(a) | 3.4.9(a) | Objective | A policy for controlling the installation of software by users is established | Shared |
| Configuration Management (CM) | CM.L2-3.4.9(b) | 3.4.9(b) | Objective | Installation of software by users is controlled based on the established policy | Shared |
| Configuration Management (CM) | CM.L2-3.4.9(c ) | 3.4.9(c ) | Objective | Installation of software by users is monitored | Shared |
| Identification and Authentication (IA) | IA.L1-3.5.1 | 3.5.1 | Control | Identify information system users, processes acting on behalf of users, or devices. | Shared |
| Identification and Authentication (IA) | IA.L1-3.5.1(a) | 3.5.1(a) | Objective | System users are identified | Shared |
| Identification and Authentication (IA) | IA.L1-3.5.1(b) | 3.5.1(b) | Objective | Processes acting on behalf of users are identified | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L1-3.5.1(c ) | 3.5.1(c ) | Objective | Devices accessing the system are identified | Shared |
| Identification and Authentication (IA) | IA.L1-3.5.2 | 3.5.2 | Control | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L1-3.5.2(a) | 3.5.2(a) | Objective | The identity of each user is authenticated or verified as a prerequisite to system access | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L1-3.5.2(b) | 3.5.2(b) | Objective | The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L1-3.5.2(c ) | 3.5.2(c ) | Objective | The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L2-3.5.3 | 3.5.3 | Control | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.3(a) | 3.5.3(a) | Objective | Privileged accounts are identified | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L2-3.5.3(b) | 3.5.3(b) | Objective | Multifactor authentication is implemented for local access to privileged accounts | Customer Responsibility |
| Identification and Authentication (IA) | IA.L2-3.5.3(c ) | 3.5.3(c ) | Objective | Multifactor authentication is implemented for network access to privileged accounts | Customer Responsibility |
| Identification and Authentication (IA) | IA.L2-3.5.3(d) | 3.5.3(d) | Objective | Multifactor authentication is implemented for network access to non-privileged accounts | Customer Responsibility |
| Identification and Authentication (IA) | IA.L2-3.5.4 | 3.5.4 | Control | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. | PreVeil Inherited |
| Identification and Authentication (IA) | IA.L2-3.5.4(a) | 3.5.4(a) | Objective | Replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts | PreVeil Inherited |

# **PreVeil** Customer Responsibility Matrix
# Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| Identification and Authentication (IA) | IA.L2-3.5.5 | 3.5.5 | Control | Prevent the reuse of identifiers for a defined period. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.5(a) | 3.5.5(a) | Objective | A period within which identifiers cannot be reused is defined | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.5(b) | 3.5.5(b) | Objective | Reuse of identifiers is prevented within the defined period | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.6 | 3.5.6 | Control | Disable identifiers after a defined period of inactivity. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.6(a) | 3.5.6(a) | Objective | A period of inactivity after which an identifier is disabled is defined | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.6(b) | 3.5.6(b) | Objective | Identifiers are disabled after the defined period of inactivity | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.7 | 3.5.7 | Control | Enforce a minimum password complexity and change of characters when new passwords are created. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.7(a) | 3.5.7(a) | Objective | Password complexity requirements are defined | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.7(b) | 3.5.7(b) | Objective | Password change of character requirements are defined | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.7(c ) | 3.5.7(c ) | Objective | Minimum password complexity requirements as defined are enforced when new passwords are created | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.7(d) | 3.5.7(d) | Objective | Minimum password change of character requirements as defined are enforced when new passwords are created | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.8 | 3.5.8 | Control | Prohibit password reuse for a specified number of generations. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.8(a) | 3.5.8(a) | Objective | The number of generations during which a password cannot be reused is specified | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.8(b) | 3.5.8(b) | Objective | Reuse of passwords is prohibited during the specified number of generations | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.9 | 3.5.9 | Control | Allow temporary password use for system logons with an immediate change to a permanent password. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.9(a) | 3.5.9(a) | Objective | An immediate change to a permanent password is required when a temporary password is used for system logon | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.10 | 3.5.10 | Control | Store and transmit only cryptographically-protected passwords. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.10(a) | 3.5.10(a) | Objective | Passwords are cryptographically protected in storage | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.10(b) | 3.5.10(b) | Objective | Passwords are cryptographically protected in transit | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.11 | 3.5.11 | Control | Obscure feedback of authentication information. | Shared |
| Identification and Authentication (IA) | IA.L2-3.5.11(a) | 3.5.11(a) | Objective | Authentication information is obscured during the authentication process | Shared |
| Incident Response (IR) | IR.L2-3.6.1 | 3.6.1 | Control | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | Shared |
| Incident Response (IR) | IR.L2-3.6.1(a) | 3.6.1(a) | Objective | An operational incident-handling capability is established | Shared |
| Incident Response (IR) | IR.L2-3.6.1(b) | 3.6.1(b) | Objective | The operational incident-handling capability includes preparation | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.1(c ) | 3.6.1(c ) | Objective | The operational incident-handling capability includes detection | Shared |
| Incident Response (IR) | IR.L2-3.6.1(d) | 3.6.1(d) | Objective | The operational incident-handling capability includes analysis | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.1(e ) | 3.6.1(e ) | Objective | The operational incident-handling capability includes containment | Shared |
| Incident Response (IR) | IR.L2-3.6.1(f) | 3.6.1(f) | Objective | The operational incident-handling capability includes recovery | Shared |
| Incident Response (IR) | IR.L2-3.6.1(g) | 3.6.1(g) | Objective | The operational incident-handling capability includes user response activities | Shared |
| Incident Response (IR) | IR.L2-3.6.2 | 3.6.2 | Control | Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.2(a) | 3.6.2(a) | Objective | Incidents are tracked | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.2(b) | 3.6.2(b) | Objective | Incidents are documented | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.2(c ) | 3.6.2(c ) | Objective | Authorities to whom incidents are to be reported are identified | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.2(d) | 3.6.2(d) | Objective | Organizational officials to whom incidents are to be reported are identified | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.2(e ) | 3.6.2(e ) | Objective | Identified authorities are notified of incidents | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.2(f) | 3.6.2(f) | Objective | Identified organizational officials are notified of incidents | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.3 | 3.6.3 | Control | Test the organizational incident response capability. | Customer Responsibility |
| Incident Response (IR) | IR.L2-3.6.3(a) | 3.6.3(a) | Objective | The incident response capability is tested | Customer Responsibility |
| Maintenance (MA) | MA.L2-3.7.1 | 3.7.1 | Control | Perform maintenance on organizational systems. | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.1(a) | 3.7.1(a) | Objective | System maintenance is performed | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.2 | 3.7.2 | Control | Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.2(a) | 3.7.2(a) | Objective | Tools used to conduct system maintenance are controlled | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.2(b) | 3.7.2(b) | Objective | Techniques used to conduct system maintenance are controlled | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.2(c ) | 3.7.2(c ) | Objective | Mechanisms used to conduct system maintenance are controlled | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.2(d) | 3.7.2(d) | Objective | Personnel used to conduct system maintenance are controlled | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.3 | 3.7.3 | Control | Ensure equipment removed for off-site maintenance is sanitized of any CUI. | Shared |
| Maintenance (MA) | MA.L2-3.7.3(a) | 3.7.3(a) | Objective | Equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI | Shared |
| Maintenance (MA) | MA.L2-3.7.4 | 3.7.4 | Control | Check media containing diagnostic and test programs for malicious code before the media is used in organizational systems. | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.4(a) | 3.7.4(a) | Objective | Media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.5 | 3.7.5 | Control | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.5(a) | 3.7.5(a) | Objective | Multifactor authentication is used to establish nonlocal maintenance sessions via external network connections | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.5(b) | 3.7.5(b) | Objective | Nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.6 | 3.7.6 | Control | Supervise the maintenance activities of personnel without required access authorization. | PreVeil Inherited |
| Maintenance (MA) | MA.L2-3.7.6(a) | 3.7.6(a) | Objective | Maintenance personnel without required access authorization are supervised during maintenance activities. | PreVeil Inherited |
| Media Protection (MP) | MP.L1-3.8.3 | 3.8.3 | Control | Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. | Shared |
| Media Protection (MP) | MP.L1-3.8.3(a) | 3.8.3(a) | Objective | System media containing FCI is sanitized or destroyed before disposal | Shared |
| Media Protection (MP) | MP.L1-3.8.3(b) | 3.8.3(b) | Objective | System media containing FCI is sanitized before it is released for reuse | Shared |
| Media Protection (MP) | MP.L2-3.8.1 | 3.8.1 | Control | Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. | Shared |
| Media Protection (MP) | MP.L2-3.8.1(a) | 3.8.1(a) | Objective | Paper media containing CUI is physically controlled | Customer Responsibility |
| Media Protection (MP) | MP.L2-3.8.1(b) | 3.8.1(b) | Objective | Digital media containing CUI is physically controlled | Shared |
| Media Protection (MP) | MP.L2-3.8.1(c ) | 3.8.1(c ) | Objective | Paper media containing CUI is securely stored | Customer Responsibility |
| Media Protection (MP) | MP.L2-3.8.1(d) | 3.8.1(d) | Objective | Digital media containing CUI is securely stored | Shared |
| Media Protection (MP) | MP.L2-3.8.2 | 3.8.2 | Control | Limit access to CUI on system media to authorized users. | Shared |
| Media Protection (MP) | MP.L2-3.8.2(a) | 3.8.2(a) | Objective | Access to CUI on system media is limited to authorized users | Shared |
| Media Protection (MP) | MP.L2-3.8.4 | 3.8.4 | Control | Mark media with necessary CUI markings and distribution limitations. | Shared |
| Media Protection (MP) | MP.L2-3.8.4(a) | 3.8.4(a) | Objective | Media containing CUI is marked with applicable CUI markings | Shared |
| Media Protection (MP) | MP.L2-3.8.4(b) | 3.8.4(b) | Objective | Media containing CUI is marked with distribution limitations | Shared |

# **PreVeil** Customer Responsibility Matrix
# Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| Media Protection (MP) | MP.L2-3.8.5 | 3.8.5 | Control | Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. | Shared |
| Media Protection (MP) | MP.L2-3.8.5(a) | 3.8.5(a) | Objective | Access to media containing CUI is controlled | Shared |
| Media Protection (MP) | MP.L2-3.8.5(b) | 3.8.5(b) | Objective | Accountability for media containing CUI is maintained during transport outside of controlled areas | Shared |
| Media Protection (MP) | MP.L2-3.8.6 | 3.8.6 | Control | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. | Shared |
| Media Protection (MP) | MP.L2-3.8.6(a) | 3.8.6(a) | Objective | The confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical | Shared |
| Media Protection (MP) | MP.L2-3.8.7 | 3.8.7 | Control | Control the use of removable media on system components. | Shared |
| Media Protection (MP) | MP.L2-3.8.7(a) | 3.8.7(a) | Objective | The use of removable media on system components is controlled | Shared |
| Media Protection (MP) | MP.L2-3.8.8 | 3.8.8 | Control | Prohibit the use of portable storage devices when such devices have no identifiable owner. | Shared |
| Media Protection (MP) | MP.L2-3.8.8(a) | 3.8.8(a) | Objective | The use of portable storage devices is prohibited when such devices have no identifiable owner | Shared |
| Media Protection (MP) | MP.L2-3.8.9 | 3.8.9 | Control | Protect the confidentiality of backup CUI at storage locations. | Shared |
| Media Protection (MP) | MP.L2-3.8.9(a) | 3.8.9(a) | Objective | The confidentiality of backup CUI is protected at storage locations | Shared |
| Personnel Security (PS) | PS.L2-3.9.1 | 3.9.1 | Control | Screen individuals prior to authorizing access to organizational systems containing CUI. | Shared |
| Personnel Security (PS) | PS.L2-3.9.1(a) | 3.9.1(a) | Objective | Individuals are screened prior to authorizing access to organizational systems containing CUI | Shared |
| Personnel Security (PS) | PS.L2-3.9.2 | 3.9.2 | Control | Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. | Shared |
| Personnel Security (PS) | PS.L2-3.9.2(a) | 3.9.2(a) | Objective | A policy and/or process for terminating system access and any credentials coincident with personnel actions is established | Customer Responsibility |
| Personnel Security (PS) | PS.L2-3.9.2(b) | 3.9.2(b) | Objective | System access and credentials are terminated consistent with personnel actions such as termination or transfer | Shared |
| Personnel Security (PS) | PS.L2-3.9.2(c ) | 3.9.2(c ) | Objective | The system is protected during and after personnel transfer actions | Shared |
| Physical Protection (PE) | PE.L1-3.10.1 | 3.10.1 | Control | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.1(a) | 3.10.1(a) | Objective | Authorized individuals allowed physical access are identified | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.1(b) | 3.10.1(b) | Objective | Physical access to organizational systems is limited to authorized individuals | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.1(c ) | 3.10.1(c ) | Objective | Physical access to equipment is limited to authorized individuals | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.1(d) | 3.10.1(d) | Objective | Physical access to operating environments is limited to authorized individuals | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.3 | 3.10.3 | Control | Escort visitors and monitor visitor activity. | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.3(a) | 3.10.3(a) | Objective | Visitors are escorted | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.3(b) | 3.10.3(b) | Objective | Visitor activity is monitored | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.4 | 3.10.4 | Control | Maintain audit logs of physical access. | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.4(a) | 3.10.4(a) | Objective | Audit logs of physical access are maintained | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.5 | 3.10.5 | Control | Control and manage physical access devices. | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.5(a) | 3.10.5(a) | Objective | Physical access devices are identified | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.5(b) | 3.10.5(b) | Objective | Physical access devices are controlled | PreVeil Inherited |
| Physical Protection (PE) | PE.L1-3.10.5(c ) | 3.10.5(c ) | Objective | Physical access devices are managed | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.2 | 3.10.2 | Control | Protect and monitor the physical facility and support infrastructure for organizational systems. | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.2(a) | 3.10.2(a) | Objective | The physical facility where organizational systems reside is protected | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.2(b) | 3.10.2(b) | Objective | The support infrastructure for organizational systems is protected | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.2(c ) | 3.10.2(c ) | Objective | The physical facility where organizational systems reside is monitored | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.2(d) | 3.10.2(d) | Objective | The support infrastructure for organizational systems is monitored | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.6 | 3.10.6 | Control | Enforce safeguarding measures for CUI at alternate work sites. | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.6(a) | 3.10.6(a) | Objective | Safeguarding measures for CUI are defined for alternate work sites | PreVeil Inherited |
| Physical Protection (PE) | PE.L2-3.10.6(b) | 3.10.6(b) | Objective | Safeguarding measures for CUI are enforced for alternate work sites | PreVeil Inherited |
| Risk Assessment (RM) | RA.L2-3.11.1 | 3.11.1 | Control | 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. | Shared |
| Risk Assessment (RM) | RA.L2-3.11.1(a) | 3.11.1(a) | Objective | The frequency to assess risk to organizational operations, organizational assets, and individuals is defined | Shared |
| Risk Assessment (RM) | RA.L2-3.11.1(b) | 3.11.1(b) | Objective | Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency | Shared |
| Risk Assessment (RM) | RA.L2-3.11.2 | 3.11.2 | Control | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | Shared |
| Risk Assessment (RM) | RA.L2-3.11.2(a) | 3.11.2(a) | Objective | The frequency to scan for vulnerabilities in organizational systems and applications is defined | Shared |
| Risk Assessment (RM) | RA.L2-3.11.2(b) | 3.11.2(b) | Objective | Vulnerability scans are performed on organizational systems with the defined frequency | Shared |
| Risk Assessment (RM) | RA.L2-3.11.2(c ) | 3.11.2(c ) | Objective | Vulnerability scans are performed on applications with the defined frequency | Shared |
| Risk Assessment (RM) | RA.L2-3.11.2(d) | 3.11.2(d) | Objective | Vulnerability scans are performed on organizational systems when new vulnerabilities are identified | Shared |
| Risk Assessment (RM) | RA.L2-3.11.2(e ) | 3.11.2(e ) | Objective | Vulnerability scans are performed on applications when new vulnerabilities are identified | Shared |
| Risk Assessment (RM) | RA.L2-3.11.3 | 3.11.3 | Control | Remediate vulnerabilities in accordance with risk assessments. | Shared |
| Risk Assessment (RM) | RA.L2-3.11.3(a) | 3.11.3(a) | Objective | Vulnerabilities are identified | Shared |
| Risk Assessment (RM) | RA.L2-3.11.3(b) | 3.11.3(b) | Objective | Vulnerabilities are remediated in accordance with risk assessments | Shared |
| Security Assessment (CA) | CA.L2-3.12.1 | 3.12.1 | Control | Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. | Shared |
| Security Assessment (CA) | CA.L2-3.12.1(a) | 3.12.1(a) | Objective | The frequency of security control assessments is defined | Shared |
| Security Assessment (CA) | CA.L2-3.12.1(b) | 3.12.1(b) | Objective | Security controls are assessed with the defined frequency to determine if the controls are effective in their application | Shared |
| Security Assessment (CA) | CA.L2-3.12.2 | 3.12.2 | Control | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. | Shared |
| Security Assessment (CA) | CA.L2-3.12.2(a) | 3.12.2(a) | Objective | Deficiencies and vulnerabilities to be addressed by the plan of action are identified | Shared |
| Security Assessment (CA) | CA.L2-3.12.2(b) | 3.12.2(b) | Objective | A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities | Shared |
| Security Assessment (CA) | CA.L2-3.12.2(c ) | 3.12.2(c ) | Objective | The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities | Shared |
| Security Assessment (CA) | CA.L2-3.12.3 | 3.12.3 | Control | Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. | Shared |
| Security Assessment (CA) | CA.L2-3.12.3(a) | 3.12.3(a) | Objective | Security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls | Shared |
| Security Assessment (CA) | CA.L2-3.12.4 | 3.12.4 | Control | 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. | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(a) | 3.12.4(a) | Objective | A system security plan is developed | Customer Responsibility |

**PreVeil** Customer Responsibility Matrix
Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**
The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.
PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.
**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| Security Assessment (CA) | CA.L2-3.12.4(b) | 3.12.4(b) | Objective | The system boundary is described and documented in the system security plan | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(c ) | 3.12.4(c ) | Objective | The system environment of operation is described and documented in the system security plan | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(d) | 3.12.4(d) | Objective | The security requirements identified and approved by the designated authority as non-applicable are identified; | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(e ) | 3.12.4(e ) | Objective | The method of security requirement implementation is described and documented in the system security plan | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(f) | 3.12.4(f) | Objective | The relationship with or connection to other systems is described and documented in the system security plan | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(g) | 3.12.4(g) | Objective | The frequency to update the system security plan is defined | Customer Responsibility |
| Security Assessment (CA) | CA.L2-3.12.4(h) | 3.12.4(h) | Objective | System security plan is updated with the defined frequency | Customer Responsibility |
| System and Communications Protection (SC) | SC.L1-3.13.1 | 3.13.1 | Control | 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. | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.1(a) | 3.13.1(a) | Objective | The external system boundary is defined | Customer Responsibility |
| System and Communications Protection (SC) | SC.L1-3.13.1(b) | 3.13.1(b) | Objective | Key internal system boundaries are defined | Customer Responsibility |
| System and Communications Protection (SC) | SC.L1-3.13.1(c ) | 3.13.1(c ) | Objective | Communications are monitored at the external system boundary | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.1(d) | 3.13.1(d) | Objective | Communications are monitored at key internal boundaries | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.1(e ) | 3.13.1(e ) | Objective | Communications are controlled at the external system boundary | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.1(f) | 3.13.1(f) | Objective | Communications are controlled at key internal boundaries | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.1(g) | 3.13.1(g) | Objective | Communications are protected at the external system boundary | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.1(h) | 3.13.1(h) | Objective | Communications are protected at key internal boundaries | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.5 | 3.13.5 | Control | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | Shared |
| System and Communications Protection (SC) | SC.L1-3.13.5(a) | 3.13.5(a) | Objective | Publicly accessible system components are identified | Customer Responsibility |
| System and Communications Protection (SC) | SC.L1-3.13.5(b) | 3.13.5(b) | Objective | Subnetworks for publicly accessible system components are physically or logically separated from internal networks | Shared |
| System and Communications Protection (SC) | SC.L2-3.13.2 | 3.13.2 | Control | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.2(a) | 3.13.2(a) | Objective | Architectural designs that promote effective information security are identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.2(b) | 3.13.2(b) | Objective | Software development techniques that promote effective information security are identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.2(c ) | 3.13.2(c ) | Objective | Systems engineering principles that promote effective information security are identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.2(d) | 3.13.2(d) | Objective | Identified architectural designs that promote effective information security are employed | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.2(e ) | 3.13.2(e ) | Objective | Identified software development techniques that promote effective information security are employed | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.2(f) | 3.13.2(f) | Objective | Identified systems engineering principles that promote effective information security are employed | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.3 | 3.13.3 | Control | Separate user functionality from system management functionality. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.3(a) | 3.13.3(a) | Objective | User functionality is identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.3(b) | 3.13.3(b) | Objective | System management functionality is identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.3(c ) | 3.13.3(c ) | Objective | User functionality is separated from system management functionality | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.4 | 3.13.4 | Control | Prevent unauthorized and unintended information transfer via shared system resources. | Shared |
| System and Communications Protection (SC) | SC.L2-3.13.4(a) | 3.13.4(a) | Objective | Unauthorized and unintended information transfer via shared system resources is prevented. | Shared |
| System and Communications Protection (SC) | SC.L2-3.13.6 | 3.13.6 | Control | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | Shared |
| System and Communications Protection (SC) | SC.L2-3.13.6(a) | 3.13.6(a) | Objective | Network communications traffic is denied by default | Shared |
| System and Communications Protection (SC) | SC.L2-3.13.6(b) | 3.13.6(b) | Objective | Network communications traffic is allowed by exception | Shared |
| System and Communications Protection (SC) | SC.L2-3.13.7 | 3.13.7 | Control | 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). | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.7(a) | 3.13.7(a) | Objective | Remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling). | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.8 | 3.13.8 | Control | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.8(a) | 3.13.8(a) | Objective | Cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.8(b) | 3.13.8(b) | Objective | Alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.8(c ) | 3.13.8(c ) | Objective | Either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.9 | 3.13.9 | Control | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.9(a) | 3.13.9(a) | Objective | A period of inactivity to terminate network connections associated with communications sessions is defined | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.9(b) | 3.13.9(b) | Objective | Network connections associated with communications sessions are terminated at the end of the sessions | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.9(c ) | 3.13.9(c ) | Objective | Network connections associated with communications sessions are terminated after the defined period of inactivity | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.10 | 3.13.10 | Control | Establish and manage cryptographic keys for cryptography employed in organizational systems. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.10(a) | 3.13.10(a) | Objective | Cryptographic keys are established whenever cryptography is employed | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.10(b) | 3.13.10(b) | Objective | Cryptographic keys are managed whenever cryptography is employed | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.11 | 3.13.11 | Control | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.11(a) | 3.13.11(a) | Objective | FIPS-validated cryptography is employed to protect the confidentiality of CUI | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.12 | 3.13.12 | Control | Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. | Customer Responsibility |
| System and Communications Protection (SC) | SC.L2-3.13.12(a) | 3.13.12(a) | Objective | Collaborative computing devices are identified | Customer Responsibility |
| System and Communications Protection (SC) | SC.L2-3.13.12(b) | 3.13.12(b) | Objective | Collaborative computing devices provide indication to users of devices in use | Customer Responsibility |
| System and Communications Protection (SC) | SC.L2-3.13.12(c ) | 3.13.12(c ) | Objective | Remote activation of collaborative computing devices is prohibited | Customer Responsibility |
| System and Communications Protection (SC) | SC.L2-3.13.13 | 3.13.13 | Control | Control and monitor the use of mobile code. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.13(a) | 3.13.13(a) | Objective | Use of mobile code is controlled | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.13(b) | 3.13.13(b) | Objective | Use of mobile code is monitored | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.14 | 3.13.14 | Control | Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. | Customer Responsibility |
| System and Communications Protection (SC) | SC.L2-3.13.14(a) | 3.13.14(a) | Objective | Use of Voice over Internet Protocol (VoIP) technologies is controlled | Customer Responsibility |
| System and Communications Protection (SC) | SC.L2-3.13.14(b) | 3.13.14(b) | Objective | Use of Voice over Internet Protocol (VoIP) technologies is monitored. | Customer Responsibility |

**PreVeil** Customer Responsibility Matrix
Controls and Objectives

**PREVEIL PROPRIETARY**

**Assumption: All CUI data will be transmitted and stored using PreVeil, only.**

The customer is responsible for determining which controls are applicable, and for developing and maintaining the customer SSP as well as policies, procedures, and supplemental documentation required for compliance related to assessments and audits.

PreVeil claims no responsibility or liability regarding customers information, effort, and execution of their compliance related tasks.

**NOTE:** The responses contained within this document are specific to PreVeil and the customer's instance of PreVeil. This document does not address any other systems or endpoints that may be considered in scope for a PreVeil customer's assessment.

Control/Objectives Status Legend

| | |
|---|---|
| Shared | In addition to the customer responsibilities listed in the assumptions and notes statements above, there will be some customer responsibility within the control/objective. This can include, but not limited to, additional documentation, end point management activities, application/system scanning, administrative management activities, asset management, etc. PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |
| PreVeil Inherited | As long as all assumptions and notes above are understood and addressed, PreVeil addresses the control/objective. Note: the customer may still have outstanding responsibilities, based on their internal business processes, technology infrastructure, CUI/FCI handling processes, and/or end point management activities (i.e., ensuring Bitlocker or other hard drive encryption methods are used for any laptop/desktop processing, transmitting, and/or storing CUI). PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information as to how PreVeil manages controls marked in this way for PreVeil customers. |
| Customer Responsibility | The customer will be reponsible for the objective/control marked "Customer Responsibility". PreVeil's SSP template, POA&M documentation, and Assessment Version of the CRM add additional information, suggestions, and examples of addressing these controls and objectives marked this way. |

| Practice Area | CMMC Practice | NIST SP 800-171 | Objective/Control | Practice Statement/Objective | Control/Objective Status |
|---|---|---|---|---|---|
| System and Communications Protection (SC) | SC.L2-3.13.15 | 3.13.15 | Control | Protect the authenticity of communications sessions. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.15(a) | 3.13.15(a) | Objective | The authenticity of communications sessions is protected. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.16 | 3.13.16 | Control | Protect the confidentiality of CUI at rest. | PreVeil Inherited |
| System and Communications Protection (SC) | SC.L2-3.13.16(a) | 3.13.16(a) | Objective | The confidentiality of CUI at rest is protected | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1 | 3.14.1 | Control | Identify, report, and correct information and information system flaws in a timely manner. | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1(a) | 3.14.1(a) | Objective | The time within which to identify system flaws is specified | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1(b) | 3.14.1(b) | Objective | System flaws are identified within the specified time frame | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1(c ) | 3.14.1(c ) | Objective | The time within which to report system flaws is specified | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1(d) | 3.14.1(d) | Objective | System flaws are reported within the specified time frame | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1(e ) | 3.14.1(e ) | Objective | The time within which to correct system flaws is specified | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.1(f) | 3.14.1(f) | Objective | System flaws are corrected within the specified time frame | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.2 | 3.14.2 | Control | Provide protection from malicious code at appropriate locations within organizational information systems. | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.2(a) | 3.14.2(a) | Objective | Designated locations for malicious code protection are identified | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.2(b) | 3.14.2(b) | Objective | Protection from malicious code at designated locations is provided | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.4 | 3.14.4 | Control | Update malicious code protection mechanisms when new releases are available. | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.4(a) | 3.14.4(a) | Objective | Malicious code protection mechanisms are updated when new releases are available | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.5 | 3.14.5 | Control | Perform periodic scans of the information system and real- time scans of files from external sources as files are downloaded, opened, or executed. | Shared |
| System and Information Integrity (SI) | SI.L1-3.14.5(a) | 3.14.5(a) | Objective | The frequency for malicious code scans is defined | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.5(b) | 3.14.5(b) | Objective | Malicious code scans are performed with the defined frequency | PreVeil Inherited |
| System and Information Integrity (SI) | SI.L1-3.14.5(c ) | 3.14.5(c ) | Objective | Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.3 | 3.14.3 | Control | Monitor system security alerts and advisories and take action in response. | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.3(a) | 3.14.3(a) | Objective | Response actions to system security alerts and advisories are identified | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.3(b) | 3.14.3(b) | Objective | System security alerts and advisories are monitored | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.3(c ) | 3.14.3(c ) | Objective | Actions in response to system security alerts and advisories are taken | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.6 | 3.14.6 | Control | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.6(a) | 3.14.6(a) | Objective | The system is monitored to detect attacks and indicators of potential attacks | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.6(b) | 3.14.6(b) | Objective | Inbound communications traffic is monitored to detect attacks and indicators of potential attacks | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.6(c ) | 3.14.6(c ) | Objective | Outbound communications traffic is monitored to detect attacks and indicators of potential attacks | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.7 | 3.14.7 | Control | Identify unauthorized use of organizational systems | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.7(a) | 3.14.7(a) | Objective | Authorized use of the system is defined | Shared |
| System and Information Integrity (SI) | SI.L2-3.14.7(b) | 3.14.7(b) | Objective | Unauthorized use of the system is identified | Shared |

| | |
|---|---|
| Total Controls Inherited by PreVeil (PreVeil Inherited) | 37 |
| Total Controls supported by PreVeil with Customer Responsibilities (Shared) | 65 |
| Total Controls not supported by PreVeil with Customer Responsibilities (Customer Responsibility) | 8 |
| Total number of Controls | 110 |

| | |
|---|---|
| Total Objectives Inherited by PreVeil (PreVeil Inherited) | 113 |
| Total Objectives supported by PreVeil with Customer Responsibilities (Shared) | 147 |
| Total Objectives not supported by PreVeil with Customer Responsibilities (Customer Responsibility) | 60 |
| Total number of Controls | 320 |

| | |
|---|---|
| Total Controls and Objectives Inherited by PreVeil (PreVeil Inherited) | 150 |
| Total Controls and Objectives supported by PreVeil with Customer Responsibilities (Shared) | 212 |
| Total Controls and Objectives not supported by PreVeil with Customer Responsibilities (Customer Responsibility) | 68 |
| Total number of Controls and Objectives | 430 |

## Appendix B: Case Study—How a contractor using PreVeil achieved the highest possible NIST SP 800-171 audit score

PreVeil can help your organization comply with NIST SP 800-171, as illustrated by an actual case study of how a small defense contractor achieved a score of 110 out of 110 on a NIST SP 800-171 DIBCAC audit.

In early 2021, a team of seven DIBCAC auditors undertook a rigorous audit of a small defense contractor that we'll call DIBCo, with fewer 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 as an overlay to its existing O365 Commercial system for 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.

DIBCo initially achieved a near-maximum score on its DIBCAC audit, meeting 109 of the 110 NIST SP 800-171 controls and creating a POA&M for the one outstanding control. DIBCo pursued implementation of that final control and within a few months DIBCAC verified they had met it.

As a result, DIBCo received the highest possible NIST SP 800-171 score of 110 out of 110.

DIBCo's impressive score clearly enhances their competitive standing in the DIB by placing them along-side 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.

The key to the contractor's success was PreVeil's advanced technology that enabled protection of their CUI. Without it, the contractor's NIST SP 800-171 score would have been significantly lower. With PreVeil, if CMMC had been in effect, the contractor likely would have been deemed to have met the new Level 2 requirements.

PreVeil also helped DIBCo meet compliance requirements beyond NIST SP 800-171, which flow from the fact that defense contractors that handle CUI are 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 protect CUI. PreVeil meets all of these requirements, as noted above, unlike Microsoft 365 Commercial.

Finally, PreVeil 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 file sharing and email platform. 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: Defense contractor achieves 110/110 score in NIST SP 800-171 DoD 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, *NIST SP 800-171 Self-Assessment: Improving Cybersecurity and Raising Your SPRS Score*.

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

## Appendix C: PreVeil vs. Alternatives

The Department of Defense requires organizations that store, process or transmit CUI to meet the requirements for CMMC 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 CMMC Level 2 requirements related to storing, processing and transmitting 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 may be a 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 may be 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 large 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 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.[1]

- PreVeil uses end-to-end encryption so that only senders and recipients of files and emails can see the data; PreVeil servers operate only with encrypted data and can never access the decryption keys. Conversely, both Microsoft GCC High and Box for Government offer an option to enhance the encryption they offer, but that's done via a centralized key server, whereby client information is encrypted/decrypted on the server using keys stored on another server. This scheme is vulnerable 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 enhanced encryption uses key server (a central point of attack) | Optional enhanced encryption uses key server (a 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** | $32/user/month | $$$$ | $$$$ |

1 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 D: PreVeil CMMC, DFARS, NIST and ITAR compliance resources

- *Case Study: Defense contractor achieves 110/110 in NIST SP 800-171 DoD audit.* A defense contractor using PreVeil as an overlay to its existing O365 Commercial system for all its users handling CUI achieved the highest possible score of 110 on a NIST SP 800-171 DIBCAC audit. This case study explains how the contractor got it done.
- *NIST SP 800-171 Self-Assessment: Improving Cybersecurity and Raising Your SPRS Score.* DFARS 252.204-7019 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 more than 125 points.
- *PreVeil Update: DoD to Ramp Up Enforcement of Compliance with NIST SP 800-171*. The DoD cemented clauses 7019 and 7020 of its 2020 DFARS Interim Rule into a Final Rule in December 2022. With this action, DoD clearly signaled its intent to enforce defense contractors' compliance with NIST SP 800-171.
- *PreVeil Update: Cyber AB Enables Voluntary Assessments with Release of Draft CMMC Assessment Process (CAP).* In July 2022, the Cyber Accreditation Board (Cyber AB) released its draft CMMC Assessment Process (aka CAP). The release of the CAP meant that voluntary third-party NIST SP 800-171 assessments could begin.
- *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 800-171equirements to protect federal student aid data. This brief outlines steps for universities to take now to achieve compliance.
- *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.
- *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.
- *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.

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

# About PreVeil

PreVeil makes military-grade security accessible to everyone. Its encrypted Drive and Email platform helps organizations improve their cybersecurity, reduce their compliance burdens, and achieve 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. Because it works with your existing tools, PreVeil is easy to implement and use. All documents and messages are automatically encrypted end-to-end, which eliminates central points of attack and means that no one other than intended recipients can read or scan your sensitive information—not even PreVeil.

More than 750 companies in the Defense Industrial Base trust PreVeil for their cybersecurity needs. Visit **www.preveil.com** to learn more.

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

PREVEIL

June 2023 v14