PREVEIL

Case Study:

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

Overview

IN MARCH 2021, a team of seven auditors from the US Department of Defense's (DoD's) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) conducted a rigorous audit of a defense contractor, which for purposes of this case study we'll call "DIBCo". DIBCAC—the DoD's ultimate authority on compliance—conducted the audit using the DoD's NIST SP 800-171 Basic Assessment Framework. The contractor achieved a near-perfect score by meeting 109 out of 110 NIST SP 800-171 controls, placing them alongside the nation's top prime contractors for cybersecurity.

Since DIBCo underwent its audit, the DoD released CMMC 2.0, a streamlined version of its original CMMC framework. Under CMMC 2.0, security controls for the new Level 2 (Advanced)—the level comparable to the old CMMC Level 3—will be in complete alignment with NIST SP 800-171 security controls. Given that PreVeil also complies with the CMMC Level 2 requirements that go beyond NIST SP 800-171, it is reasonable to assume that DIBCo also would have been certifiable at the new Level 2 if it had been in effect at the time of the audit.[1]

DIBCo used PreVeil's end-to-end encrypted email and file 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. DIBCo'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 mid-size defense contractors (SMBs).

This case study is written to help SMBs gain a better understanding of best practices for audit preparation and how to achieve compliance with NIST SP 800-171 now and the new Level 2 later, when CMMC 2.0 becomes law.

DIBCo Audit: Background

In late 2020, the Defense Contract Management Agency (DCMA) randomly selected DIBCo for an audit, for which DIBCo was given five months' notice to prepare. DIBCo is a typical SMB contractor: the company has been in business for 15 years and has less than 100 employees. In compliance with DoD cybersecurity requirements, DIBCo previously had conducted a NIST SP 800-171 self-assessment and estimated its score. DIBCo employees began preparations for the DIBCAC audit on their own, but later realized that they needed expert cybersecurity support and brought in PC-Warriors. One of PC-Warriors first tasks was to conduct a comprehensive and detailed NIST SP 800-

1 To learn more about CMMC 2.0, please see PreVeil's paper, *Complying with the Department of Defense's Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0)*.

171 audit, which revealed that DIBCo's actual score was significantly lower than its original self-assessed score. This is not unexpected, however, as most organizations with limited compliance resources and unfamiliarity with stringent audit requirements tend to overestimate their score.

Why the NIST SP 800-171 Self-Assessment Score Matters

Defense contractors have been required to self-assess their compliance with NIST SP 800-171 since those security requirements went into effect in 2017. Starting in late 2020, however, the Department of Defense (DoD) began to require not only that all defense contractors conduct NIST SP 800-171 self-assessments according to the DoD's Assessment Methodology, but also to file those scores with the DoD's Supplier Performance Risk System, known as SPRS. Scoring is on a scale ranging from -203 to +110. A score of less than a perfect 110 necessitates submission of Plans of Action and Milestones (POAMs), which indicate when the controls that have not yet been met will be met.

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

The significance of the NIST SP 800-171 assessment and score is twofold. First, it demonstrates an organization's cybersecurity posture and is an important determinant of their advantage versus competitors when seeking to be part of a defense contract. Second and more important, an excellent score on NIST SP 800-171—demonstrated via external audit or internal assessment—is an essential step now for any organization that hopes to attain the new CMMC Level 2 certification later. Again, security controls for the new CMMC Level 2 will be in complete alignment with NIST SP 800-171's security controls.

The DIBCAC audit results achieved by DIBCo demonstrate how PC Warriors and PreVeil helped the organization move toward both improving their competitive advantage and getting on the right path to achieving CMMC Level 2 without business disruption.

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

A team of seven DIBCAC auditors conducted the NIST SP 800-171 audit over a period of five days. The process was extremely rigorous and thorough, and revealed several 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. A comprehensive SSP was essential to success.
- ***An experienced ISSM/security expert:*** The exhaustive nature of the audit required a highly skilled Information System Security Manager (ISSM) or security professional to work 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. Even though DIBCo was well prepared, the audit team 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 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 describing how its system encrypts and decrypts data, as well as how it supports compliance with NIST SP 800-171. PreVeil meets FedRAMP Baseline Moderate or Equivalent, stores all data on FedRAMP High AWS GovCloud, uses the FIPS 140-2 validated cryptographic module, and complies with DFARS 7012 (c-g), which stipulates requirements for cyber incident reporting.

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

Upon the recommendation of Dr. Neto, DIBCo prepared for its DIBCAC audit by deploying PreVeil as an overlay to its existing O365 system for all its users handling CUI. DIBCo 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 users is automatically end-to-end encrypted. This simple deployment laid the foundation for NIST SP 800-171 compliance now, and Level 2 compliance later when CMMC 2.0 becomes law.

DIBCo achieved a near-perfect score on its DIBCAC audit of NIST SP 800-171 controls, meeting 109 of the 110 controls and creating a POAM for the one control that was not immediately achieved. DIBCo's score is especially notable in light of the fact that a recent DIBCAC review of its assessments conducted during FY 2019 and FY 2020 found that just 22% of companies assessed satisfactorily demonstrated that they met all 110 NIST SP 800-171 controls. 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 key to achieving NIST SP 800-171 compliance is to implement technology solutions in conjunction with appropriate policies and procedures to ensure the security of CUI. Widely-deployed commercial systems—such as Microsoft 365 Commercial and Gmail--do not comply with DoD requirements for the protection of CUI. Therefore, organizations using those standard commercial solutions will need to adopt new platforms to improve their cybersecurity, meet NIST SP 800-171, and comply with the new CMMC Level 2 when that time comes.

Given that secure email systems and file storage and access are addressed in the majority of NIST SP 800-171's security controls—which the new CMMC Level 2 security controls will mirror—perhaps the most important decision in embarking on both a NIST SP 800-171 and a CMMC Level 2 compliance effort is choosing a technology platform to store and share CUI.

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 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, and keep their regular email address, which keeps it simple. 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:

PreVeil 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 makes attacks on servers useless because the data is never decrypted on a server. 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 SP 800-171 now, and the new Level 2 requirements later when CMMC 2.0 is implemented.

- ***Affordability:*** PreVeil is typically 75 percent 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 compared to months of migration and setup for GCC High. PreVeil seamlessly coexists as an overlay with an organization's existing O365 or

Gmail systems. This eliminates the costs of both an expensive rip and replace of existing systems and business disruptions. 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 System Security Plan (SSP) Template

An SSP is required for any DoD work. To help defense contractors get this essential task done, PreVeil provides an SSP template to companies that deploy its platform. The SSP template is based on the 110 NIST SP 800-171 controls and has been filled in to reflect PreVeil's capabilities and the requirements it meets. This comprehensive 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 will serve as an important resource for customers undergoing NIST SP 800-171 audits in the future as well, as it will be constantly updated to reflect new learnings and compliance requirements.

PreVeil has several resources that provide detailed background and information on the fast-changing landscape of compliance and its ramifications for defense companies. For example, our paper, *Complying with the Department of Defense's Cybersecurity Maturity Model (CMMC)*, offers a clear summary of CMMC and tips on how to get started on your organization's CMMC journey. The paper has been updated to reflect changes to the CMMC framework coming with the introduction of CMMC 2.0, and includes an appendix with a detailed list of NIST SP 800-171 controls addressed by PreVeil. Again, when implemented, security controls for the new CMMC Level 2 will completely align with NIST SP 800-171's security controls.

PreVeil also has written a brief, *DFARS Self-Assessment: How to Raise Your NIST SP 800-171 Score*, which shows specifically how PreVeil can help raise your company's NIST SP 800-171 self-assessment score by nearly 40 points.

Conclusion

DIBCo's remarkably high NIST SP 800-171 score has given the company's senior officials and IT staff total confidence that their company is in compliance with DoD cybersecurity regulations currently in effect and, importantly, is on an accelerated path to attain the new Level 2 once CMMC 2.0 is implemented. DIBCo's use of PreVeil was instrumental to successfully navigating the DIBCAC

audit, earning a near-perfect NIST SP 800-171 score, and achieving peace of mind knowing that their companies' data is secure.

This actual case study demonstrates that small to mid-size defense contractors can achieve an extremely high level of cybersecurity and be well positioned for NIST SP 800-171 and CMMC Level 2 compliance by adhering to three fundamental principles: First, hire a skilled partner to guide, plan and execute the compliance initiative; second, prepare a comprehensive SSP; and third, choose a core technology platform such as PreVeil for securely storing and sharing CUI.

To learn more about how PreVeil's state-of-the-art Zero Trust platform can help improve the security of your organization's communication and collaboration system, please access the compliance resources linked throughout this case study and contact us at preveil.com/contact or +1 (857) 353-6480.

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 email and file sharing system to help organizations comply with NIST SP 800-171 and CMMC Level 2 compliance. Key attributes of PreVeil's SaaS platform include:

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

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

PREVEIL

December 2021