# Case Study: Defense contractor achieves 110/110 score in NIST SP 800-171 DoD audit

## *Demonstrates CMMC Level 2 compliance*

### THE AUDIT

The Defense Contract Management Agency (DCMA) randomly selected the SMB in this case study for an audit, for which it was given five months' notice to prepare. The SMB was asked to demonstrate that it meets its existing contractual DFARS obligations for complying with NIST SP 800-171 security controls. The SMB is a typical defense contractor: the company has been in business for 15 years and has fewer than 100 employees. Understandably, they were deeply concerned about the time, complexity and expense associated with the audit process, as well as with showing compliance. Typically, it takes a year to prepare for an audit of this kind, but the SMB got it done in five months with the help of an expert compliance consultant from PreVeil's partner network.

**A SMALL TO MID-SIZE (SMB) DEFENSE CONTRACTOR** using PreVeil for storing and sharing Controlled Unclassified Information (CUI) achieved the highest possible score of 110 on a rigorous NIST SP 800-171 audit. The SMB deployed PreVeil as an overlay of its Microsoft 365 Commercial environment, which it continued to use for other business. The audit was conducted by the US Department of Defense's (DoD) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), the DoD's ultimate authority on compliance. And because the principal requirement for certification at CMMC 2.0 Level 2 (Advanced) is to achieve compliance with NIST SP 800-171's 110 security controls, the contractor also demonstrated they have met the new Level 2 security requirements for CMMC 2.0.

It is important to understand that Microsoft 365 Commercial Email and One Drive, as well as most Google Workspace and Exchange environments, do not meet all the necessary DoD requirements for handling CUI. On the other hand, PreVeil—an encrypted file sharing and email platform for storing and sharing CUI—is designed to comply with DFARS, NIST, CMMC and ITAR requirements. This brief describes how an actual SMB defense contractor using Microsoft 365 and a PreVeil overlay achieved NIST SP 800-171 compliance simply and cost effectively, and demonstrated CMMC Level 2 compliance in the process.

**CYBERSECURITY ENFORCEMENT RAMPING UP**

DIBCAC can select any contractor for an audit, and has been increasing its audit staff. The Department of Justice (DoJ) also has raised the stakes for compliance with the launch of its Civil Cyber-Fraud Initiative. DoJ is utilizing the power of the False Claims Act to help enforce cybersecurity compliance and is encouraging whistleblowers to come forward. A new DoJ task force will focus on investigating reports of contractors choosing to withhold reports of breaches or that falsify claims of self-assessment scores. The consequences of withholding information or submitting false scores are severe.

## Why your NIST SP 800-171 score matters

Defense contractors have been required to self-assess their compliance with NIST SP 800-171 since 2017, and since 2020 the DoD has required that defense contractors file those scores with the DoD's Supplier Performance Risk System, known as SPRS. If a company has a low self-assessment score, it stands to reason that the DoD will consider that company to be a higher security risk than an alternative supplier with a better score. Likewise, primes will consider self-assessment scores when evaluating possible subcontractors with which to work, and it is reasonable to expect that subcontractors with higher scores are more likely to win the work. The SMB in this case study was able to file a score of 110, the highest possible NIST SP 800-171 score.

## PreVeil's proven ability to comply with DFARS, NIST, CMMC and ITAR requirements

Given the critical importance of achieving compliance with NIST SP 800-171—which the National Institute of Techology and Standards (NIST) developed specifically to protect CUI—it is important for SMBs to derisk their compliance iniatives by choosing only proven technology solutions for securely handling CUI. Solution providers should be able to present strong evidence of their ability to help defense contractors comply with federal regulations. In this actual case study of a DIBCAC audit of an SMB, PreVeil proves its ability to do just that.

Rigorous and objective evidence of how PreVeil helps defense contractors achieve compliance is shown in the table on the next page.

As this case study shows, compliance with NIST SP 800-171 will make compliance under CMMC 2.0 much simpler because the new CMMC Level 2 will require demonstration of compliance with the very same 110 NIST SP 800-171 security controls. Failure to comply with NIST SP 800-171 now, in advance of CMMC, can subject contractors to severe financial penalties and criminal liabilities if an audit uncovers any misrepresentation of compliance, or if a whistleblower flags security gaps. (See related sidebar.) The SMB in this case study took the necessary steps toward NIST SP 800-171 compliance prior to its DIBCAC audit and had no such problems.

The key takeaways for defense contractors are to work on improving implementation of NIST SP 800-171's security controls—which they're already required to implement under current DFARS regulations—and to choose only a proven technology solution to help them do so.

| Existing DFARS contractual obligations and CMMC 2.0 Level 2 require defense contractors to: | Evidence that the SMB defense contractor in the case study met these requirements using PreVeil: |
|---|---|
| Comply with NIST SP 800-171's 110 security controls, conduct a self-assessment of that compliance, and submit the self-assessment score to the DoD's Supplier Performance Risk System (SPRS). Note that defense contractors have been required to comply with NIST SP 800-171 as part of their DFARS contract obligations since 2017, and to report those scores since 2020. The new CMMC Level 2 security controls will mirror those of NIST SP 800-171, and so Level 2 will essentially require contractors to demonstrate compliance with their already existing contractual commitments. | Upon completion of a rigorous DIBCAC audit for NIST SP 800-171 compliance and fulfillment of their Plan of Actions & Milestones (POA&M) soon thereafter, the SMB defense contractor demonstrated compliance with all 110 NIST SP 800-171 security controls. Deployment of PreVeil as on overlay on Microsoft 365 helped the contractor comply with 84 security controls, in conjunction with policies and procedure documentation. As required, the contractor submitted its NIST SP 800-171 audit score—a highest possible 110—to the DoD's Supplier Performance Risk System (SPRS). |
| Meet applicable FedRAMP standards: if a cloud system is used for handling CUI, the cloud service providers must be certified at FedRAMP Baseline Moderate or Equivalent. | PreVeil meets FedRAMP Baseline Moderate Equivalent with attestation from an Accredited FedRAMP 3PAO (3rd Party Audit Organization). It achieved this attestation upon the successful completion of an independent audit. PreVeil formally received acceptance from the CIO and CISO of the DoD that FedRAMP Moderate Equivalency may be established via an audit by an accredited 3PAO. As the designation indicates, FedRAMP Baseline Moderate Equivalent is the same as being assessed at FedRAMP Baseline Moderate; that is, from a security and compliance viewpoint and as far as the DoD is concerned, the two are the same. |
| Meet FIPS 140-2 Validated Encryption standards when handling CUI. | PreVeil achieved FIPS 140-2 validation from the Cryptographic Module Validation Program (CMVP), ensuring that the PreVeil system is FIPS compliant. See PreVeil's FIPS 140-2 certificate on NIST's Computer Security Resource website here. |
| Comply with Defense Federal Acquisition Regulation (DFARS) 252.204-7012, which all contractors that handle CUI are currently subject to. This includes 7012 (c)-(g), which stipulate requirements for cyber incident reporting. | PreVeil meets DFARS 252.204-7012 requirements by storing all CUI encrypted data on the Amazon Web Services (AWS) Gov Cloud, which is assessed at FedRAMP High. Further, PreVeil meets 7012 (c)-(g) by managing all logs and forensic information for reporting, and making them available to the DoD upon request to assist with investigations of cyber incidents. |
| Demonstrate compliance by documenting adherence to NIST SP 800-171 controls, along with appropriate policies and procedures, in a System Security Plan (SSP). An SSP is a prerequisite for any work for the DoD. | To simplify demonstration of compliance, PreVeil offers its customers a comprehensive compliance documentation package that includes an SSP template. The template is pre-filled to reflect PreVeil's capabilities and the NIST SP 800-171 security controls it meets, along with relevant procedures. The package also includes policy templates for the NIST SP 800-171 control families, along with additional required documentation. The SMB in this case study began with a rudimentary SSP about 25 pages long; by the time of its audit, its SSP was approximately 225 pages long—and satisfied the DIBCAC auditors. |

Note that defense contractors that need to meet International Traffic in Arms Regulations (ITAR) can use the same PreVeil system to support their compliance efforts. PreVeil uses end-to-end encryption to store and share email and files containing CUI and ITAR data. Under State Department Regulation FIPS 120.54, a system that employs FIPS 140-2 algorithms for its end-to-end encryption can be used to store and share ITAR data via the cloud. The PreVeil system meets all these requirements.

# Case study demonstrates PreVeil's benefits of high security, simplicity, and low cost

PreVeil understands that SMB defense contractors are deeply concerned about the complexity, time and cost to achieve NIST SP 800-171 compliance and CMMC Level 2 certification. This case study demonstrates how an SMB dramatically reduced its time and effort—and, importantly, its costs—to secure its CUI and achieve compliance. The benefits of using PreVeil's secure platform for organizations with limited cybersecurity expertise and compliance resources—as is the case for the SMB in this case study—are its world class security, simplicity, and low cost:

- ***PreVeil is built on a modern Zero Trust security model***, one strongly recommended by the National Security Administration (NSA) and President Biden's 2021 *Executive Order on Improving the Nation's Cybersecurity*. PreVeil takes an uncompromised security-first approach, which compliance logically follows. PreVeil's security-first approach supports NIST SP 800-171 and CMMC 2.0's core objectives to protect CUI—and not just achieve compliance. This approach differs from other systems that assemble disjointed tactics designed to check off compliance lists, but inevitably compromise data security in the process.
- ***PreVeil reduces complexity***, making configuration and deployment simple and inexpensive. PreVeil deploys as an overlay to existing Microsoft 365, Exchange, and Google Workspace platforms, and so there's no need to rip and replace existing file and email servers. Solutions such as Microsoft's GCC High, on the other hand, require an organization to decommission their existing email and file sharing systems and replace them with GCC High—an extremely time consuming and expensive process. By contrast, the PreVeil platform can be deployed as an overlay in a matter of hours for most organizations, saving defense contractors tens of thousands in costs and lost time.
- ***PreVeil needs to be deployed only to users handling CUI***, establishing an enclave that results in significantly lower licensing costs. Alternatives, on the other hand, require deployment across entire organizations.
- ***PreVeil is easy to use*** and therefore requires no user training, which means no costly disruptions of productivity. Further, because PreVeil is simple to use, it will be used, keeping your CUI data secure.
- ***PreVeil's SSP template*** helps SMBs tackle the complex but required task of providing objective evidence of their ability to protect CUI. The SSP template is pre-filled with detailed documentation showing how PreVeil supports 84 of NIST SP 800-171's security controls, along with procedures relevant to those controls. The SSP template is part of a comprehensive documentation package that PreVeil provides to its customers, saving them tens of thousands of dollars and months of preparation and consulting time, depending on their size and cybersecurity levels to start.

All of these benefits add up to making PreVeil's world-class security far less expensive than the alternative solution, GCC High. Depending on the size of your organization and current cybersecurity levels, achieving compliance with PreVeil costs from 50% to 75% less than GCC High.

**PREVEIL**

PreVeil is a cloud-based, end-to-end encrypted email and file sharing system built in a modern Zero Trust environment. Unlike existing services, all information is encrypted at the sender's device and can be decrypted only by the recipient, and no one else—not even PreVeil.

***PreVeil Drive*** lets users encrypt, store and share their files, similar to OneDrive or DropBox. PreVeil Drive offers data visibility and access control, so that files can be shared with different permissions—such as view only or edit—and with expirations, allowing the highest levels of control over CUI. Users can access files stored on PreVeil Drive from any of their devices, and changes on one are synched to all their devices.

***PreVeil Email*** adds an encrypted mailbox with a single click to Outlook, Gmail, and Apple Mail. Unlike regular email, PreVeil messages are encrypted and protected from phishing, spoofing, password, server and admin attacks. Emails to users that handle CUI can be automatically encrypted, and PreVeil Email can be used to communicate CUI securely with the Department of Defense. Users send and receive emails just as they are used to, and keep their regular email address, which keeps it simple.

# PreVeil's three-step roadmap to NIST and CMMC compliance

SMBs concerned about complexity and costs can follow PreVeil's practical three-step roadmap outlined below. These practical steps will raise your organization's cybersecurity levels and compliance will logically follow, paving your path to NIST SP 800-171 compliance and CMMC 2.0 Level 2 certification.

## Step One: Adopt a proven cloud platform to secure, store and share CUI.

The key to achieving NIST SP 800-171 compliance and the new CMMC Level 2 certification is to implement proven technology solutions in conjunction with appropriate policies and procedures to ensure the security of CUI. But most widely-deployed commercial systems used to store and share CUI—such as Microsoft 365 Commercial, Google Workspace, and Exchange email—do not comply with all the necessary DoD requirements. Organizations using those standard commercial solutions will need to adopt new platforms to improve their cybersecurity.

As shown in this case study, organizations can easily add PreVeil as an overlay to their existing IT environments, dramatically improving their cybersecurity and raising their NIST SP 800-171 scores.

## Step Two: Take advantage of PreVeil's compliance documentation package.

To help defense contractors get essential documentation tasks done, PreVeil provides a comprehensive documentation package to customers that deploy its platform. The package includes an SSP template that's based on NIST SP 800-171's 110 security controls—which the new CMMC Level 2's controls now mirror—and is prefilled to reflect PreVeil's capabilities and the 84 security controls it meets, along with procedures relevant to those controls. To help complete the SSP, PreVeil's package also includes policies templates for the NIST SP 800-171 control families, as well as templates for a Customer Responsibility Matrix (CRM) that dives into compliance details, and a POA&M for showing how the controls that PreVeil doesn't meet can be met.

The SMB in this case study began with a rudimentary SSP about 25 pages long; by the time of its audit, its SSP was approximately 225 pages long—and satisfied the DIBCAC auditors.

## Step Three: Finish with PreVeil's partner community.

While PreVeil Drive and Email support compliance with virtually all of NIST and CMMC 2.0 mandates related to the storage and communication of CUI, other mandates will need to be addressed too. Fortunately, under CMMC 2.0, POA&Ms will be permitted to address those gaps, although within an expected 180-day time limit. With PreVeil, POA&Ms generally can be fulfilled with policies and procedures, and appropriate configuration of computers and mobile devices that handle CUI, because CUI is secure once PreVeil has been deployed. To facilitate meeting the very few controls that will remain after deployment, PreVeil staff can provide ready access to more than a hundred partner organizations and compliance experts certified by the CMMC-AB, with deep knowledge of DFARS, NIST, CMMC and PreVeil.

The SMB in this case study worked with a PreVeil partner—a highly skilled compliance consultant—who helped throughout the entire audit process. That process culminated with satisfying the DIBCAC auditors by readily addressing the just three findings in the SMB's POA&M, and thereby achieving the highest possible score on its NIST SP 800-171 audit. PreVeil also responded quickly when the DIBCAC audit team independently reached out directly to its staff to seek further clarification on security aspects of its end-to-end encrypted email and file sharing system.

# PreVeil's security-first approach to compliance: Key principles

PreVeil helps contractors meet DoD compliance regulations with an uncompromising security-first approach. Its Zero Trust security model provides unrivalled protection of CUI and critical business information from sophisticated attacks on servers, passwords and admins, as well as from ransomware, spoofing and phishing. Compliance logically follows PreVeil's security-first approach, as it did for the SMB in this case study. In short, PreVeil's state-of-the art security features can help your organization raise its cybersecurity levels, comply with NIST SP 800-171 requirements, and achieve the new CMMC Level 2 when that becomes law.

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

**Zero Trust**
never trust, always verity explicitly, and assume a breach

**End-to-end encryption**
data is decrypted only on users' devices and never in the cloud

**Elimination of central points of attack**
trust is distributed amongst the admin team

**No more passwords**
impossible-to-crack cryptographic keys automatically created instead

**Secure activity logs**
attackers can neither glean information nor cover their tracks

**Readily accessible data backups**
constantly backed up, encrypted, and retained data is immutable and can be readily recovered in the event of an attack

## LEARN MORE

- Schedule a free 15-minute consultation with our compliance experts to answer your questions about NIST SP 800-171 and CMMC 2.0

- Read PreVeil's briefs:

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

NIST SP 800-171 Self-Assessment: Improving Your Cybersecurity and Raising Your SPRS Score

Zero Trust: A Better Way to Enhance Cybersecurity and Achieve Compliance

PREVEIL

March 2022 v2