PREVEIL

Guide to Achieving CMMC Compliance: A Proven Path to 110

Table of Contents

Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) program is moving toward full enforcement and is already being included in contract solicitations. **48 CFR** left the Office of Management and Budget (OMB) on August 28, 2025, with expected publication in October 2025.This new requirement will authorize contracting officers to add CMMC clauses to Department of Defense (DoD) contracts via DFARS 252.204-7021. Together with the CMMC Final Rule **(32 CFR)**, effective in December 2024, these rules complete the CMMC regulatory framework — defining both the requirements and how they will be enforced through contracts.

DoD created the CMMC program to defend the vast attack surface of the Defense Industrial Base (DIB). One of DoD's top goals for CMMC is to better protect Controlled Unclassified Information (CUI), a prime target for cybercriminals and adversaries. Currently, if your organization handles CUI, you have a DFARS 252.204-7012 clause in your contract that requires you to comply with NIST SP 800-171. That's been mandated since 2017, but self-assessment has been permitted and compliance has been weak. That will change under the CMMC framework, which establishes mechanisms to verify compliance with DoD security requirements.

CMMC has three levels, starting with safeguarding of Federal Contract Information (FCI) at Level 1 (Self), moving to protection of CUI at Level 2, and culminating with higher-level protection of CUI against Advanced Persistent Threats (APTs) at Level 3 (DIBCAC). Nearly 80,000 organizations that handle CUI will need to achieve CMMC Level 2, which is split into Level 2 (C3PAO) and Level 2 (Self). DoD estimates that 95% of organizations at Level 2 will fall into the C3PAO category, which requires independent third-party assessments rather than self-assessments. In either case, Level 2's security controls are in alignment with the 110 security controls of NIST SP 800-171 Rev. 2.

This paper offers an overview of CMMC and the steps your organization needs to take to prepare for CMMC Level 2 certification. It outlines PreVeil's three-step roadmap to streamline your journey to CMMC Level 2, and concludes with detailed appendices, including a Shared Responsibility Matrix (SRM) and a case study of how a small defense contractor using PreVeil achieved the highest score of 110 out of 110 on their CMMC Level 2 certification. Many defense contractors, higher education institutions, MSPs, and even C3PAOs (CMMC Assessors) have used PreVeil to achieve 110 out of 110 scores on DoD and CMMC assessments.

Finally, note that earlier versions of this paper have been downloaded more than 6,000 times by defense contractors. It is our hope that this updated version reflecting the CMMC Final Rule serves to help your organization, too, as you work to protect your data resources and CUI, and win defense contracts.

CMMC overview

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

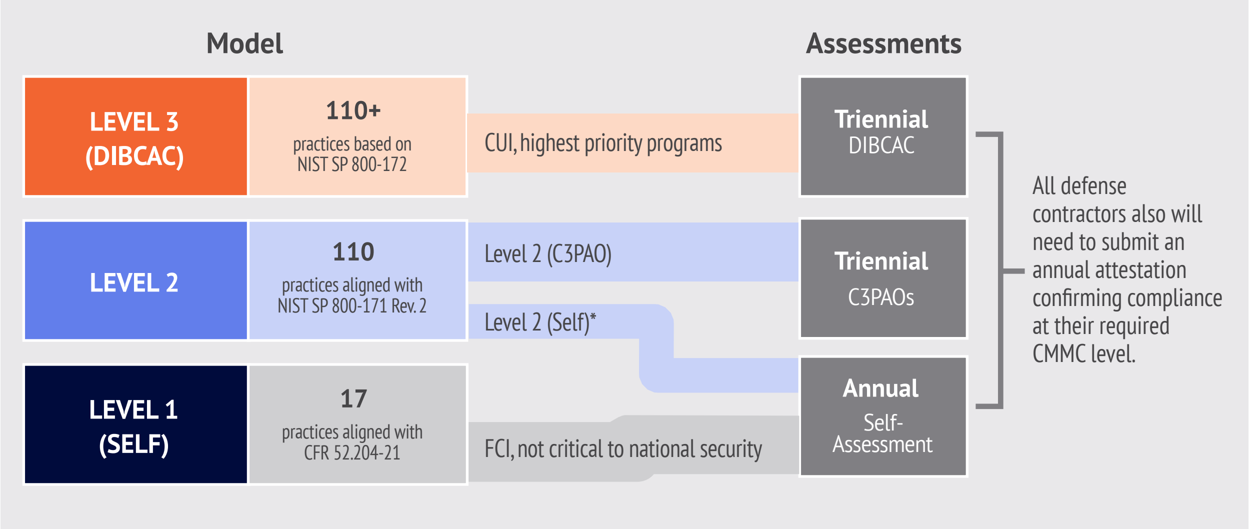
CMMC has three compliance levels, based on the type of information DIB organizations are working with:

- Level 1 is for organizations working with FCI only
- Level 2 is for organizations working with CUI
- Level 3 is for organizations working with CUI and subject to Advanced Persistent Threats (APTs)

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


Model
Assessments
LEVEL 3 (DIBCAC)
110+ practices based on NIST SP 800-172
CUI, highest priority programs
Triennial DIBCAC
LEVEL 2
110 practices aligned with NIST SP 800-171 Rev. 2
Level 2 (C3PAO)
Triennial C3PAOs
Level 2 (Self)*
LEVEL 1 (SELF)
17 practices aligned with CFR 52.204-21
FCI, not critical to national security
Annual Self-Assessment
All defense contractors also will need to submit an annual attestation confirming compliance at their required CMMC level.

Source: DoD Chief Information Officer website.

* DoD estimates that just 5% of the more than 80,000 organizations that will need to achieve CMMC Level 2 will be permitted to self-assess, given the nature of their contract work.

At Level 1, all defense contractors handling FCI will be required to perform annual self-assessments.

At Level 2, it's estimated just 5% of contractors that handle CUI will be permitted to achieve Level 2 (Self), meaning they are permitted to perform annual self-assessments of their CMMC compliance. The wide majority—over 95%—of contractors that handle CUI will need to achieve Level 2 (C3PAO), meaning they will need to undergo third-party assessments once every three years, conducted by accredited C3PAOs (CMMC Third Party Assessment Organizations). After completion of the CMMC assessment, the C3PAO will provide an assessment report to the Cyber AB, CMMC's official accreditation body.

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

Defense contractors at all CMMC levels also will need to submit an annual attestation signed by a senior executive confirming compliance at their required CMMC level.

CMMC Level 2 controls mirror NIST SP 800-171 Revision 2

CMMC Level 2 security controls are in complete alignment with the 110 security controls stipulated in NIST SP 800-171 Rev 2. If your organization handles CUI, then you are currently obligated to implement the NIST SP 800-171 security controls per DFARS 252.204-7012.[1]

CMMC will allow POA&Ms in limited circumstances

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 highest score of 110. Points are deducted for each control not met, down to -203. Negative scores are possible, as scores can range from +110 to -203, a spread of 313 points.

Organizations required to achieve CMMC levels 2 and 3 may have POA&Ms (Plans of Action & Milestones) in place for NIST SP 800-171 security controls not yet met at the time of assessment. POA&Ms indicate how and when unmet controls will be met. POA&Ms are not permitted for organizations required to achieve CMMC Level 1.

But POA&Ms will be permitted at CMMC levels 2 and 3 only for some one-point controls. At Level 2, with two exceptions, POA&Ms will not be permitted for any three- or five-point controls—some of the hardest requirements to meet. Further, if POA&Ms are needed, organizations can receive a "CMMC Level 2 Conditional Certification" following their initial C3PAO assessment only if: 1) a CMMC Level 2/NIST SP 800-171 assessment score of at least 88 is achieved (meaning that at least 80% of the 110 controls are met), *and* 2) all controls not met upon initial assessment are permitted to be met via POA&Ms.[2]

[1] In November 2023, NIST released a full draft of NIST SP 800-171 Revision 3. To learn more about NIST SP 800-171 Rev 3 and its potential impact on CMMC Level 2 requirements, see PreVeil's blog, *Key Takeaways from NIST Release of SP 800-171 Revision 3.*

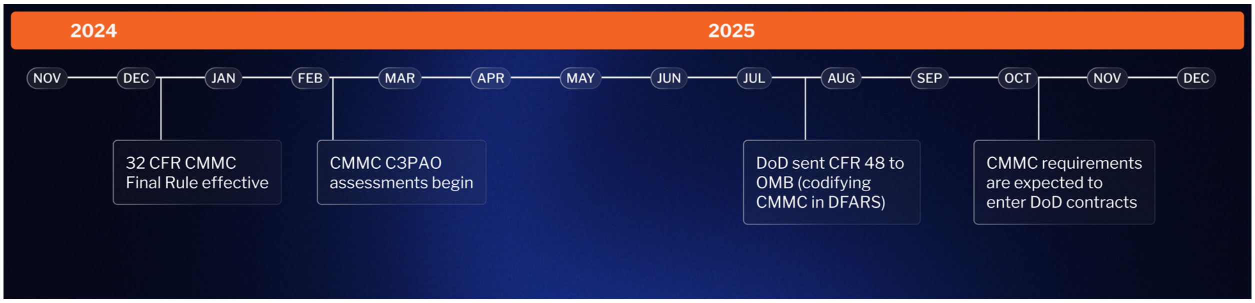
[2] A list of all controls that may *not* be met via POA&Ms is available in the 32 CFR CMMC Final Rule published in the Federal Register (see Section 170.21.)

Finally, POA&Ms will be time-bound: 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 180 days includes a CMMC POA&M Close-Out Assessment. If an organization has deficiencies remaining after 180 days, its Level 2 Conditional Certification will be revoked.

CMMC rulemaking and timeline

CMMC will take its final step toward implementation with the publication of 48 CFR in the Federal Register, which is expected in October 2025. This rule will authorize the DoD to use DFARS 252.204-7021 to add CMMC requirements directly into contracts—triggering Phase 1 of the program's rollout.

Figure 2: CMMC Timeline


2024
2025
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
32 CFR CMMC Final Rule effective
CMMC C3PAO assessments begin
DoD sent CFR 48 to OMB (codifying CMMC in DFARS)
CMMC requirements are expected to enter DoD contracts

The Department of Defense is adopting a four-phase approach for incorporating CMMC requirements into solicitations and contracts:

PHASE 1 begins on the effective date of the complementary 48 CFR CMMC Acquisition Final Rule. During Phase 1, the DoD intends to include the requirement for CMMC Level 1 (Self) or Level 2 (Self) in self-assessments in all applicable DoD solicitations and contracts as a condition of contract award. Additionally, DoD may include the requirement for CMMC Level 1 (Self) or Level 2 (Self) as a condition for exercising an option on a contract awarded prior to the CMMC effective date. DoD may also include the requirement for CMMC Level 2 (C3PAO) in place of the Level 2 (Self) in applicable DoD solicitations and contracts.

PHASE 2 begins one calendar year following the start date of Phase 1. In addition to Phase 1 requirements, DoD intends to include the requirement for CMMC Level 2 (C3PAO) in applicable DoD solicitations and contracts as a condition of contract award.

PHASE 3 begins one calendar year following the start date of Phase 2. In addition to Phase 1 and 2 requirements, DoD intends to include the requirement for CMMC Level 3 (DIBCAC) in all applicable DoD solicitations and contracts as a condition of contract award.

PHASE 4, full implementation, begins one calendar year following the start date of Phase 3. All DoD solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award, including options exercised on contracts awarded prior to the beginning of Phase 4.

Note that during any phase, DoD may implement CMMC requirements in advance of the planned phase indicated above.

> ***"If you're one of those companies... hoping that the protracted rulemaking will save you, you're misguided and that's a pretty reckless way to run your business"***
>
> **– Matt Travis, CEO of Cyber AB**

Finally, it's important for contractors to understand that even though CMMC will be phased in over time, it does not necessarily follow that you have more time to achieve CMMC certification. Your organization, for example, could be far down the supply chain from a contractor subject to CMMC in Phase 1, in which case that contractor must flow down CMMC requirements to your organization at that time.

As Matt Travis, CEO of Cyber AB, the CMMC accreditation body, said during PreVeil's CMMC Summit, "If you're one of those companies…hoping that the protracted rulemaking will save you, you're misguided and that's a pretty reckless way to run your business."

How do I prepare for CMMC?

Now is the time to take action to improve your organization's cybersecurity. Informed estimates from experienced C3PAOs are that it takes typical small to midsize organizations between 6–12 months to meet CMMC Level 2 requirements. That time frame extends beyond when CMMC requirements will begin to appear in DoD contracts. So, again, now is the time to get started on CMMC compliance.

Here are the steps your organization needs to take to achieve CMMC Level 2 certification:

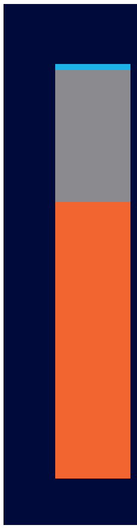
Familiarize yourself with the CMMC framework

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. CMMC levels are based on the type of information your organization works with: Organizations that handle just FCI will need to achieve Level 1. Any organization that handles CUI will need to achieve at least Level 2.

CMMC Level 3 is for defense contractors and university researchers that work with CUI and are subject to Advanced Persistent Threats (APTs).



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

Level 3
1,500 organizations

Level 2
80,000 organizations

Level 1
140,000 organizations

Scope your compliance boundary

Organizations 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.

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. 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 by creating a separate enclave. It stands to reason that a smaller compliance scope means a simpler assessment process that saves you time and money.

Note that if your organization uses External Service Providers (ESPs), such as Managed Service Providers (MSPs), to deliver services that function as Security Protection Assets—such as SIEM services, antivirus, or multi-factor authentication (MFA)—the DoD has determined that those services fall within the organization's compliance boundary and, therefore, will be subject to assessment.

Adopt a platform to secure CUI

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 can help you achieve CMMC Level 2.

Specifically, Cloud Service Providers (CSPs) should:

- ***Support the security controls of NIST SP 800-171.*** The most heavily weighted of the 110 controls, at 5 points each, 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 and CMMC Level 2 certification.
- ***Meet DFARS 252.204-7012 (c)-(g) for incident reporting.*** The DoD places the DFARS 252.204-7012 clause in its contracts that entail handling CUI, which includes the (c)-(g) incident reporting mandates. These requirements—in addition to NIST 800-171—must be met to achieve CMMC Level 2.
- ***Meet FedRAMP Moderate Baseline or Equivalent standards.*** Organizations that sell directly to the Federal government can achieve FedRAMP Baseline Moderate status; those that sell to other entities such as defense contractors (and not directly to the government) need to achieve FedRAMP Baseline Moderate Equivalent instead, as defined in DoD's December 2023 memo. Equivalency is a more rigorous standard because CSPs must demonstrate 100% compliance with all security controls; no POAMs are allowed.
- ***Utilize a FIPS 140-2 validated cryptographic module if CUI is encrypted.*** CSPs that use encryption to protect CUI must submit their cryptographic modules to approved independent laboratories for extensive testing to obtain a FIPS 140-2 certificate.

Finally, know that responsibility for choosing a CMMC-compliant CSP rests squarely on the shoulders of defense contractors, as noted above. Don't simply accept a CSP's self-attestation that they meet all these standards. Ask for documented evidence of its FedRAMP moderate equivalency, for example, or for its FIPS 140-2 certification.

Develop compliance documentation

Documentation of your organization's compliance entails thorough and meticulous work. The first task you'll need to tackle is development of a System Security Plan (SSP) as required by NIST SP 800-171. The SSP explains how your organization meets each of NIST SP 800-171's 110 security controls. The SSP is the foundational document for a NIST SP 800-171 assessment and is a prerequisite for consideration for any DoD contract. You'll also need policy and procedure documents associated with each NIST SP 800-171 security control and, following your self-assessment, POA&Ms for all controls not yet met.

Conduct your NIST SP 800-171 self-assessment

The only path to CMMC Level 2 certification is through NIST SP 800-171. Your best course of action is to focus on complying with that standard now, as has been required by DFARS 7012 since 2017. Figure 3 briefly summarizes DFARS 7012 requirements, along with DFARS clauses 7019 and 7020, which were previously released by DoD to ramp up compliance with NIST SP 800-171 and, likewise, position defense contractors to achieve CMMC Level 2.

After you've implemented the NIST SP 800-171 security controls as best you can on your own and developed your SSP according to DFARS 7012, DFARS 7019 requires your organization to:

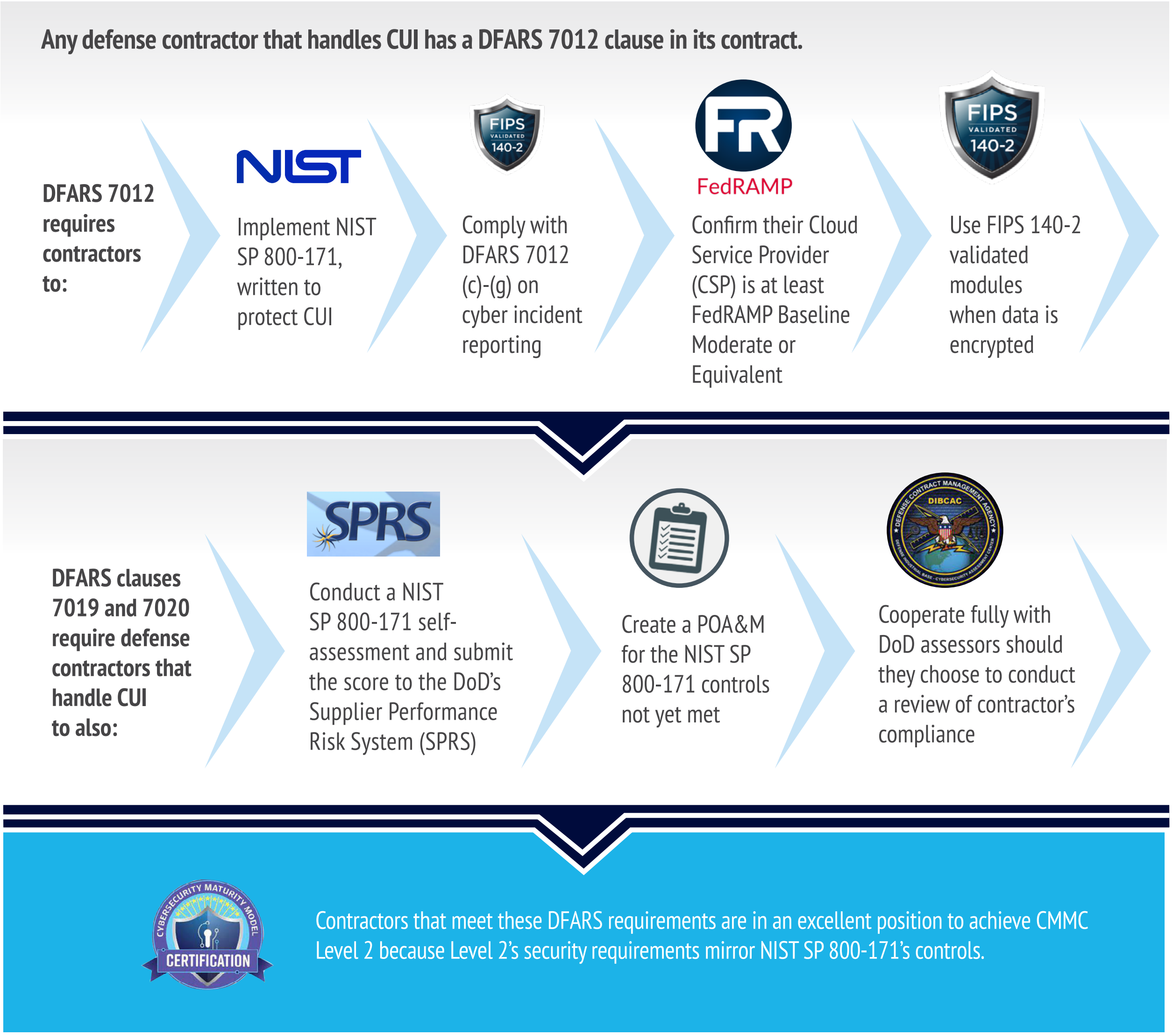
- ***Conduct a NIST SP 800-171 self-assessment*** according to the DoD's Assessment Methodology, which specifies 320 objectives spread across the 110 security requirements (more on this below). All contractors that handle CUI must perform at least a basic level self-assessment.
- ***Submit your self-assessment scores to the DoD's Supplier Performance Risk System (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.
- ***If your organization's self-assessment score falls below 110, create POA&Ms*** for security controls not met, and indicate by what date those security gaps will be remediated and a score of 110 will be achieved. Start to address those gaps.

The only path to CMMC Level 2 certification is through NIST SP 800-171. Your best course of action is to focus on complying with that standard now.

Your organization's SPRS score demonstrates its cybersecurity posture and is an important determinant of your position vis-à-vis competitors when seeking to be part of a defense contract. Lack of an SPRS score altogether is a breach of DFARS 7019 contractual requirements and severely jeopardizes your organization's eligibility to keep existing DoD contracts and win new ones.

DFARS requirements don't end with subcontractors: DFARS 7020 requires prime defense contractors to ensure that their subcontractors comply with 7019 by confirming they have completed their NIST SP 800-171 self-assessment and submitted their score to SPRS. Not surprisingly, primes are already requesting SPRS scores from their subcontractors, and some have specified minimum scores required to enter into contracts with them.

Figure 3: 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

Use FIPS 140-2 validated modules when data is encrypted

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

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

Create a POA&M for the NIST SP 800-171 controls not yet met

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

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

Identify partners and get the help you need

You needn’t take on CMMC compliance on your own. It’s understandable that many organizations lack the necessary internal security expertise to achieve CMMC Level 2.

Depending upon your organization’s circumstances, it may be most cost effective to bring in outside help after you’ve adopted a platform to secure CUI and done your own NIST SP 800-171 assessment to identify security gaps. From there—or whenever you get stuck and need help—outside partners can help you save time and money by creating a smooth path to CMMC Level 2. Note that the consultant or organization that helps you prepare for CMMC certification cannot also serve as the C3PAO that conducts your external assessment.

Crossing the finish line to CMMC Level 2 certification

Once you've worked through the steps above, you'll be ready to move on to your third-party assessment. Here's how that process will unfold.

CMMC Level 2 (C3PAO) assessment	■ Schedule a C3PAO for your external assessment ■ Conduct a readiness review with your C3PAO ■ Undergo C3PAO CMMC Level 2 assessment ■ Address findings from C3PAO assessment and complete C3PAO delta review (if applicable)
CMMC certification	■ C3PAO submits assessment results to Cyber AB ■ Cyber AB reviews and issues CMMC Level 2 (C3PAO) certification or Conditional CMMC Certification ■ If conditional, close out POA&M items within 180 days

Given the high demand for limited numbers of C3PAO organizations that can conduct CMMC assessments, it's highly recommended that you begin to contact C3PAOs now to start planning for and scheduling your assessment.

About costs

Costs associated with CMMC Level 2 certification will vary widely across organizations. Variables include current cybersecurity maturity 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.

As you consider whether to pursue CMMC Level 2 certification so that your organization can continue to do work for the DoD, keep in mind that technology solutions that reduce the time and costs to achieve CMMC Level 2 are available. For a personalized estimate of the expenses required to achieve CMMC Level 2, visit PreVeil's CMMC Level 2 Cost Calculator, developed in collaboration with MSPs and authorized C3PAOs.

PreVeil’s CMMC Solution

PreVeil is the leading CMMC compliance solution. Trusted by thousands of defense contractors, PreVeil's proven solution is secure, easy to use, and saves typical small to midsize organizations 75% compared to alternatives.

Compliance with PreVeil

PreVeil supports more than 90% of the security controls required for CMMC Level 2 certification. 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 4.

For more details, Appendix A presents a comprehensive Shared Responsibility 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.

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 standards[3]
- Encrypts and stores data on FedRAMP High AWS GovCloud
- Meets DFARS 252.204-7012 (c)-(g), which stipulate requirements for cyber incident reporting[4]
- Meets FIPS 140-2 standards for cryptographic modules used for encryption.[5]

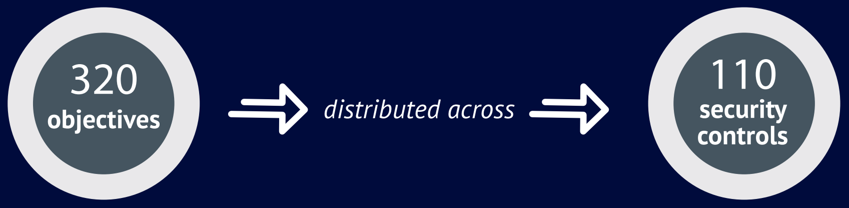
[3] The FedRAMP Baseline Moderate “Equivalent” category exists because only organizations that sell directly to the Federal government need to achieve FedRAMP Baseline Moderate status; cloud service providers that sell to other entities, such as defense contractors (and not directly to the government), can 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.

[4] 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.

[5] See PreVeil’s FIPS 140-2 certificate on NIST’s Computer Security Resource website here.

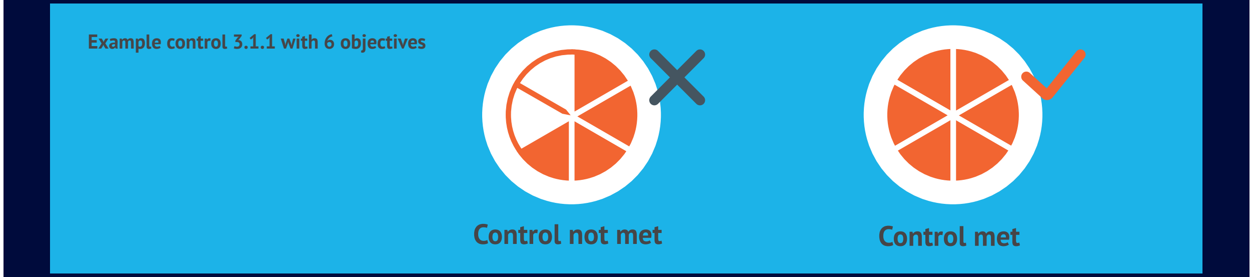
Figure 4: CMMC Level 2/NIST SP 800-171 assessment and how PreVeil helps

CMMC Level 2/NIST SP 800-171 assessors will review compliance with:

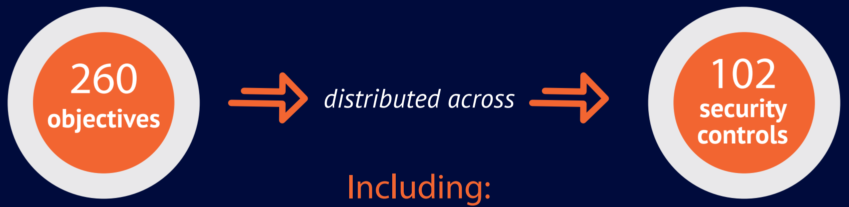


320 objectives → *distributed across* → 110 security controls

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



260 objectives → *distributed across* → 102 security controls

Including:

every objective for 37 controls

+

shared responsibility for 65 controls

Total = 102 controls

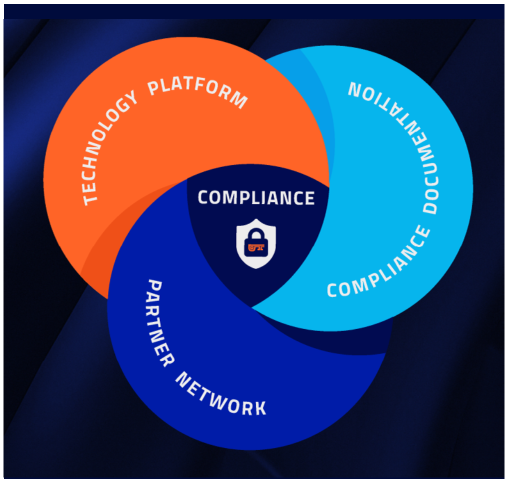
PreVeil vs. Alternatives

Most widely-deployed commercial systems used to store, process and transmit CUI do not comply with CMMC Level 2 requirements. That includes Microsoft 365 Commercial. Instead, Microsoft offers GCC High, a solution suitable for very large organizations that work exclusively for the DoD. However, the complexity and costs of GCC High are a burden for small to midsize companies and universities. For those organizations, PreVeil offers compelling advantages, namely, military-grade security that integrates directly with Outlook and File Explorer. PreVeil eliminates costly deployments and requires fewer and lower-cost licenses than GCC High. And unlike GCC High's costly guest accounts, PreVeil let's you invite any contractor to create a free account, enabling secure communication within minutes. See Appendix B, How PreVeil Saves 75% vs. Microsoft GCC High, to learn more.

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's proven roadmap to CMMC certification

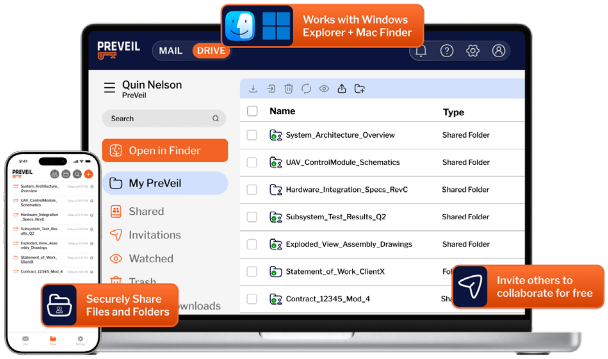
PreVeil's straightforward three-step roadmap to CMMC Level 2 certification streamlines your compliance journey, making it more efficient and affordable.



1 Adopt PreVeil to process, store 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 CMMC Level 2.

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.

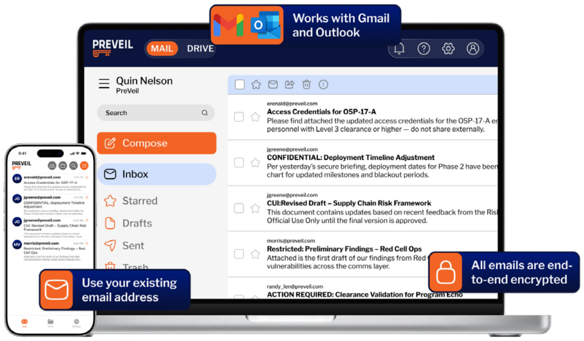

Works with Windows Explorer + Mac Finder
PREVEIL
MAIL
DRIVE
Quin Nelson
PreVeil
Search
Open in Finder
My PreVeil
Shared
Invitations
Watched
Trash
wnloads
Securely Share Files and Folders
Invite others to collaborate for free

Name	Type
System_Architecture_Overview	Shared Folder
UAV_ControlModule_Schematics	Shared Folder
Hardware_Integration_Specs_RevC	Shared Folder
Subsystem_Test_Results_Q2	Shared Folder
Exploded_View_Assembly_Drawings	Shared Folder
Statement_of_Work_ClientX	Fol
Contract_12345_Mod_4	Sha

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.



Works with Gmail and Outlook

erenald@preveil.com
Access Credentials for OSP-17-A
Please find attached the updated access credentials for the OSP-17-A e
personnel with Level 3 clearance or higher — do not share externally.

jgreene@preveil.com
CONFIDENTIAL: Deployment Timeline Adjustment
Per yesterday's secure briefing, deployment dates for Phase 2 have been
chart for updated milestones and blackout periods.

jgreene@preveil.com
CUI:Revised Draft – Supply Chain Risk Framework
This document contains updates based on recent feedback from the Ris
Official Use Only until the final version is approved.

morris@preveil.com
Restricted: Preliminary Findings – Red Cell Ops
Attached is the first draft of our findings from Red
vulnerabilities across the comms layer.

randy_len@preveil.com
ACTION REQUIRED: Clearance Validation for Program Echo

Use your existing email address

All emails are end-to-end encrypted

A PROVEN SOLUTION

As of August2025, over 35 defense contractors and C3PAOs have used PreVeil to achieve CMMC compliance with perfect 110 scores on their CMMC Level 2 assessments.

- **Kokosing achieves perfect 110 score on their CMMC their CMMC Level 2 assessment.**
- **Regola Cyber, a CMMC Assessor (C3PAO), Achieves Authorization Using PreVeil**

Read more on PreVeil's resources page.

2 Take advantage of PreVeil's Compliance Accelerator documentation.

PreVeil offers an industry-first, comprehensive set of assessment-ready documentation that covers everything you need to achieve a 110/110 CMMC score in just 4-6 months. Every document has been reviewed by compliance experts and CMMC assessors (C3PAOs) for accuracy and completeness. At the core of this toolkit is a fictional company operating a PreVeil-secured CUI enclave that has all the documentation that they would need for assessment, including:

- ***System Security Plan (SSP) template:*** The SSP provides detailed language that explains how a customer will be able to meet each of the CMMC Level 2/NIST SP 800- 171 controls and objectives—for both the ones directly related to PreVeil but also others beyond the scope of the core PreVeil platform.

> ***"The Accelerator Package documentation was fabulous and easy to use—we did not get a single comment on our SSP from the C3PAO or DIBCAC. And it was a BARGAIN—the documentation alone saved me $100,000."***
>
> **— Vice President of Operations at a defense contractor that achieved a perfect score on their CMMC Level 2 assessment**

- ***Standard Operating Procedures:*** The documentation includes SOPs for all fourteen control families that detail the organization's policies for how it addresses the CMMC Level 2/NIST SP 800-171 controls listed in the SSP.
- ***Network & CUI Flow Diagrams:*** Ready-to-use diagram templates that show where CUI flows within your enclave and with guidance on how to adapt them for your specific environment.
- ***Shared Responsibility Matrix (SRM):*** The SRM lists each of the CMMC Level 2/NIST SP 800-171 controls and objectives, indicating if they are fully, partially, or not met by PreVeil. It also provides language describing the responsibilities that PreVeil has for each control along with the responsibilities of the customer.
- ***Assessment Checklists & Implementation Guidance:*** Comprehensive checklists which cover every step for ongoing compliance management and assessment preparation. PreVeil's subscription model ensures that your organization automatically receives ongoing updates and enhancements to the package.
- ***POA&M template:*** The POA&M template lists the objectives not met by the organization when deploying PreVeil. The template provides examples the organization can use to address these unmet controls and objectives. PreVeil's subscription model ensures that your organization automatically receives ongoing updates and enhancements to the package.

3 **Leverage PreVeil's partner network.** To facilitate connections to the specialized help many small to midsize businesses need, PreVeil has built a partner network of C3PAOs, Certified CMMC Assessors, Registered Practitioners, MSPs, and other consultants and organizations certified by the Cyber AB—all with expert knowledge of DFARS, NIST, CMMC and PreVeil.

PREFERRED PARTNER NETWORK

Assessors | Consultants | Service Providers

The partners' expert knowledge of PreVeil significantly streamlines your engagement because no time is spent learning how PreVeil supports compliance. This 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 to its partner community, all while saving you time, minimizing your risks, and reducing your costs.

PreVeil Benefits

PreVeil understands the challenges that small to midsize contractors must overcome to achieve CMMC Level 2. For organizations with limited cybersecurity expertise and compliance resources, PreVeil's proven solution is easy to deploy and use, cost-effective, and offers best-in-class security.

Easy to deploy

PreVeil works alongside and has no impact on existing file and email servers. There's no need to rip and replace servers or domains, and PreVeil can be deployed to an enclave created just for users who handle CUI—as opposed to alternative solutions that often require deployment across entire organizations.

Easy to use

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

Cost effective

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

Best-in-class security

PreVeil's state-of-the art security features help your organization raise its cybersecurity levels, comply with NIST SP 800-171 and, likewise, achieve CMMC Level 2. That's because PreVeil's platform supports compliance with 260 of the 320 assessment objectives specified in the NIST SP 800-171 Assessment Guide, and 102 of the 110 NIST SP 800-171 security controls. PreVeil features that enable this best-in-class security are described in the following section.

PreVeil Security Features

PreVeil's security features incorporate modern cybersecurity principles that help your organization protect CUI and achieve CMMC Level 2. Following the descriptions of each those features below, we also note the specific CMMC/NIST SP 800-171 control families that each feature addresses.

End-to-end encryption

PreVeil's 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 means that only the sender and recipient can ever read the information being shared—and no one else. Unlike systems that rely on encryption in transit and at rest, with end-to-end encryption data can never be decrypted on a server anywhere. That's because the decryption keys are stored only on personal devices and never in key servers, which are irresistible targets for cybercriminals. Thus, even if attackers successfully steal data from a server that's part of an end-to-end encrypted system, the data will be just useless gibberish. If devices are lost or stolen, PreVeil's device management controls allow administrators to quickly disable them.

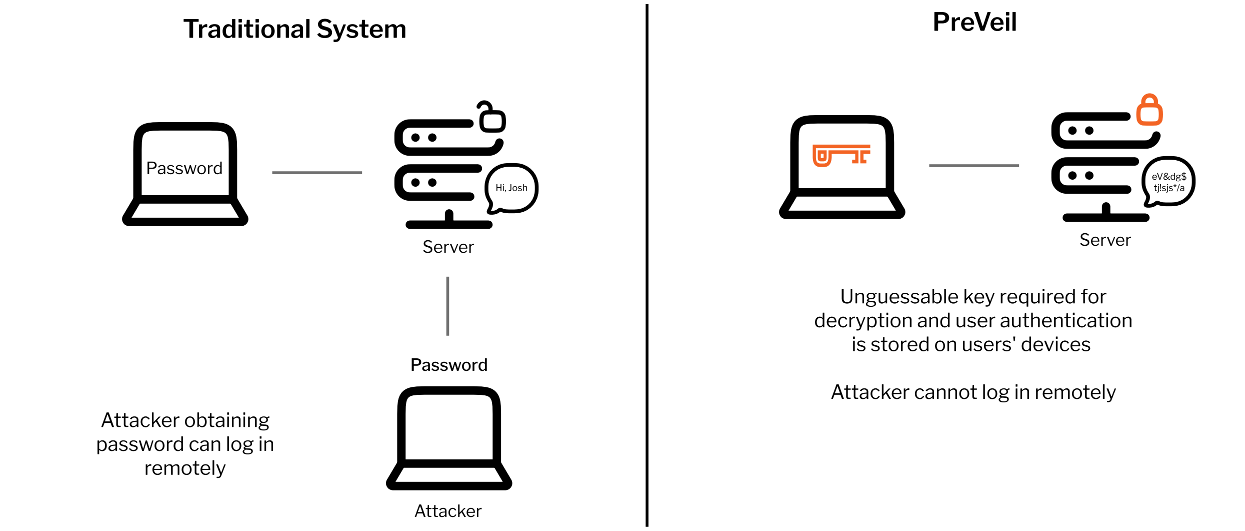
End-to-end encryption supports compliance with the following CMMC/NIST SP 800-171 control families: Access Control, Configuration Management, Media Protection, Systems & Communications Protection, and System & Informational Integrity.

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

Key-based authentication instead of passwords

Passwords create a significant security risk because they are routinely guessed or stolen. 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 5 below. Moreover, device-based keys prevent hackers from ever remotely accessing user accounts.

Figure 5: PreVeil eliminates password vulnerabilities with keys


Traditional System
Password
Hi, Josh
Server
Password
Attacker
Attacker obtaining password can log in remotely
PreVeil
eV&dg$ tj!sjs*/a
Server
Unguessable key required for decryption and user authentication is stored on users' devices
Attacker cannot log in remotely

Key-based authentication supports compliance with the following CMMC/NIST SP 800-171 control families: Identification & Authentication, System & Communications Protection, and Systems & Informational Integrity.

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 advantages of cloud-based services such as lower costs, less risk, better scalability, fewer administrative and maintenance responsibilities, and faster routes to compliance with cybersecurity regulations.

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.

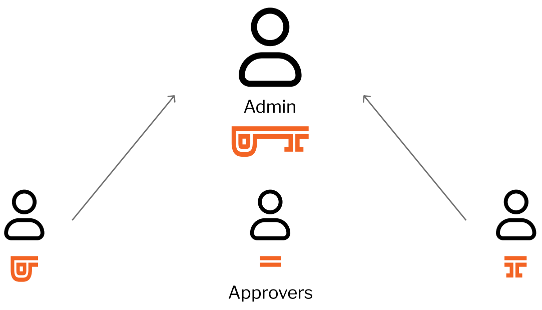
> ***Passwords create a significant security risk because they are routinely guessed or stolen. A much better approach is to authenticate users with private keys that are stored only on the user's device.***

Cloud-based services supports compliance with the following CMMC/NIST SP 800-171 control families: Maintenance, Media Protection, and Physical Protection.

Administrative distributed trust via Approval Groups

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. 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 6. Approval is a critical but seamless process.

Figure 6: PreVeil Approval Groups: Admin access to other users' data only with complete key



Administrative distributed trust supports compliance with the following CMMC/NIST SP 800-171 control families: Access Control and Systems & Communications Protection.

Controlled access via Trusted Communities

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. PreVeil's Trusted Communities feature allows administrators to restrict communication to pre-approved domains and email addresses, virtually eliminating phishing and spoofing attacks and allowing organizations to control the flow of CUI. Individuals outside the trusted community are blocked from sending or receiving encrypted information.

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

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 quickly disable lost or stolen devices. 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.

Administrative consoles support compliance with the following CMMC/NIST SP 800-171 control families: Access Control, Audit & Accountability, Identification & Authentication, and System & Information Integrity.

Encrypted logs 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.

Encrypted logs support compliance with the following CMMC/NIST SP 800-171 control family: Audit & Accountability.

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 midsize 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.

Readily accessible data backups support compliance with the following CMMC/NIST SP 800-171 control family: Media Protection.

PreVeil's security features all contribute to supporting your organization's compliance with CMMC Level 2 and NIST SP 800-171's requirements. In fact, PreVeil's protection of CUI addresses what are often the most difficult security controls for organizations to meet. Deploying PreVeil's proven and trusted solution will help your organization take a huge leap toward achieving CMMC Level 2 certification.

Conclusion

CMMC establishes assessment mechanisms to verify compliance with DoD cybersecurity requirements and is on the fast track to appear in defense contracts in mid-2025. Today, if your organization handles CUI, you have a DFARS 252.204-7012 clause in your contract that requires you to comply with NIST SP 800-171. CMMC Level 2 security controls will mirror these same NIST SP 800-171 controls.

Now is the time to get started on CMMC compliance and protect your business from penalties and contract loss. While CMMC may seem overwhelming to small and midsize organizations, PreVeil was built to help defense companies achieve CMMC Level 2 faster and more affordably. PreVeil 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.

PreVeil is the leading solution for NIST, CMMC and DFARS compliance and is trusted by thousands of defense contractors. A dozen PreVeil customers have achieved CMMC compliance by the highest possible NIST SP 800-171 score of 110 out of 110 in rigorous DIBCAC and JSVA assessments (see Appendix C).

To learn more about how PreVeil can help your organization achieve NIST SP 800-171 and CMMC Level 2 compliance more affordably, sign up here for a short demo with our team.

Appendix A: PreVeil Shared Responsibility Matrix (SRM)

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

The PreVeil SRM 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 SRM also shows which assessment objectives are associated with each CMMC Level 2/NIST SP 800-171 control.

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Access Control (AC)	CMMC Level 1	3.1.1	-5	Control	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system allows the customer to control access to the customer's instance of the PreVeil system. Only customer authorized and added users will be able to access the customer's instance of the PreVeil system and administrators of the customer's instance of the PreVeil system will be able to limit the processes acting on behalf to authorized users, or devices in the administrative functions available to the customer's PreVeil instance administrators. The customer is responsible for granting and controlling the access to authorized users and authorized devices accessing the customer's instance of the PreVeil system.	Shared			0
Access Control (AC)	CMMC Level 1	3.1.2	-5	Control	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system ensures that the customer administering the customer's instance of the PreVeil system is able to limit system access to the types of transactions and functions that authorized users are permitted to execute. The customer inherits the PreVeil access transaction types and functions to the following Roles: Administrative and User. The customer inherits the PreVeil access transaction types and functions to the following functions: View-Only, Read, Edit, Edit & Share, Administrator. NOTE: For all controls, there may be customer responsibility, within each control (even if it is marked as PreVeil Inherited), if there are other systems and/or security protection assets that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that ALL endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that ALL CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that ALL relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Access Control (AC)	CMMC Level 1	3.1.20	-1	Control	Verify and control/limit connections to and use of external information systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes verifying and controlling/limiting connections to and use of external information systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system does not allow external systems to connect directly to the PreVeil system (PVCS). The customer's instance of the PreVeil system does not have any external connections from the PreVeil system due to this PreVeil system policy. However, for any other systems used within the customer's organization or possible external information system connections that would affect the customer's instance of the PreVeil system, the customer is responsible for addressing these within this control.	Shared			0
Access Control (AC)	CMMC Level 1	3.1.22	-1	Control	Control information posted or processed on publicly accessible information systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. The customer is responsible for controlling information posted or processed on public accessible information systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0
Access Control (AC)	CMMC Level 2	3.1.3	-1	Control	Control the flow of CUI in accordance with approved authorizations.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes controlling the flow of CUI in accordance with approved authorizations for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system gives the customer the ability to control the flow of CUI within customer's instance of the PreVeil system in accordance with approved customer organizational authorizations. The administrators of the customer's instance of the PreVeil system have the ability to limit the access to CUI within folders, as needed, and to ensure that all CUI access is only granted to the customer identified authorized users within the customer's instance of the PreVeil system.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Access Control (AC)	CMMC Level 2	3.1.4	-1	Control	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes separating the duties of individuals to reduce the risk of malevolent activity without collusion for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system gives the customer the ability to separate the duties of individuals to reduce the risk of malevolent activity without collusion in the customer's instance of the PreVeil system. PreVeil allows the customer to assign duties and access to the PreVeil system based on the need for separation of duties, as needed. PreVeil has administrative and user function separated within the PreVeil interface and customers may choose to have separate logons within their instance of the PreVeil system, as requested by the customer to PreVeil.	Shared			0
Access Control (AC)	CMMC Level 2	3.1.5	-3	Control	Employ principle of least privilege, including for specific security functions and privileged accounts.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes employing the principle of least privilege, including for specific security functions and privileged accounts for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system gives the customer the ability to enforce the principle of least privilege by allowing the customer to enforce the principle of least privilege for specific security functions and privileged accounts within the customer's instance of the PreVeil system. PreVeil allows the customer to control the customer defined specific security functions, as assigned based on those defined security functions, and allows the customer to employ least privilege on privileged accounts as defined by the customer policies and procedures. Customer's have the ability within their PreVeil instance to assign individuals based on the customer's organizational requirements, including the ability to identify privileged accounts within the customer's PreVeil system and enforce the principle of least privilege as defined and executed for all systems and endpoints in scope.	Shared			0
Access Control (AC)	CMMC Level 2	3.1.6	-1	Control	Use non-privileged accounts or roles when accessing nonsecurity functions.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes ensuring the use of non-privileged accounts or roles when accessing nonsecurity functions for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil allows the customer to assign duties and access to the customer's instance of the PreVeil system based on the need for separation of duties, as needed. PreVeil has administrative and user function separated within the PreVeil interface and customers may choose to have separate logons within their instance of the PreVeil system, as requested by the customer to PreVeil.	Shared			0
Access Control (AC)	CMMC Level 2	3.1.7	-1	Control	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil defines user based, non-privileged functions, within the customer's instance of PreVeil, as those pertaining to PreVeil users who do not have administrative access. Users are able to interact with PreVeil information based on their specific level of access to the specific information granted to them by other users or the customer's PreVeil instance administrators. Users in the PreVeil system are unable to access privileged functions. Those privileged functions are only accessible by those who are granted administrative access to the customer's instance of the PreVeil system. All administrative actions are captured in the customer's instance of PreVeil in the administrative console within the audit log functionality. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Access Control (AC)	CMMC Level 2	3.1.8	-1	Control	Limit unsuccessful logon attempts.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system does not allow for any unsuccessfully logon attempts due to the nature of the end-to-end encryption, key authentication based (not password based)security infrastructure the PreVeil system is based on. Authorized users can only access the customer's instance of PreVeil with the correct security key, making unsuccessfully logons impossible. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Access Control (AC)	CMMC Level 2	3.1.9	-1	Control	Provide privacy and security notices consistent with CUI rules.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes providing privacy and security notices consistent with CUI rules for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system provides the ability to add privacy and security notices based on CUI rules to PreVeil messaging (with the email signature option) and on all files and folders within the customer's instance of the PreVeil system. These file and folder notices can be placed in the file and/or folder name and folders can be nested under a main CUI folder with security banner information present.	Shared			0
Access Control (AC)	CMMC Level 2	3.1.10	-1	Control	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. The customer is responsible for ensuring the use of session lock with patter-hiding displays to prevent access and viewing of data after a period of inactivity for all systems and endpoint in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0
Access Control (AC)	CMMC Level 2	3.1.11	-1	Control	Terminate (automatically) user sessions after a defined condition.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes ensuring the automatic termination of user sessions after a defined condition for all systems and endpoint in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. In addition, PreVeil grants the customer's instance of PreVeil administrators the ability to manually remove user access to PreVeil either ad hoc or through setting a time limit for access to information on the system (i.e., user will only have access through a certain date).	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Access Control (AC)	CMMC Level 2	3.1.12	-5	Control	Monitor and control remote access sessions.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system is cloud based and inherently remote. The customer's instance of the PreVeil system inherits monitoring and controlling of the remote access sessions through the PreVeil system. The customer's instance of PreVeil uses user and device keys to manage access to the system. Device keys are rotated, automatically, every 24 hours. Access to the customer's instance of the PreVeil system, being inherently remote, is limited to the authorized users within the system and actions that are associated with that authorized user. There is no VPN inherent to the customer's instance of the PreVeil system. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Access Control (AC)	CMMC Level 2	3.1.13	-5	Control	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system uses end-to-end encrypts data at rest and in transit, using NIST validated and certified FIPS 140-2 algorithms. The NIST PreVeil system certification for FIPS validation may be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. The PreVeil system is cloud based and inherently remote. The customer's instance of the PreVeil system inherits monitoring and controlling of the remote access sessions through the PreVeil system. The customer's instance of PreVeil uses user and device keys to manage access to the system. Device keys are rotated, automatically, every 24 hours. Access to the customer's instance of the PreVeil system, being inherently remote, is limited to the authorized users within the system and actions that are associated with that authorized user. There is no VPN inherent to the customer's instance of the PreVeil system. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Access Control (AC)	CMMC Level 2	3.1.14	-1	Control	Route remote access via managed access control points.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system is only accessible remotely and only accessible by customer authorized users. The customer's instance of the PreVeil system end-to-end encrypts data at rest and in transit, using NIST validated and certified FIPS 140-2 algorithms. The NIST PreVeil system certification for FIPS validation may be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. The PreVeil system is cloud based and inherently remote. The customer's instance of the PreVeil system inherits monitoring and controlling of the remote access sessions through the PreVeil system. The customer's instance of PreVeil uses user and device keys to manage access to the system. Device keys are rotated, automatically, every 24 hours. Access to the customer's instance of the PreVeil system, being inherently remote, is limited to the authorized users within the system and actions that are associated with that authorized user. There is no VPN inherent to the customer's instance of the PreVeil system. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Access Control (AC)	CMMC Level 2	3.1.15	-1	Control	Authorize remote execution of privileged commands and remote access to security-relevant information.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system is only accessible remotely and only accessible by customer authorized users. This includes remote execution of privileged commands and remote access to security-relevant information on the customer's instance of PreVeil. The PreVeil system infrastructure also limits remote execution of privileged commands and remote access to security-relevant information to authorized individuals (see column J of this control). The customer's instance of the PreVeil system end-to-end encrypts data at rest and in transit, using NIST validated and certified FIPS 140-2 algorithms. The NIST PreVeil system certification for FIPS validation may be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. The PreVeil system is cloud based and inherently remote. The customer's instance of the PreVeil system inherits monitoring and controlling of the remote access sessions through the PreVeil system. The customer's instance of PreVeil uses user and device keys to manage access to the system. Device keys are rotated, automatically, every 24 hours. Access to the customer's instance of the PreVeil system, being inherently remote, is limited to the authorized users within the system and actions that are associated with that authorized user. There is no VPN inherent to the customer's instance of the PreVeil system. Any customer assigned administrator is authorized to execute privileged commands and will have remote access to any relevant security information granted by the customer. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Access Control (AC)	CMMC Level 2	3.1.16	-5	Control	Authorize wireless access prior to allowing such connections.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. The customer is responsible for authorizing wireless access prior to allowing such connections for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0
Access Control (AC)	CMMC Level 2	3.1.17	-5	Control	Protect wireless access using authentication and encryption.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system is only accessible remotely and only accessible by customer authorized users. This includes remote execution of privileged commands and remote access to security-relevant information on the customer's instance of PreVeil. The PreVeil system infrastructure also limits remote execution of privileged commands and remote access to security-relevant information to authorized individuals (see column J of this control). The customer's instance of the PreVeil system end-to-end encrypts data at rest and in transit, using NIST validated and certified FIPS 140-2 algorithms. The NIST PreVeil system certification for FIPS validation may be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. The PreVeil system is cloud based and inherently remote. The customer's instance of the PreVeil system inherits monitoring and controlling of the remote access sessions through the PreVeil system. The customer's instance of PreVeil uses user and device keys to manage access to the system. Device keys are rotated, automatically, every 24 hours. Access to the customer's instance of the PreVeil system, being inherently remote, is limited to the authorized users within the system and actions that are associated with that authorized user. There is no VPN inherent to the customer's instance of the PreVeil system. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Access Control (AC)	CMMC Level 2	3.1.18	-5	Control	Control connection of mobile devices.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes controlling connection of mobile devices for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil allows for the customer's instance of PreVeil administrators to allow mobile devices such as cellphones and tablets to connect to the customer's instance of the PreVeil system. The customer's PreVeil administrators are responsible for managing access and authorization of such devices onto the customer's instance of the PreVeil system. The PreVeil system allows administrators to allow or disallow mobile devices, at their discretion, to connect to the customer's instance of PreVeil, as well as providing monitoring and audit logging functionality for such connections.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Access Control (AC)	CMMC Level 2	3.1.19	-3	Control	Encrypt CUI on mobile devices and mobile computing platforms.	the company's instance of PreVeil. This includes ensuring encryption of CUI on mobile devices and mobile computing platforms for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil allows for the customer's instance of PreVeil administrators to allow mobile devices such as cellphones and tablets to connect to the customer's instance of the PreVeil system. The customer's PreVeil administrators are responsible for managing access and authorization of such devices onto the customer's instance of the PreVeil system. The PreVeil system allows administrators to allow or disallow mobile devices, at their discretion, to connect to the customer's instance of PreVeil, as well as providing monitoring and audit logging functionality for such connections. All data transmitted and stored via the PreVeil system is FIPS 140-2 end-to-end encrypted, including on mobile devices and mobile computing platforms through the PreVeil mobile app. The PreVeil NIST CMVP certification may be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804	Shared			0
Access Control (AC)	CMMC Level 2	3.1.21	-5	Control	Limit use of portable storage devices on external systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Access Control activities within the company's instance of PreVeil. This includes limiting the use of portable storage devices on external systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system does not allow for portable storage devices to connect to the PreVeil system infrastructure backend. The customer is responsible for ensuring the limitation of portable storage devices on external systems outside of the customer's instance of the PreVeil system and for any systems and endpoints in scope.	Shared			0
Awareness and Training (AT)	CMMC Level 2	3.2.1	-5	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.	Customer Responsibility: The customer is expected to assign administrators to manage the Awareness and Training activities within the company's instance of PreVeil. This includes ensuring 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 for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil has awareness and training available regarding the PreVeil system security risks associated with system administrator and user actions, as well as insider threat awareness training. PreVeil customers are responsible for addressing training regarding their internal policies, procedures, and standards applicable to each role within the company's hierarchy.	Shared			0
Awareness and Training (AT)	CMMC Level 2	3.2.2	-5	Control	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Customer Responsibility: The customer is expected to assign administrators to manage the Awareness and Training activities within the company's instance of PreVeil. This includes ensuring that personnel are trained to carry out the assigned information security-related duties and responsibilities for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil has awareness and training available regarding the PreVeil system security risks associated with system administrator and user actions, as well as insider threat awareness training. PreVeil customers are responsible for addressing training regarding their internal policies, procedures, and standards applicable to each role within the company's hierarchy.	Shared			0
Awareness and Training (AT)	CMMC Level 2	3.2.3	-1	Control	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Customer Responsibility: The customer is expected to assign administrators to manage the Awareness and Training activities within the company's instance of PreVeil. This includes providing security awareness training on recognizing and reporting potential indicators of insider threat for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil has awareness and training available regarding the PreVeil system security risks associated with system administrator and user actions, as well as insider threat awareness training. PreVeil customers are responsible for addressing training regarding their internal policies, procedures, and standards applicable to each role within the company's hierarchy.	Shared			0
Audit and Accountability (AU)	CMMC Level 2	3.3.1	-5	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.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and may be monitored according to the company's internal policies and procedures. These audit logs ensure the capturing of data required for enabling the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. PreVeil ensures that these audit logs capture all administrative functions, user accesses of data within the system, multiple different actions performed by users and administrators within the system, and ensures that all audit logs are time stamped and can be traced back to the individual who performed the action. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Audit and Accountability (AU)	CMMC Level 2	3.3.2	-3	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.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. These audit logs ensure the capturing of data required for enabling the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. PreVeil ensures that these audit logs capture all administrative functions, user accesses of data within the system, multiple different actions performed by users and administrators within the system, and ensures that all audit logs are time stamped and can be traced back to the individual who performed the action. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Audit and Accountability (AU)	CMMC Level 2	3.3.3	-1	Control	Review and update logged events.	Customer Responsibility: The customer is expected to assign administrators to manage the Audit and Accountability activities within the company's instance of PreVeil. This includes reviewing and updating logged events for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. These audit logs ensure the capturing of data required for enabling the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. PreVeil ensures that these audit logs capture all administrative functions, user accesses of data within the system, multiple different actions performed by users and administrators within the system, and ensures that all audit logs are time stamped and can be traced back to the individual who performed the action.	Shared			0
Audit and Accountability (AU)	CMMC Level 2	3.3.4	-1	Control	Alert in the event of an audit logging process failure.	Customer Responsibility: The customer is expected to assign administrators to manage the Audit and Accountability activities within the company's instance of PreVeil. This includes ensuring alerts in the event of an audit logging process failure for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. These audit logs ensure the capturing of data required for enabling the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. PreVeil ensures that these audit logs capture all administrative functions, user accesses of data within the system, multiple different actions performed by users and administrators within the system, and ensures that all audit logs are time stamped and can be traced back to the individual who performed the action. In the event of an audit log failure within the PreVeil system, PreVeil will alert, via email, the identified customer PreVeil instance administrators (or other designated POCs) of this failure. Customers may also access and subscribe to the PreVeil Status page for additional information regarding the current status of the PreVeil system found here: https://status.preveil.com/	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Audit and Accountability (AU)	CMMC Level 2	3.3.5	-5	Control	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Customer Responsibility: The customer is expected to assign administrators to manage the Audit and Accountability activities within the company's instance of PreVeil. This includes ensuring the correlation of audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activities for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. These audit logs ensure the capturing of data required for enabling the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activities. PreVeil ensures that these audit logs capture all administrative functions, user accesses of data within the system, multiple different actions performed by users and administrators within the system, and ensures that all audit logs are time stamped and can be traced back to the individual who performed the action. The PreVeil customer instance audit logs support the correlation of audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activities.	Shared			0
Audit and Accountability (AU)	CMMC Level 2	3.3.6	-1	Control	Provide audit record reduction and report generation to support on-demand analysis and reporting.	Customer Responsibility: The customer is expected to assign administrators to manage the Audit and Accountability activities within the company's instance of PreVeil. This includes providing audit record reduction and report generation support on-demand analysis and reporting for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. These audit logs support on-demand analysis and reporting. Customer's PreVeil instance administrators, at any time, any run reports regarding audit logging information with their instance of the PreVeil system to support on-demand analysis and to be used within a audit record reductions process defined by the customer.	Shared			0
Audit and Accountability (AU)	CMMC Level 2	3.3.7	-1	Control	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. These audit logs are compared and synchronized with internal system clocks with an authoritative source (AWS) to generate time stamps for audit records. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Audit and Accountability (AU)	CMMC Level 2	3.3.8	-1	Control	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Customer Responsibility: The customer is expected to assign administrators to manage the Audit and Accountability activities within the company's instance of PreVeil. This includes protecting audit information and audit logging tools from unauthorized access, modification, and deletion for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. The audit logs and audit logging functionality and tools are protected from unauthorized access, modification, and deletion through encryption and digital signatures. PreVeil audit logs cannot be modified or deleted by anyone from PreVeil, or within the customer's PreVeil instance. Only authorized customer instance of PreVeil administrators can access the PreVeil audit logging function and cannot delete or modify these logs. The customer is responsible for protecting audit information once it leaves the customer's instance of the PreVeil system.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Audit and Accountability (AU)	CMMC Level 2	3.3.9	-1	Control	Limit management of audit logging functionality to a subset of privileged users.	Customer Responsibility: The customer is expected to assign administrators to manage the Audit and Accountability activities within the company's instance of PreVeil. This includes limiting management of audit logging functionality to a subset of privileged users for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides audit log capabilities that may be accessed by the customer's instance of PreVeil administrators. These audit logs are retained, indefinitely, within the customer's instance of the PreVeil system and PreVeil ensures that the actions of individual customer's instance of the PreVeil system users can be uniquely traced to those users, so they can be held accountable for their actions. Audit logging functionality within the customer's instance of PreVeil is limited to the customer identified administrators who can perform administrative functions, including audit log report creation and review, to the customer's instance of PreVeil administrators.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.1	-5	Control	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. The customer is responsible for establishing and maintaining baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system inherits PreVeil system infrastructure baseline configurations and inventories throughout the PreVeil system. However, the customer is responsible for managing the installation of the PreVeil system on customer's endpoints. When installed on the endpoint, the hardware of that endpoint must be configured under the customer's established and maintained baseline configuration.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.2	-5	Control	Establish and enforce security configuration settings for information technology products employed in organizational systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes establishing and enforcing security configuration settings for information technology products employed in organizational systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance is able to support security configuration settings established and enforced by the customer's organization in the customer's PreVeil instance. It is the customer's responsibility to ensure that the configuration of the customer's instance of PreVeil is configured to best suit the needs of the customer and that configuration of the customer's instance of the PreVeil system is documented within the customer's organization.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.3	-1	Control	Track, review, approve, or disapprove, and log changes to organizational systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes tracking, reviewing, approving, or disapproving, and logging changes to organizational systems for information technology products employed in organizational systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance is able to support the tracking, reviewing, approving, or disapproving, and logging of changes to the customer's instance of the PreVeil system. PreVeil tracks, reviews, approves/disapproves changes to the PreVeil system (PVCS). For more information, see control 3.4.3, column J.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.4	-1	Control	Analyze the security impact of changes prior to implementation.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes analyzing the security impact of changes prior to implementation for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance is able to support analyzing the security impact of changes prior to implementation to the customer's instance of the PreVeil system. PreVeil analyzes the security impact of changes prior to implementation to the PreVeil system (PVCS). For more information, see control 3.4.4, column J.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.5	-5	Control	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes analyzing the security impact of changes prior to implementation for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance is able to support defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the customer's instance of the PreVeil system. The PreVeil system is hosted within the AWS environment and inherits physical access restrictions associated with AWS' security related to physical system access.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Configuration Management (CM)	CMMC Level 2	3.4.6	-5	Control	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes employing the principle of least functionality by configuring organizational systems to provide only essential capabilities for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance is able to support the employment of the principle of least functionality by providing only essential capabilities (i.e., user functionality is limited to non-privileged access) within the customer's instance of the PreVeil system.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.7	-5	Control	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes restricting, disabling, or preventing the use of nonessential programs, functions, ports, protocols, and services for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not allow for prevents the use of nonessential programs, functions, and services within the customer's instance of the PreVeil system. The PreVeil system prevents the use of nonessential programs, functions, ports, protocols, and services within the PreVeil system. For more information, please see the PVCS information found in column J of this control.	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.8	-5	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.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. The customer is responsible for applying 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 for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system gives the customer's organization the ability to create allow listing for the customer's instance of the PreVeil system. The PreVeil system infrastructure (PVCS) applies deny listing policies to prevent the use of unauthorized software and allow listing for the use of authorized software on the PVCS. .	Shared			0
Configuration Management (CM)	CMMC Level 2	3.4.9	-1	Control	Control and monitor user-installed software.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. The customer is responsible for controlling and monitoring user installed software for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system gives the customer's organization the ability to create allow listing for the customer's instance of the PreVeil system. The PreVeil system infrastructure (PVCS) applies deny listing policies to prevent the use of unauthorized software and allow listing for the use of authorized software on the PVCS. .	Shared			0
Identification and Authentication (IA)	CMMC Level 1	3.5.1	-5	Control	Identify information system users, processes acting on behalf of users, or devices.	Customer Responsibility: The customer is expected to assign administrators to manage the Configuration Management activities within the company's instance of PreVeil. This includes identifying system users, processes acting on behalf of users, or devices for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance identifies PreVeil users, processes acting on behalf of users or devices. The PreVeil customer instance has the ability to trace activities back to each user and device that the action was attributed to. This ability to granted to the customer's instance of PreVeil administrator and can be found within the audit logging functionality housed within the customer's instance of the PreVeil system. It is the customer's responsibility to manage system user accounts within their instance of the PreVeil system.	Shared			0
Identification and Authentication (IA)	CMMC Level 1	3.5.2	-5	Control	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system administrators are able to authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to the customer's instance of the PreVeil system. The customer's instance of the PreVeil system requires that the customer's instance of PreVeil verifies the identity of the user, processes, or devices through the user and device key management security infrastructure within the PreVeil security architecture (please see the PreVeil Security Whitepaper for more information). NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Identification and Authentication (IA)	CMMC Level 2	3.5.3	-5	Control	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes using multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance supports the use of multifactor authentication for privileged accounts and non-privileged accounts by identifying privileged and non-privileged accounts within the customer's instance of the PreVeil system.	Shared			0
Identification and Authentication (IA)	CMMC Level 2	3.5.4	-1	Control	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. The nature of the PreVeil security posture is based on device key authentication, illuminating logins and thus the likelihood of replay-resistant mechanisms being employed to gain access to the customer's instance of the PreVeil system. For more information, please see the PreVeil Security Whitepaper. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Identification and Authentication (IA)	CMMC Level 2	3.5.5	-1	Control	Prevent the reuse of identifiers for a defined period.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes preventing the reuse of identifiers for a defined period for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. For more information, please see the PreVeil Security Whitepaper.	Shared			0
Identification and Authentication (IA)	CMMC Level 2	3.5.6	-1	Control	Disable identifiers after a defined period of inactivity.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes disabling identifiers after a defined period of inactivity for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. For more information, please see the PreVeil Security Whitepaper.	Shared			0
Identification and Authentication (IA)	CMMC Level 2	3.5.7	-1	Control	Enforce a minimum password complexity and change of characters when new passwords are created.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes enforcing a minimum password complexity and change of characters when new passwords are created for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. For more information, please see the PreVeil Security Whitepaper.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Identification and Authentication (IA)	CMMC Level 2	3.5.8	-1	Control	Prohibit password reuse for a specified number of generations.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes prohibiting password reuse for a specified number of generations for all systems and endpoints in scope. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours.. For more information, please see the PreVeil Security Whitepaper.	Shared			0
Identification and Authentication (IA)	CMMC Level 2	3.5.9	-1	Control	Allow temporary password use for system logons with an immediate change to a permanent password.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes allowing temporary password use for system logons with an immediate change to a permanent password for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. For more information, please see the PreVeil Security Whitepaper.	Shared			0
Identification and Authentication (IA)	CMMC Level 2	3.5.10	-5	Control	Store and transmit only cryptographically-protected passwords.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes storing and transmitting only cryptographically-protected passwords for system logons with an immediate change to a permanent password for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. All storage and transmission of information within the customer's instance of the PreVeil system, including device key authentication, is FIPS 140-2 encrypted. For more information, please see the PreVeil Security Whitepaper.	Shared			0
Identification and Authentication (IA)	CMMC Level 2	3.5.11	-1	Control	Obscure feedback of authentication information.	Customer Responsibility: The customer is expected to assign administrators to manage the Identification and Authentication activities within the company's instance of PreVeil. This includes obscuring feedback of authentication information for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. All storage and transmission of information within the customer's instance of the PreVeil system, including device key authentication, is FIPS 140-2 encrypted. For more information, please see the PreVeil Security Whitepaper.	Shared			0
Incident Response (IR)	CMMC Level 2	3.6.1	-5	Control	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Customer Responsibility: The customer is expected to assign administrators to manage the Incident Response activities within the company's instance of PreVeil. This includes establishing an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance supports incident response handling by allowing for detection, containment, and user response activities within the customer's instance of the PreVeil system. Incident detection and analysis is supported through the PreVeil customer instance through the audit logging and reporting functionality available to the customer's instance of the PreVeil system administrators. Customer's instance of the PreVeil system administrators have the ability to contain information by removing privileges and device key access, as needed. The customer's instance of the PreVeil system supports the recovery actions deemed appropriate within the customer's incident response plan, policy, and procedures. The customer must determine and document where the customer's instance of the PreVeil system is integrated within the customer's incident response plan, policy, and procedures.	Shared			0
Incident Response (IR)	CMMC Level 2	3.6.2	-5	Control	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Customer Responsibility: The customer is expected to assign administrators to manage the Incident Response activities within the company's instance of PreVeil. The customer is responsible for tracking, documenting, and reporting incidents to designated officials and/or authorities both internal and external to the organization for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Incident Response (IR)	CMMC Level 2	3.6.3	-1	Control	Test the organizational incident response capability.	Customer Responsibility: The customer is expected to assign administrators to manage the Incident Response activities within the company's instance of PreVeil. The customer is responsible for testing the organizational incident response capability for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0
Maintenance (MA)	CMMC Level 2	3.7.1	-3	Control	Perform maintenance on organizational systems.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits maintenance from the PreVeil system, this includes performing maintenance on the PreVeil system, and thus for the customer's instance of the PreVeil system. System maintenance for the PreVeil system is partially inherited by AWS, which hosts the PreVeil system instance for all PreVeil customers. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Maintenance (MA)	CMMC Level 2	3.7.2	-5	Control	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits maintenance from the PreVeil system, this includes providing controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance on the PreVeil system, and thus for the customer's instance of the PreVeil system. System maintenance for the PreVeil system is partially inherited by AWS, which hosts the PreVeil system instance for all PreVeil customers. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Maintenance (MA)	CMMC Level 2	3.7.3	-1	Control	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Customer Responsibility: The customer is expected to assign administrators to manage the Maintenance activities within the company's instance of PreVeil. This includes ensuring equipment removed for off-site maintenance is sanitized of any CUI for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits maintenance from the PreVeil system. System maintenance for the PreVeil system is partially inherited and fully inherited by AWS, which hosts the PreVeil system instance for all PreVeil customers. For more information, please see column J of this control.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Maintenance (MA)	CMMC Level 2	3.7.4	-3	Control	Check media containing diagnostic and test programs for malicious code before the media is used in organizational systems.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits maintenance from the PreVeil system, this includes checking media containing diagnostic and test programs for malicious code before the media is used on the PreVeil system, and thus for the customer's instance of the PreVeil system. System maintenance for the PreVeil system is partially inherited by AWS, which hosts the PreVeil system instance for all PreVeil customers. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Maintenance (MA)	CMMC Level 2	3.7.5	-5	Control	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits maintenance from the PreVeil system, this includes requiring multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete on the PreVeil system, and thus for the customer's instance of the PreVeil system. System maintenance for the PreVeil system is partially inherited by AWS, which hosts the PreVeil system instance for all PreVeil customers. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Maintenance (MA)	CMMC Level 2	3.7.6	-1	Control	Supervise the maintenance activities of personnel without required access authorization.	Customer Responsibility NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits maintenance from the PreVeil system, this includes supervising the maintenance activities of personnel without required access authorization on the PreVeil system, and thus for the customer's instance of the PreVeil system. System maintenance for the PreVeil system is partially inherited by AWS, which hosts the PreVeil system instance for all PreVeil customers. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Media Protection (MP)	CMMC Level 1	3.8.3	-5	Control	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes sanitizing or destroying information system media containing Federal Contract Information (FCI) before disposal or release for reuse for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the sanitization or destruction of system media of FCI before disposal or release from reuse from the PreVeil system only for the media hosted by PreVeil (i.e., servers that host the customer's instance of the PreVeil system). All other system media that the customer uses in the processing, storing, or transmitting of FCI data is the responsibility of the customer.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.1	-3	Control	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes protecting system media containing CUI, both paper and digital for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the physical and securely stored system media containing CUI, digitally, if the customer does not use any other system media outside of the PreVeil system to digitally store CUI. If the customer keeps all CUI data in the digitally storage of the customer's instance of the PreVeil system (including the PreVeil mobile app for mobile phones), the customer inherits the digital protections of the PreVeil system. If the customer stores paper CUI, PreVeil does not have any responsibility for the safeguarding of customer paper CUI. . NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.2	-3	Control	Limit access to CUI on system media to authorized users.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes limiting access to CUI on system media to authorized users for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the physical and securely stored system media containing CUI, digitally, if the customer does not use any other system media outside of the PreVeil system to digitally store CUI. If the customer keeps all CUI data in the digitally storage of the customer's instance of the PreVeil system (including the PreVeil mobile app for mobile phones), the customer inherits the digital protections of the PreVeil system. If the customer stores paper CUI, PreVeil does not have any responsibility for the safeguarding of customer paper CUI. . NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.4	-1	Control	Mark media with necessary CUI markings and distribution limitations.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes marking media with necessary CUI markings and distribution limitations for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the physical and securely stored system media containing CUI, digitally, if the customer does not use any other system media outside of the PreVeil system to digitally store CUI. If the customer keeps all CUI data in the digitally storage of the customer's instance of the PreVeil system (including the PreVeil mobile app for mobile phones), the customer inherits the digital protections of the PreVeil system. If the customer stores paper CUI, PreVeil does not have any responsibility for the safeguarding of customer paper CUI. . PreVeil gives the customer the ability to mark information within the customer's instance of the PreVeil system with CUI markings and distribution limitations, as necessary, but it is the customer's responsibility to mark CUI information that will be accessed from the customer's instance of PreVeil appropriately. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.5	-1	Control	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes controlling access to media containing CUI and maintain accountability for media during transport outside of controlled areas for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the physical and securely stored system media containing CUI, digitally, if the customer does not use any other system media outside of the PreVeil system to digitally store CUI. If the customer keeps all CUI data in the digitally storage of the customer's instance of the PreVeil system (including the PreVeil mobile app for mobile phones), the customer inherits the digital protections of the PreVeil system, as well as the ability to control access to information on the customer's instance of the PreVeil system and associated system media (i.e., PreVeil mobile application for mobile devices). If the customer stores paper CUI, PreVeil does not have any responsibility for the safeguarding of customer paper CUI. . PreVeil gives the customer the ability to mark information within the customer's instance of the PreVeil system with CUI markings and distribution limitations, as well as controlling user access via access and device controls, as necessary, but it is the customer's responsibility to mark CUI information that will be accessed from the customer's instance of PreVeil, appropriately. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Media Protection (MP)	CMMC Level 2	3.8.6	-1	Control	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes implementing cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the physical and securely stored, FIPS 140-2 (PreVeil NIST FIPS 140-2 certification can be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804) E2EE of system media containing CUI, digitally, if the customer does not use any other system media outside of the PreVeil system to digitally store CUI. If the customer keeps all CUI data in the digitally storage of the customer's instance of the PreVeil system (including the PreVeil mobile app for mobile phones), the customer inherits the digital protections of the PreVeil system, as well as the ability to control access to information on the customer's instance of the PreVeil system and associated system media (i.e., PreVeil mobile application for mobile devices). If the customer stores paper CUI, PreVeil does not have any responsibility for the safeguarding of customer paper CUI. . PreVeil gives the customer the ability to mark information within the customer's instance of the PreVeil system with CUI markings and distribution limitations, as well as controlling user access via access and device controls, as necessary, but it is the customer's responsibility to mark CUI information that will be accessed from the customer's instance of PreVeil, appropriately. It is also the customer's responsibility to ensure that any digital media that is transported outside the PreVeil system is protected during transport, cryptographically. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.7	-5	Control	Control the use of removable media on system components.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes controlling the use of removable media on system components for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits control of the use of removable media on the PreVeil system and PreVeil system components. It is the customer's responsibility to ensure that all system and system components processing, storing, and/or transmitting CUI are controlled regarding their use of removable media on system components outside of the PreVeil system (i.e., endpoint management). NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.8	-3	Control	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes prohibiting the use of portable storage devices when such devices had no identifiable owner for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits control of the use of removable media on the PreVeil system and PreVeil system components regarding portable storage devices with no identifiable owner. It is the customer's responsibility to ensure that all system and system components processing, storing, and/or transmitting CUI are controlled regarding their use of removable media on system components outside of the PreVeil system (i.e., endpoint management). NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Media Protection (MP)	CMMC Level 2	3.8.9	-1	Control	Protect the confidentiality of backup CUI at storage locations.	Customer Responsibility: The customer is expected to assign administrators to manage the Media Protection activities within the company's instance of PreVeil. This includes protecting the confidentiality of backup CUI at storage locations for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the physical and securely stored, FIPS 140-2 (PreVeil NIST FIPS 140-2 certification can be found here: HTTPs://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. E2EE of system media containing CUI, digitally, if the customer does not use any other system media outside of the PreVeil system to digitally store CUI. The PreVeil customer's instance inherits control of the use of removable media on the PreVeil system and PreVeil system components regarding protecting the confidentiality of backup CUI at storage locations. It is the customer's responsibility to ensure that all system and system components processing, storing, and/or transmitting CUI are controlled regarding their use of removable media on system components outside of the PreVeil system (i.e., endpoint management). NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared			0
Personnel Security (PS)	CMMC Level 2	3.9.1	-3	Control	Screen individuals prior to authorizing access to organizational systems containing CUI.	Customer Responsibility: The customer is expected to assign administrators to manage the Personnel Security activities within the company's instance of PreVeil. This includes screening individuals prior to authorizing access to organizational systems containing CUI for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system is hosted within the PreVeil system, which is hosted through AWS GovCloud. AWS GovCloud is FedRAMP High authorized and screens all US-only persons to gain access to any equipment and applications used in the hosting requirements of the PreVeil system. Neither PreVeil nor AWS ever have access to customer CUI data due to the FIPS 140-2 encryption used within the PreVeil system. The PreVeil FIPS 140-2 certification can be found here: HTTPs://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Personnel Security (PS)	CMMC Level 2	3.9.2	-5	Control	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Customer Responsibility: The customer is expected to assign administrators to manage the Personnel Security activities within the company's instance of PreVeil. This includes ensuring that organizational systems containing CUI are protected during and after personnel actions, such as terminations and transfers, for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance provides the customer the ability to remove personnel access to the customer's instance of the PreVeil system, as needed, following terminations and/or transfers. The customer instance of the PreVeil system allow for customer instances of the PreVeil system administrators to remove access to any and all personnel, ad hoc, and ensure that devices with PreVeil system access are removed, as well as removing any elevated privileges, as necessary.	Shared			0
Physical Protection (PE)	CMMC Level 1	3.10.1	-5	Control	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits all physical access to PreVeil equipment and operating environments, including limiting physical access to organizational information systems equipment and the respective operating environments to authorized individuals, as part of the PreVeil infrastructure from the PreVeil system, which inherits these physical controls from AWS (the PreVeil hosting environment). For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Physical Protection (PE)	CMMC Level 1	3.10.3	-1	Control	Escort visitors and monitor visitor activity.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits all physical access to PreVeil equipment and operating environments, including escorting visitors and monitoring visitor activity, as part of the PreVeil infrastructure from the PreVeil system, which inherits these physical controls from AWS (the PreVeil hosting environment). For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Physical Protection (PE)	CMMC Level 1	3.10.4	-1	Control	Maintain audit logs of physical access.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits all physical access to PreVeil equipment and operating environments, including maintaining audit logs of physical access, as part of the PreVeil infrastructure from the PreVeil system, which inherits these physical controls from AWS (the PreVeil hosting environment). For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Physical Protection (PE)	CMMC Level 1	3.10.5	-1	Control	Control and manage physical access devices.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits all physical access to PreVeil equipment and operating environments, including controlling and managing physical access devices, as part of the PreVeil infrastructure from the PreVeil system, which inherits these physical controls from AWS (the PreVeil hosting environment). For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Physical Protection (PE)	CMMC Level 2	3.10.2	-5	Control	Protect and monitor the physical facility and support infrastructure for organizational systems.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits all physical access to PreVeil equipment and operating environments, including protecting and monitoring they physical facility and support infrastructure, as part of the PreVeil infrastructure from the PreVeil system, which inherits these physical controls from AWS (the PreVeil hosting environment). For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Physical Protection (PE)	CMMC Level 2	3.10.6	-1	Control	Enforce safeguarding measures for CUI at alternate work sites.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits all physical access to PreVeil equipment and operating environments, including enforcing safeguarding measures for CUI at alternate work sites, as part of the PreVeil infrastructure from the PreVeil system, which inherits these physical controls from AWS (the PreVeil hosting environment). For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
Risk Assessment (RM)	CMMC Level 2	3.11.1	-3	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.	Customer Responsibility: The customer is expected to assign administrators to manage the Risk Assessment activities within the company's instance of PreVeil. This includes periodically assessing the risk to organizational operations (including mission, functions, images, or reputations), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, and/or transmission of CUI for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the risk assessments to the organization via the PreVeil system from PreVeil. The customer is still responsible for all risk assessments required to satisfy this control regarding internal organizational risk and assessments that are not directly related to the PreVeil system. Only the PreVeil system related risk assessment portion is inherited by the customer for their customer instance of the PreVeil system.	Shared			0
Risk Assessment (RM)	CMMC Level 2	3.11.2	-5	Control	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Customer Responsibility: The customer is expected to assign administrators to manage the Risk Assessment activities within the company's instance of PreVeil. This includes scanning for vulnerabilities in organizational systems and applications, periodically, and when new vulnerabilities affecting those systems and applications are defined for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the vulnerability scans for the PreVeil system from PreVeil. The customer is still responsible for all vulnerability scans required to satisfy this control regarding other systems and endpoints that are not directly related to the PreVeil system. Only the PreVeil system related vulnerability scanning portion is inherited by the customer for their customer instance of the PreVeil system.	Shared			0
Risk Assessment (RM)	CMMC Level 2	3.11.3	-1	Control	Remediate vulnerabilities in accordance with risk assessments.	Customer Responsibility: The customer is expected to assign administrators to manage the Risk Assessment activities within the company's instance of PreVeil. This includes remediating vulnerabilities in accordance with risk assessments for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the vulnerability scans and remediation for the PreVeil system from PreVeil. The customer is still responsible for all vulnerability scans and remediation required to satisfy this control regarding other systems and endpoints that are not directly related to the PreVeil system. Only the PreVeil system related vulnerability scanning and remediation portion is inherited by the customer for their customer instance of the PreVeil system.	Shared			0
Security Assessment (CA)	CMMC Level 2	3.12.1	-5	Control	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Customer Responsibility: The customer is expected to assign administrators to manage the Security Assessment activities within the company's instance of PreVeil. This includes periodically assessing the security controls in organizational systems to determine if the controls are effective in their application for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the periodic assessment of the security controls in the PreVeil system to determine if the controls are effective in their application for the PreVeil system from PreVeil. The customer is still responsible for all assessments of security controls in organizational systems required to satisfy this control regarding other systems and endpoints that are not directly related to the PreVeil system. Only the PreVeil system related period assessment of security controls portion is inherited by the customer for their customer instance of the PreVeil system.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
Security Assessment (CA)	CMMC Level 2	3.12.2	-3	Control	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Customer Responsibility: The customer is expected to assign administrators to manage the Security Assessment activities within the company's instance of PreVeil. This includes developing and implementing plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil has developed and implemented plans of actions designed to correct deficiencies and reduce or eliminate vulnerabilities in the PreVeil system. The customer's instance of PreVeil inherits the development and implementation of plans of actions within the PreVeil system, only. The customer is responsible for all development and implementation of plans of actions designed to correct deficiencies and reduce or eliminate vulnerabilities in their organizational systems outside of the customer's instance of the PreVeil system.	Shared			0
Security Assessment (CA)	CMMC Level 2	3.12.3	-5	Control	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Customer Responsibility: The customer is expected to assign administrators to manage the Security Assessment activities within the company's instance of PreVeil. This includes monitoring security controls on an ongoing basis to ensure continued effectiveness of the controls for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil monitors security controls on an ongoing basis to ensure continued effectiveness of the control within the PreVeil system. Customers inherit this control only as it pertains to the customer's instance of the PreVeil system. Customers are responsible for addressing the monitoring of security controls for their organization and other organizational systems in use by the customer.	Shared			0
Security Assessment (CA)	CMMC Level 2	3.12.4	-5	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: The customer is expected to assign administrators to manage the Security Assessment activities within the company's instance of PreVeil. The customer is responsible for developing, documenting, and periodically updating 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 for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0
System and Communications Protection (SC)	CMMC Level 1	3.13.1	-5	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.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes monitoring, controlling, and protecting organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil monitors, controls, and protects PreVeil system communications (i.e., information transmitted or received by the PreVeil system) at the external boundaries and key internal boundaries of the PreVeil system. The customer inherits this monitoring, controlling, and protection of communications as it pertains to the customer's instance of the PreVeil system, only. All other communications and boundary definitions will be the responsibility of the customer to address for all systems and applications, outside of the customer's instance of the PreVeil system, within scope of this control.	Shared			0
System and Communications Protection (SC)	CMMC Level 1	3.13.5	-5	Control	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes implementing subnetworks for publicly accessible system components that are physically or logically separated from internal networks for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil has implemented subnetworks for publicly accessible system components that are physically or logically separated from internal networks used by the PreVeil system. The customer's instance of the PreVeil system is physically and logically separated from publicly accessible system components, unless otherwise configured by the customer to remove that physical and logical separation. By default, the customer's instance of PreVeil will not touch any publicly accessible system components. The PreVeil system does not allow for the interaction of the PreVeil system and/or system components with publicly accessible system components.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
System and Communications Protection (SC)	CMMC Level 2	3.13.2	-5	Control	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the employing of architectural designs, software development, techniques, and system engineering principles that promote effective information security, as part of the PreVeil infrastructure from the PreVeil system. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.3	-1	Control	Separate user functionality from system management functionality.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance inherits the separation of user functionality from system management functionality, as part of the PreVeil infrastructure from the PreVeil system. For more information, please see column J of this control. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.4	-1	Control	Prevent unauthorized and unintended information transfer via shared system resources.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes preventing unauthorized and unintended information transfer via shared system resources for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system grants all users their own account information and access. For shared system resources, the customer can work with PreVeil support to establish these unique accounts, with separated access, on shared devices, as needed. It is the customer's responsibility to ensure that unauthorized and unintended information transfers are prevented via shared system resources outside of PreVeil and to work with PreVeil support to set up the solution for the customer's instance of the PreVeil system on shared system resources.	Shared			0
System and Communications Protection (SC)	CMMC Level 2	3.13.6	-5	Control	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes preventing unauthorized and unintended information transfer via shared system resources for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system can be configured to deny network communications traffic by default and allow network communications traffic by expectation. The customer's instance of the PreVeil system has allow listing capabilities that can be set up by the customer within their instance of PreVeil. It is the customer's responsibility to deny network communications by default and allow by exception on all customer systems outside of the customer's instance of the PreVeil system.	Shared			0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
System and Communications Protection (SC)	CMMC Level 2	3.13.7	-1	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).	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system grants the ability to prevent remote devices from simultaneously establishing non-remote connections with organizational systems as communicating via some other connection to resources in external networks (i.e., split tunneling). The PreVeil system is not accessed via VPN and is end-to-end encrypted making split tunneling not possible within the PreVeil system. The customer inherits this control from the PreVeil system for the customer's instance of the PreVeil system. NOTE: There may be customer responsibility, within this control, if there are other systems that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary or additional VPNs in use by the customer that may be considered in scope.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.8	-3	Control	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system ensures FIPS 140-2 validated and certified cryptographic protection for all CUI stored and transmitted within the customer's instance of the PreVeil system. The PreVeil system is FIPS 140-2 certified by NIST. The NIST FIPS 140-2 certification can be found here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.9	-1	Control	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. In addition, PreVeil grants the customer's instance of PreVeil administrators the ability to manually remove user access to PreVeil either ad hoc or through setting a time limit for access to information on the system (i.e., user will only have access through a certain date). NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
System and Communications Protection (SC)	CMMC Level 2	3.13.10	-1	Control	Establish and manage cryptographic keys for cryptography employed in organizational systems.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil customer's instance does not use traditional identifiers based on the security infrastructure of the PreVeil system. PreVeil uses user key and device key authentication, not traditional user name and password logins, to authenticate sessions into the customer's instance of the PreVeil system. Device keys are automatically regenerated with a new encryption key every 24 hours. In addition, PreVeil grants the customer's instance of PreVeil administrators the ability to manually remove user access to PreVeil either ad hoc or through setting a time limit for access to information on the system (i.e., user will only have access through a certain date). The PreVeil system (and all customer data transmitted and stored within the customer's instance of the PreVeil system) is cryptographically protected using FIPS 140-2 validated and certified encryption. See the PreVeil FIPS 140-2 NIST certification here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. PreVeil cryptographic keys are managed for the customer's instance of PreVeil through the customer authorized devices and users established by the customer as part of the customer's access control policies and procedures. The customer administrators, users, and PreVeil system resources do not have access to the customer's instance of the PreVeil system device level keys, at any time. For more information, please see the PreVeil Security Whitepaper. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.11	-5	Control	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system (and all customer data transmitted and stored within the customer's instance of the PreVeil system) is cryptographically protected using FIPS 140-2 validated and certified encryption. See the PreVeil FIPS 140-2 NIST certification here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. PreVeil cryptographic keys are managed for the customer's instance of PreVeil through the customer authorized devices and users established by the customer as part of the customer's access control policies and procedures. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.12	-1	Control	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. The customer is responsible for prohibiting remote activation of collaborative computing devices and provide indication of devices in use to users present at the devices for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
System and Communications Protection (SC)	CMMC Level 2	3.13.13	-1	Control	Control and monitor the use of mobile code.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system is controlled and monitored for the use of mobile code through the PreVeil system, thus the customer's instance of the PreVeil system inherits this control from the PreVeil system. PreVeil ensures that the use of mobile code is limited to only PreVeil CISO authorized business essential purposes. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.14	-1	Control	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. The customer is responsible for controlling and monitoring the use of Voice over Internet Protocol (VoIP) technologies for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: N/A	Customer Responsibility	This control is always a Customer Responsibility. This control is out of the scope of the PreVeil system.		0
System and Communications Protection (SC)	CMMC Level 2	3.13.15	-5	Control	Protect the authenticity of communications sessions.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The customer's instance of the PreVeil system communications session are cryptographically protected using FIPS 140-2 validated and certified encryption. See the PreVeil FIPS 140-2 NIST certification here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. PreVeil cryptographic keys are managed for the customer's instance of PreVeil through the customer authorized devices and users established by the customer as part of the customer's access control policies and procedures. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/ or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
System and Communications Protection (SC)	CMMC Level 2	3.13.16	-1	Control	Protect the confidentiality of CUI at rest.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: The PreVeil system (and all customer data transmitted and stored within the customer's instance of the PreVeil system) is cryptographically protected using FIPS 140-2 validated and certified encryption. See the PreVeil FIPS 140-2 NIST certification here: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3804. PreVeil cryptographic keys are managed for the customer's instance of PreVeil through the customer authorized devices and users established by the customer as part of the customer's access control policies and procedures. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Information Integrity (SI)	CMMC Level 1	3.14.1	-5	Control	Identify, report, and correct information and information system flaws in a timely manner.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system and subsequently the customer's instance of the PreVeil system, identifies, reports, and corrects information and information system flaws in a timely manner as they pertain to the PreVeil system. . NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Information Integrity (SI)	CMMC Level 1	3.14.2	-5	Control	Provide protection from malicious code at appropriate locations within organizational information systems.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes identifying, reporting, and correcting information and information system flaws in a timely manner for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system and subsequently the customer's instance of the PreVeil system provides protection from malicious code at appropriate locations within the PreVeil system, thus the customer's instance of PreVeil inherits this control from the PreVeil system. . NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary.	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0

PreVeil Shared Responsibility Matrix Controls and Objectives	**Directions for using this document:** This document outlines the shared responsbilities between PreVeil, a Cloud Service Provider (CSP) an PreVeil customers who are seeking NIST 800-171/CMMC compliance. This document is to be used as a tool to help identify gaps within your compliance boundary that may remain, after installing the PreVeil system. Please note that PreVeil is not responsible for any customer's inability to completely implement all of their relevant compliance requirements. The responsbiility to complete all compliance requirements, ultimately falls on PreVeil customers.	**Projected SPRS Score** **Note:** This score is not official in anyway and is only to be used as guidance through your compliance journey. PreVeil is not responsible for any customer who does not complete all the steps to compliance required of them. ***Always do your due diligence to review all controls implementation, regardless of the projected score listed on this document.*** PreVeil is not responsible for any customer's failure to address all of their applicable compliance requirements.	**-203**

Shared	In addition to the "Customer's Responsibility Statement" column statements listed below for each control, 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.
Shared*	As long as all items listed in the "Customer's Responsibility Statement" column below for the control are fully implemented, PreVeil addresses the control/objective. ***NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI.***
Customer Responsibility	The customer will be responsible 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 Assessment Level	NIST SP 800-171	SPRS Point(s) Value	Objective or Control	Practice Statement/Objective	PreVeil Specific Customer Responsibilities for Use of PreVeil System	PreVeil Customer Responsibility Status	Customer's Responsibility Statement	Customer's Implementation Status	Customer's Current SPRS Score- for Control
System and Information Integrity (SI)	CMMC Level 1	3.14.4	-5	Control	Update malicious code protection mechanisms when new releases are available.	Customer Responsibility: NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system and subsequently the customer's instance of the PreVeil system updates malicious code protection mechanisms when new releases are available, as it pertains to the PreVeil system, thus the customer inherits this control for their instance of the PreVeil system from the PreVeil system. . The customer is responsible for updating malicious code protection mechanisms when new releases are available (outside of the customer's instance of the PreVeil system) for all systems and endpoints within the organization. NOTE: There may be customer responsibility, within this control, if there are other systems or system media that are in use concerning the processing, transmission, and storing of CUI within the customer's assessment boundary	Shared*	This control can be considered PreVeil Inherited provided that: 1. The Customer ensures that **ALL** endpoints that are processing, storing, and/or transmitting CUI are compliantly secured. For more information on compliantly securing your endpoint, please see the PreVeil endpoint checklist in the PreVeil Compliance Accelerator. 2. The Customer ensures that **ALL** CUI is stored and transmitted inside the PreVeil system and nowhere else on the Customer's system. If there is CUI being processed, stored, and/or transmitted outside of the PreVeil system, the Customer will need to ensure that system outside of PreVeil that is processing, storing, and/or transmitting CUI is compliantly secured. 3. The Customer ensures that **ALL** relevant policies, procedures, artifacts, and evidence needed to consider this control/objective fully implemented by a 3rd party assessor are fully implemented.		0
System and Information Integrity (SI)	CMMC Level 1	3.14.5	-3	Control	Perform periodic scans of the information system and real- time scans of files from external sources as files are downloaded, opened, or executed.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes performing periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system and subsequently the customer's instance of the PreVeil system perform periodic scans of the PreVeil system and real time scans of files from external sources as files are downloaded, opened, or executed, as it pertains to the PreVeil system. PreVeil does not scan files that are downloaded or opened from the customer's instance of the PreVeil system to the customer's endpoints. . The customer is responsible for perform periodic scans of the information system and real time scans of files from external sources as files are downloaded, opened, or executed (outside of the customer's instance of the PreVeil system) for all systems and endpoints within the organization.	Shared			0
System and Information Integrity (SI)	CMMC Level 2	3.14.3	-5	Control	Monitor system security alerts and advisories and take action in response.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes monitoring system security alerts and advisories and taking action in response for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system monitors system security alerts and advisories and takes action in response, as it pertains to the PreVeil system. . PreVeil provides system security alerts and advisors, monthly, to all registered PreVeil users that may be used to help satisfy this control. It is the responsibility of the customer to take those system security alerts and advisories under consideration and act, as necessary, for all systems and endpoints within the organization.	Shared			0
System and Information Integrity (SI)	CMMC Level 2	3.14.6	-5	Control	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes monitoring organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks, for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system monitors PreVeil organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks, as it pertains to the PreVeil system. . It is the responsibility of the customer to monitor customer organizational systems (outside of the customer's instance of the PreVeil system), including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks, for all systems and endpoints within the organization.	Shared			0
System and Information Integrity (SI)	CMMC Level 2	3.14.7	-3	Control	Identify unauthorized use of organizational systems	Customer Responsibility: The customer is expected to assign administrators to manage the System and Communications Protection activities within the company's instance of PreVeil. This includes identifying unauthorized use of organizational systems for all systems and endpoints in scope. NOTE: Customers will still be responsible for the management of their CUI accessing endpoints, administration of their instance of the PreVeil software (i.e., adding new users, removing users, running internal audit logs, etc.), and ensuring that they do their due diligence in adding any additional CUI assets, security protection assets (SPAs), and other systems that may be processing (accessing), storing, and/or transmitting CUI. PreVeil Responsibility: PreVeil ensures that the PreVeil system identifies unauthorized use of PreVeil organizational systems, as it pertains to the PreVeil system. . It is the responsibility of the customer to identify unauthorized use of organizational systems (outside of the customer's instance of the PreVeil system), for all systems and endpoints within the organization.	Shared			0
						362	Shared*			
						68	Customer Responsibility			
						641	Total			

Appendix B: How PreVeil Saves 75% vs. Microsoft GCC High

Many higher education institutions rely on Microsoft 365 Commercial for their email and file storage needs. But that platform is not DoD compliant for handling CUI, a point that Microsoft readily acknowledges—and so recommends that institutions upgrade to GCC High. But GCC High is very expensive, disruptive and time consuming to install, and doesn't allow you to communicate with users outside of GCC High.

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."**

A Vice President of Operations for a defense contractor using PreVeil that achieved the highest possible score of 110 out of 110 on a CMMC Level 2 assessment summed it up well:

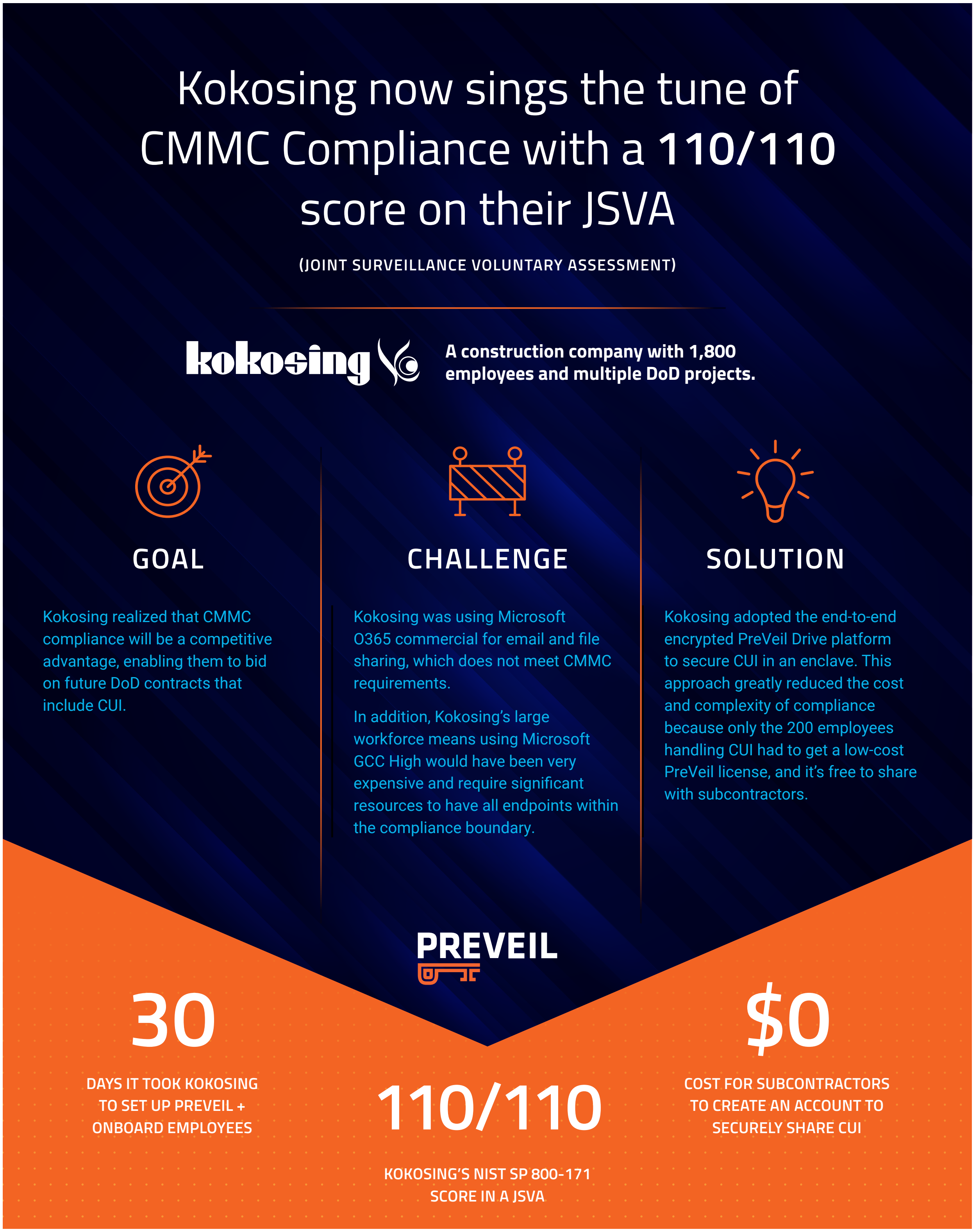
> **"When it comes to speed to compliance and cost, PreVeil is undoubtedly the right decision. We got it done on time and on budget, saving $200,000 compared to GCC High... If you care about being on time, GCC High is a much bigger risk than PreVeil."**

PreVeil's cost savings derive from a wide range of its features, from seamless deployment to free third-party collaboration, extensive compliance support and more—all without compromising security, as summarized in the following chart:

HOW PREVEIL SAVES 75% VS. MICROSOFT GCC HIGH AND OFFERS HIGHEST SECURITY LEVEL

	PREVEIL	MICROSOFT GCC HIGH
PRODUCT	**Email and File Sharing**	**Email and File Sharing**
COST	Low cost. PreVeil licenses are significantly more affordable than GCC High, and fewer licenses are needed, since you can limit to only users that access CUI. This results in a typical customer saving 75% vs GCC High.	High cost and complex. Upgrading to GCC High involves extensive planning, new infrastructure, business disruption, and higher license fees. Typically deployed across entire organization.
DEPLOYMENT	Integrates seamlessly with existing IT environments without rip and replace, saving time and money. No impact to existing file servers and users keep their regular email address.	Expensive and time-consuming rip and replace of file server and domain. Difficult to integrate with higher education's diverse computing environments, leading to compatibility issues and fragmented communication across the organization.
THIRD-PARTY COLLABORATION	Third parties can create free PreVeil accounts, enabling secure communication within minutes.	Cannot communicate with users outside of GCC High. Instead, expensive and difficult-to-manage guest licenses are required, adding admin burdens on IT team.
COMPLIANCE DOCUMENTATION SUPPORT	Save tens of thousands of dollars with pre-filled documentation including a System Security Plan, Standard Operating Procudures, POAM templates and. Plus, C3PAO-validated videos and 1×1 support from our compliance experts if you get stuck.	Institutions must develop their own documentation—a time-consuming and costly challenge given the complex configuration of the system.
MAINTENANCE	Simplified maintenance. Fewer software patches mean less time spent on maintenance and updating compliance documentation.	Frequent patches and updates required place significant burden on IT teams and divert their time from other critical tasks.
SECURITY		
ZERO TRUST	Built on Zero Trust principles as recommended by NSA.	Relies on legacy perimeter-based defenses.
ENCRYPTION	End-to-end encryption. No one but the intended recipient—including PreVeil—can ever read users' messages and files.	Optional enhanced encryption uses a key server, creating a vulnerable central point of attack.
AUTHENTICATION	Key-based authentication that eliminates passwords. Keys can't be guessed or stolen.	Uses passwords, increasing vulnerability to password theft and brute-force attacks.
ADMIN PROTECTION	Admin Approval Groups ensure that no single admin can compromise the enterprise	Administrators have full access to all data, creating a security risk
TRUSTED LISTS	Trusted Communities feature restricts communication to pre-specified domains and email addresses.	N/A—users' email exposed to untrusted phishing and spoofing attacks.

Appendix C: Case Study—Contractor using PreVeil achieves CMMC level 2 compliance with perfect 110 score on JSVA



Kokosing now sings the tune of CMMC Compliance with a **110/110** score on their JSVA

(JOINT SURVEILLANCE VOLUNTARY ASSESSMENT)

kokosing

A construction company with 1,800 employees and multiple DoD projects.

GOAL

Kokosing realized that CMMC compliance will be a competitive advantage, enabling them to bid on future DoD contracts that include CUI.

CHALLENGE

Kokosing was using Microsoft O365 commercial for email and file sharing, which does not meet CMMC requirements.

In addition, Kokosing's large workforce means using Microsoft GCC High would have been very expensive and require significant resources to have all endpoints within the compliance boundary.

SOLUTION

Kokosing adopted the end-to-end encrypted PreVeil Drive platform to secure CUI in an enclave. This approach greatly reduced the cost and complexity of compliance because only the 200 employees handling CUI had to get a low-cost PreVeil license, and it's free to share with subcontractors.

PREVEIL

30

DAYS IT TOOK KOKOSING TO SET UP PREVEIL + ONBOARD EMPLOYEES

110/110

KOKOSING'S NIST SP 800-171 SCORE IN A JSVA

$0

COST FOR SUBCONTRACTORS TO CREATE AN ACCOUNT TO SECURELY SHARE CUI

Why PreVeil?

HERE'S WHY PREVEIL WAS A GREAT FIT FOR KOKOSING:

AFFORDABLE	EASY IMPLEMENTATION + USABILITY	COMPLIANT
Only users in the CUI enclave need low-cost PreVeil licenses	Kokosing set up, onboarded, and trained their employees on PreVeil in 30 days!	PreVeil meets all CMMC requirements, including FedRAMP Equivalency, FIPS, and DFARS 7012 (c-g)

Perfect JSVA score transfers to CMMC Level 2 certification

Kokosing's perfect JSVA score will be directly transferable to CMMC Level 2 certification when CMMC is finalized.

Moreover, they are now in a great position to maintain existing DoD contracts and win future contracts.

Additional PreVeil benefits:

PROVEN SOLUTION, DOCUMENTATION PACKAGE, AND BEST-IN-CLASS SECURITY

A rapidly growing number of PreVeil customers have achieved 110/110 scores in CMMC Joint Surveillance Assessments, which is the ultimate validation of PreVeil's compliance assurance, best-in-class security and low cost for defense contractors.

> Cost was a big factor for why we chose PreVeil. We also loved the ease of implementation and how easy it was to teach a user how to use PreVeil … You put those together and it was a very simple decision to make.
>
> — MICHAEL CREAGER, IT DIRECTOR @ KOKOSING

PREVEIL

To learn how PreVeil can help your organization improve its NIST SP 800-171 score and achieve CMMC compliance, book a free 15-minute call with our compliance team.