PREVEIL

Case Study:

How a Defense Contractor using PreVeil Achieved a Near-Perfect NIST 800-171 Score in DIBCAC Audit

Overview

IN MARCH 2021, a team of seven auditors from the US Department of Defense's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) conducted a rigorous audit of a defense contractor—that we'll call "DIBCo"—with under 100 employees. The DIBCAC audit was conducted using DoD's NIST 800-171 Basic Assessment Framework. The contractor achieved a near-perfect score by meeting 109 out of 110 NIST 800-171 controls, placing them alongside the nation's top prime contractors for cybersecurity. The high score also demonstrates they are well-prepared for CMMC Level 3 certification.

DIBCo used PreVeil's end-to-end encrypted email and file storage and sharing system as its core platform to safeguard sensitive data, including Controlled Unclassified Information (CUI), and hired Dr. Jose Neto of PC-Warriors as its partner and consultant to guide them through preparation for the audit process itself. The organization's high score conclusively demonstrates the benefits of expert cybersecurity guidance along with PreVeil's high security, easy deployment, and low-cost approach to cybersecurity and compliance, particularly for small- to medium-size defense contractors.

This case study is written to help defense contractors and cybersecurity consultants gain a better understanding of best practices for achieving success in NIST 800-171 and CMMC Level 3 audit preparation and compliance.

Why the NIST 800-171 Self-Assessment Score Matters

Until now, defense contractors' compliance with NIST 800-171 has been self-attested. In September 2020, however, the Department of Defense released its long-anticipated DFARS Interim Rule, which requires all defense contractors to conduct NIST 800-171 self-assessments according to DoD's carefully defined Assessment Methodology, and to file those scores with the DoD's SPRS (Supplier Performance Risk System). Scoring is on a scale ranging from -203 to +110. A score of less than a perfect 110 necessitates the creation of a POAM (Plan of Action and Milestones) and an indication to the DoD as to when security gaps will be remediated.

The DFARS Interim Rule also includes a clause requiring defense contractors to achieve CMMC certification at the level appropriate for their contract to be eligible to do work for the DoD. Certification will be determined by outside third-party auditors known as C3PAOs. Organizations that handle CUI will be required to achieve CMMC Level 3, which requires

them to meet all of NIST 800-171's 110 practices, plus an additional 20, for a total of 130 cybersecurity practices.

The significance of the NIST 800-171 audit and score is twofold. First, it demonstrates an organization's cybersecurity posture and is an important determinant of their advantage vs. competitors when seeking to be part of a defense contract. Second and more important, there is no path to CMMC certification via partial compliance with NIST 800-171 practices. A perfect score on NIST 800-171—demonstrated via external audit or internal assessment—is an essential step for any organization seeking CMMC Level 3 compliance. The DIBCAC audit results achieved by DIBCo demonstrate how PC Warriors and PreVeil helped the organization move toward achieving each of these objectives without business disruption.

DIBCo: Background

DIBCo is a typical small- to medium-sized defense contractor and has been in business for 15 years. DIBCo conducted a NIST 800-171 self-assessment to comply with the DoD's DFARS Interim Rule and estimated their score. PC-Warriors then conducted a comprehensive and detailed NIST 800-171 audit and found that the organization's actual score was significantly lower than its original self-assessed score. This is not unexpected, as most organizations with limited compliance resources and unfamiliarity with stringent audit requirements tend to overestimate their score.

The DIBCAC NIST 800-171 Audit Process: Five Key Takeaways

A team of seven auditors conducted the NIST 800-171 audit over a period of 5 days. The process was extremely rigorous and thorough. The process revealed five key takeaways to ensure success:

- ***A detailed System Security Plan (SSP):*** The contractor had limited compliance experience and had developed a rudimentary SSP approximately 25 pages long. Dr. Neto helped improve and expand the SSP into a detailed document describing each control, how the contractor complied with it, and evidence to demonstrate compliance. By the time of the audit, the SSP was approximately 225 pages long.
- ***An experienced ISSM/security expert:*** The exhaustive nature of the audit required a highly skilled Information System Security Manager (ISSM) or security professional to interface with the audit team, one conversant with both compliance and information security. DIBCo chose Dr. Neto to represent them. This step was critical because throughout the audit the DIBCAC audit team

sought clarification on numerous aspects of the customer's security and compliance readiness. Dr. Neto's prior experience as a government assessor, as well as the audit preparation done with DIBCo, was essential to rapidly responding to the auditors' questions.

- ***Artifacts to demonstrate compliance:*** The audit team focused heavily on reviewing objective information to demonstrate compliance. While DIBCo was well prepared, the audit team nevertheless requested a large number of additional artifacts, which required significant work done quickly so as to respond in real time. The need to rapidly respond to the auditors' requests highlighted the value of a single, experienced point of contact with the audit team.
- ***PreVeil support:*** The DIBCAC audit team independently reached out to PreVeil to seek further clarification on security aspects of its modern, Zero Trust end-to-end encrypted email and file sharing system. PreVeil responded quickly and provided documents to the audit team, including a security overview and a detailed security architecture that describes how its system encrypts and decrypts data, as well as how it supports compliance with NIST 800-171. PreVeil is FedRAMP Baseline Moderate equivalent, stores all data on FedRAMP High AWS Gov Cloud, uses FIPS 140-2 validated cryptographic module, and complies with DFARS 7012 (c-g).
- ***Overpreparation and early start to demonstrate maturity:*** Dr. Neto strongly instilled the value of overpreparation and starting audit preparation several months prior to the DIBCAC audit. Without adequate time to prepare, DIBCo would not have been able to demonstrate cybersecurity maturity, an essential requirement of NIST 800-171 and CMMC practices. It is critical that organizations seeking compliance understand that there is no shortcut to NIST 800-171 and CMMC success: a key goal of these frameworks is to demonstrate maturity, which by definition cannot be shown with a last-minute effort.

PreVeil deployment at DIBCo: Impact on NIST 800-171 compliance program

Upon the recommendation of Dr Neto, DIBCo chose to deploy PreVeil to all its users handling CUI. The entire organization was rapidly upgraded to PreVeil with help from PreVeil's Customer Support team. DIBCo's users then simply dragged and dropped sensitive data and CUI into folders in their PreVeil Drive, and began using PreVeil Email for sensitive communications knowing that all communication between PreVeil Email users is automatically encrypted. This simple deployment laid the foundation for NIST 800-171 and CMMC Level 3 compliance.

DIBCo achieved a near-perfect score on its DIBCAC audit of NIST 800-171 controls, meeting 109 of the 110 controls and creating a POAM for the one control that was not immediately achieved. Without PreVeil's advanced security and compliance features, the audit score would have been significantly lower.

Options for storing and sharing CUI: Why was PreVeil chosen?

The fundamental goal of the NIST 800-171 and CMMC frameworks is to protect sensitive data, including CUI, during storage and communication. Organizations frequently use popular platforms such as O365 and Google Workspace (formerly G Suite) as their basic communication tools for email and file storage and sharing. Specifically, OneDrive, Google Drive and DropBox are often used to store and share data, and Outlook and Gmail are often used for email. However, none of these platforms comply with CMMC requirements and must be upgraded to do so. There is no path to compliance with CUI stored or shared using O365 Commercial, Google Workspace, DropBox, or other cloud services designed for commercial use.

File storage, sharing and email systems are addressed in over 60% of NIST 800-171 and CMMC Level 3 controls. Therefore, perhaps the most important decision in embarking on a CMMC Level 3 compliance effort is choosing a technology platform to store and share CUI.

PreVeil

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

PreVeil Email adds an encrypted mailbox to Outlook, Gmail, and Apple Mail using your existing email address. Unlike regular email, PreVeil messages are encrypted and protected from phishing, spoofing, password, server and admin attacks. Users send and receive emails just as they are used to, using their regular email address. Emails to users that handle CUI can be automatically encrypted.

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.

For organizations seeking world class compliance and security, the PreVeil platform offers four unique advantages:

- ***Security and compliance:*** PreVeil uses a modern Zero Trust Security paradigm, one strongly recommended by the National Security Agency (NSA). Unlike its alternatives, PreVeil is designed to protect information under the assumption that an attacker will inevitably succeed in breaching the organization's passwords, servers and IT admins. Its end-to-end encryption renders data on servers useless to attackers. And PreVeil doesn't use passwords.

Instead, authentication is done via unguessable encryption keys stored on authorized devices, preventing remote access by attackers.

Admins are protected by cryptographically distributing trust among a group. Sensitive data can be accessed only with approval from a predetermined minimum number of members of that group. This means that an organization's data cannot be accessed even if an IT admin is compromised. Finally, PreVeil enables restricting the flow of sensitive data and CUI to only authorized personnel. These modern security features enable organizations using PreVeil to achieve a high degree of compliance with NIST 800-171 and CMMC Level 3 requirements.

- ***Affordability:*** PreVeil is typically 75% lower in cost compared to alternatives such as GCC High. The cost benefits stem from needing to deploy PreVeil only to users that handle CUI, lower license costs, and most important, ease of deployment.
- ***Ease of deployment:*** PreVeil can be deployed rapidly vs. months of migration and setup for GCC High. PreVeil seamlessly coexists as an overlay with an organization's existing O365, Gmail or Exchange email systems. This eliminates both the cost of an expensive rip and replace of existing systems and business disruption. The rapid deployment results in tens to hundreds of thousands of dollars in cost savings.
- ***Free for third parties:*** PreVeil can be deployed and used for free by entities beyond primary PreVeil customers, such as partners and suppliers. This ability for contractors to bring their suppliers onto the PreVeil platform helps them enhance security throughout their supply chains. PreVeil has written a paper, *Securing the Defense Supply Chain: Helping your subcontractors comply with DFARS, NIST and CMMC*, to help primes and other contractors meet the DoD requirement to secure their supply chains.

PreVeil System Security Plan Template

PreVeil can provide its customers with a comprehensive System Security Plan. The practices section of the SSP template is based on the 130 CMMC Level 3 controls, and has been filled in to reflect PreVeil's capabilities and the requirements it meets. The template -- available for a small monthly fee -- also helps subcontractors demonstrate the required institutionalization of their security processes by offering detailed policy language for the 10 out of 17 CMMC domains that PreVeil helps to address.

This 200-page document serves as the foundation for organizations building their compliance programs using PreVeil at the core, and can immensely simplify the process. The PreVeil SSP and policy templates will serve as an important resource for customers undergoing NIST 800-171 audits in the future as well, as they will be constantly updated to reflect new learnings and compliance requirements.

PreVeil also has written a paper, *Complying with the Department of Defense's Cybersecurity Maturity Model (CMMC)*, to help defense contractors understand the CMMC process. The paper includes a detailed list of CMMC Level 3 practices addressed by PreVeil.

The Accelerated Path to CMMC Level 3 Compliance

DIBCo's remarkably high NIST 800-171 score has laid a very strong foundation for its attainment of CMMC Level 3: PC-Warriors' internal review of DiBCo indicates that the organization is very close to meeting all 130 CMMC Level 3 controls. DIBCo's use of PreVeil was instrumental in laying that foundation. At this point, the path to CMMC Level 3 compliance requires remedying just a few outstanding items on documentation, and gaining experience to demonstrate maturity and adherence to these controls.

Summary

This actual case study demonstrates that defense contractors can achieve an extremely high level of cybersecurity and NIST 800-171 and CMMC Level 3 compliance by adhering to three key principles: 1) Start your audit planning and execution process early; 2) Choose a secure core technology platform such as PreVeil; and 3) Hire a skilled partner to guide, plan and execute the compliance initiative.

About PC-Warriors

PC-Warriors is a leading US cybersecurity firm with over 20 years of combined experience in military and government cybersecurity compliance. The firm is based in Orlando, FL and services clients all over the United States, from Florida to Alaska. As a leading technology company, PC-Warriors develops proprietary cyber solutions and provides guidance to facilitate government compliance for its clients. Their impeccable track record of success has enabled their clients to fulfill and deliver their contracted mission on-time, meeting and exceeding government expectations.

For further information please contact Dr. Jose Neto at JNeto@PC-Warriors.com or 407-715-7392.

About PreVeil

PreVeil is an end-to-end encrypted cloud-based SaaS email and file sharing system for achieving NIST 800-171 and CMMC Levels 3 to 5 compliance. Key attributes of PreVeil's SaaS platform include:

- FedRAMP Baseline Moderate equivalent
- All encrypted data stored on FedRAMP High AWS Gov Cloud
- FIPS 140-2 validated cryptographic modules for encryption
- Supports DFARS 7012 (c-g) requirements

For further information, please contact PreVeil at sales@preveil.com.

PREVEIL

May 2021