PREVEIL

Securing the defense supply chain

Helping your subcontractors comply with DFARS, NIST and CMMC

Executive Summary

THE DEPARTMENT OF DEFENSE'S DFARS Interim Rule mandates that defense contractors not only perform a self-assessment based on NIST 800-171, but also report that score to the DoD. The Interim Rule, already in effect, also places responsibility for subcontractors' compliance with DFARS, NIST and CMMC squarely on the shoulders of their contractors. This responsibility extends throughout all levels of the supply chain—not just to contractors' direct suppliers. Yet it is widely acknowledged that many subcontractors are currently non-compliant with NIST 800-171 controls. Clearly, to preserve their own competitiveness, primes and other contractors stand to gain from helping their subcontractors expedite their compliance journey.

In light of contractors' increased responsibility to protect their supply chain, this brief focuses on PreVeil's unique three-step solution for contractors to help their suppliers achieve greater levels of cybersecurity and compliance. This comprehensive approach offers uncompromised cybersecurity for handling CUI, and recognizes what it takes for a small to medium-size subcontractor to achieve full compliance. The three steps are:

Step One Subcontractors need to adopt a secure platform for exchanging CUI. PreVeil Drive and Email are built on a modern Zero Trust security model, one strongly recommended by the National Security Agency (NSA) in recent guidance issued in light of the SolarWinds breach. PreVeil delivers end-to-end encryption, ease of deployment and use, and compliance related to the encryption and protection of CUI, FCI and ITAR data.

Step Two PreVeil has commissioned an SSP template to help your subcontractors that deploy its platform. The template is based on CMMC Level 3 requirements and filled in to reflect PreVeil's capabilities and the requirements it meets. The template also offers detailed policy language for the 10 out of 17 CMMC domains that PreVeil helps to address.

Step Three While PreVeil Drive and Email support compliance with virtually all of NIST and CMMC mandates related to the storage and communication of CUI, other mandates will need to be addressed too. To facilitate that, PreVeil has partnered with a wide range of organizations and individuals certified by the CMMC-AB (CMMC Accreditation Body), with expert knowledge of DFARS, NIST, CMMC and PreVeil. Coordinated access to this specialized partner community will smooth your subcontractors' path to compliance.

The aim of PreVeil's comprehensive supply chain solution is to help you accelerate your subcontractors' efforts to raise their cybersecurity levels and achieve compliance with DFARS, NIST and CMMC—enabling you to stay focused on improving your competitive position in the Defense Industrial Base.

The challenge: Supporting subcontractors' DFARS, NIST and CMMC compliance efforts

According to Ellen Lord, former DoD Undersecretary of Defense for Acquisition and Sustainment ((OUSD(A&S)), supply chain vulnerabilities are most prevalent six or seven levels down from prime contractors. Simply put, cybercriminals know that prime defense contractors are well protected, and save themselves time and effort by going after their subcontractors.

Indeed, from a cybersecurity perspective, subcontractors are the Achilles heel of the DIB's supply chain. As reported in April 2020, for example, ransomware attackers targeted Visser, a subcontractor for several prominent aerospace and defense companies, including Lockheed Martin. Visser refused to pay the ransom. In retaliation, the cybercriminals made sensitive documents publicly available, among them Lockheed Martin's designs for an antenna in an anti-mortar defense system—documents they were able to access only through Visser. Boeing and SpaceX were victims of the same attack.

Cybercriminals know that U.S. prime defense contractors are well protected, and they save themselves time and effort by going after their subcontractors. To address this weakness by improving cybersecurity up and down the supply chain, the DFARS Interim Rule turns to primes—and all contractors that have subcontractors—and mandates that:

Cybercriminals know that U.S. prime defense contractors are well protected, and they save themselves time and effort by going after their subcontractors.

- Contractors must include the NIST 800-171 self-assessment requirements stipulated in the new DFARS clause -7020 in all applicable subcontracts.
- Subcontractors must have the results of a current self-assessment filed in the DoD's SPRS (Supplier Performance Risk System), and contractors must confirm with the subcontractor that this requirement has been met prior to the award of a subcontract.

Further, new DFARS clause -7021 serves as the bridge from DFARS and NIST to CMMC and requires:

- All contractors—primes and subcontractors—must achieve CMMC certification at the level specified in the contract by time of award. CMMC certification must be maintained at the appropriate level for the duration of the contract.
- All contractors must flow down this clause's requirements to their subcontractors.

While the DFARS Interim Rule doesn't specify minimum self-assessment scores that must be achieved, it stands to reason that primes and other contractors will consider self-assessment scores

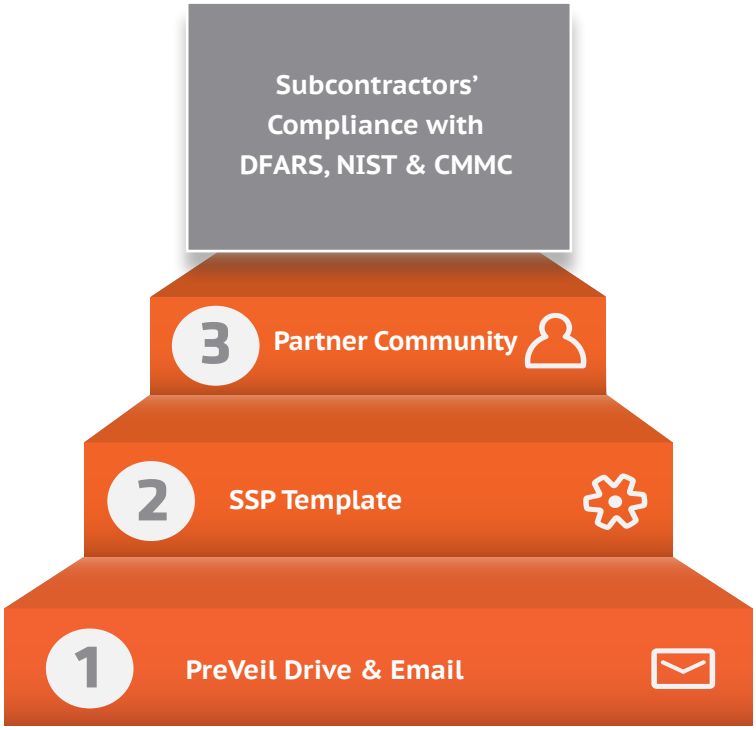
when evaluating possible subcontractors with which to work, similar to how they themselves will be assessed by the DoD. It is reasonable to expect that suppliers with higher scores are more likely to win subcontracts.[1]

Given that many subcontractors currently are non-compliant with NIST 800-171 controls, the challenge contractors now face is how best to help their subcontractors improve their cybersecurity and expedite their compliance journey.

PreVeil's three-part solution for securing your supply chain

Contractors' responsibilities for confirming their subcontractors' compliance need not be overwhelming. That said, PreVeil understands that your subcontractors need more than world class security to achieve compliance with DFARS, NIST and CMMC, and so offers a three-step solution to help you support your subcontractors' compliance journey, as illustrated below.

Figure 1: PreVeil's Three Part Supply Chain Solution



1 PreVeil recently published a brief, *DFARS Self-Assessment: Improving Cybersecurity and Raising Your Score*, explaining the Interim Rule's NIST self-assessment and reporting requirements, and showing how a company can quickly raise its self-assessment score by implementing PreVeil.

Supply chain solution Step One: PreVeil Drive and Email

PreVeil is an email and file sharing platform that provides your subcontractors *uncompromised security* for protecting and exchanging CUI. PreVeil is built on a modern Zero Trust cybersecurity model, which the NSA urged the entirety of the DoD and the DIB to adopt in its Feb. 2021 guidance issued in the wake of the SolarWinds breach. "The Zero Trust security model," the NSA wrote, "assumes that a breach is inevitable or has likely occurred, so it constantly limits access to what is needed and looks for anomalous or malicious activity."[2] With PreVeil, any user—whether from inside or outside your organization—needs to be authenticated, and the flow of CUI can be restricted to just trusted partners and suppliers.

PreVeil's Zero Trust system is grounded in end-to-end encryption,[3] wherein all user data is only ever encrypted and decrypted on a user's device—and never on a server. And because PreVeil uses automatically-generated cryptographic keys rather than passwords, CUI cannot be accessed with stolen passwords, nor by using a compromised administrator's credentials.

PreVeil Drive and Email deploy easily as an overlay system, with no impact on existing file and email servers—making *configuration and deployment simple and inexpensive* for your subcontractors.

One of PreVeil's guiding principles is that if security isn't easy to use, it won't be used. To that end, PreVeil is *easy for users to adopt* because it works with the tools they already use: PreVeil Drive's file sharing works like OneDrive and is integrated with Windows File Explorer and Mac Finder. PreVeil Email seamlessly integrates with Outlook, Gmail, or Apple Mail clients.

One of PreVeil's guiding principles is that if security isn't easy to use, it won't be used.

PreVeil Drive offers *data visibility and control* by making it just as easy to unshare files and folders as it does to share them. For example, when a subcontractor is no longer involved with a program, relevant files can be unshared, in which case the files will no longer be accessible by the subcontractor and the copies located on their PreVeil Drive directories will be removed. Alternatively, contractors can share files on a time-limited basis, whereby access automatically expires after a designated time.

PreVeil also allows contractors' administrators to see into all layers throughout their supply chain and control access down to the device level. If a user's computer or phone has been lost or stolen, for example, the missing device can be locked to prevent further access to files shared via PreVeil.

PreVeil's end-to-end encrypted Drive and Email solutions support *compliance with DFARS 252.204-7012, NIST 800-171, and CMMC Level 3,* all within a Zero Trust environment. And because

2 National Security Agency: Cybersecurity Information, *Embracing a Zero Trust Security Model*, issued Feb. 2021.

3 In NSA guidance issued in April 2020 and updated in Nov. 2020, *Selecting and Safely Using Collaboration Services for Telework—Update*, the NSA's top criteria for choosing collaboration services is whether they use end-to-end encryption.

PreVeil deploys in a matter of hours, it's an ideal way to quickly help your subcontractors raise their newly-required NIST self-assessment score and get on the path to CMMC Level 3 compliance.[4]

Finally, given its ease of deployment and use, PreVeil is *cost effective*. It need be deployed only to employees handling CUI, whereas alternatives require deployment across entire organizations. And PreVeil's straightforward, light-touch solutions help avoid expensive DFARS, NIST and CMMC consultant engagements, which are par for the course for some alternatives. As a result, PreVeil typically costs 75% less than Microsoft GCC High.

Furthermore, PreVeil Drive and Email can be *downloaded for free by subcontractors.* This gives contractors an unparalleled opportunity to help themselves and their suppliers comply with federal cybersecurity regulations—and likewise, protect and preserve their supply chain continuity.

Table 1 below offers a brief summary of how PreVeil Drive and Email help meet the challenges that subcontractors present to securing the supply chain.

Table 1: How PreVeil Drive and Email meet the challenges subcontractors present to securing the supply chain

Key Consideration	PreVeil Drive and Email solution
Uncompromised security	Zero Trust system. Provides gold standard of end-to-end encryption throughout the supply chain. Protects against modern security attacks.
Ease of deployment and use	Easy for subcontractors to deploy and use. No impact to existing email or file servers. Instructions fit on one sheet.
Data visibility	Contractors can choose to share and unshare documents with a Trusted Community of subcontractors and individuals and limit visibility.
Compliance	Meets DFARS and NIST requirements for protection of CUI and smooths path to CMMC Level 3 compliance. Meets NSA guidance on Zero Trust and end-to-end encryption.
Cost effectiveness	Highly affordable. Deploys only to users handling CUI. Contractor pays only for licenses needed internally. Free to subcontractors.

4 For more details on how PreVeil meets CMMC requirements related to the encryption and protection of CUI, see PreVeil's white paper, *Complying with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC).*

Supply chain solution Step Two: PreVeil's SSP template

An SSP is a prerequisite for any DoD work. To help subcontractors get this essential task done, PreVeil has commissioned creation of an SSP template for companies that deploy its platform. 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 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.

The SSP template has been created by PreVeil partners with extensive experience working with companies to complete their SSPs. The template will give your subcontractors a considerable head start on their SSP—otherwise a daunting, time-consuming, and costly task. The PreVeil template also will dramatically accelerate your subcontractors' paths to CMMC compliance.

Supply chain solution Step Three: PreVeil's partner community

PreVeil understands the challenges that DFARS, NIST and CMMC mandates present to all companies in the DIB. In fact, the vast majority of subcontractors likely will need to work with consultants to help them achieve compliance. To that end, PreVeil has built a partner community comprised of organizations and individuals certified by the CMMC-AB (CMMC Accreditation Body), all with expert knowledge of DFARS, NIST and, of course, CMMC and PreVeil.

PreVeil has more than 60 CMMC-AB certified partners, including C3PAOs (CMMC Third Party Assessor Organizations); Provisional Assessors; RPOs (Registered Provider Organizations); Registered Practitioners; and specialized MSPs and MSSPs.

Coordinated access to this specialized partner community will streamline your subcontractors' DFARS, NIST and CMMC Level 3 compliance efforts, saving time and reducing costs. In the end, the confidence that your company's supply chain is secure will give you the peace of mind you need to focus on improving your competitive position within the DIB.

PreVeil's partner community

Conclusion

Going forward, an increasing number of DoD contracts will require that contractors confirm that their suppliers have strong NIST self-assessment scores and achieve CMMC compliance. PreVeil is uniquely positioned to help contractors ensure that they meet these DoD mandates for securing their supply chain. Its comprehensive solution offers:

- PreVeil Drive and Email, a powerful platform that will quickly elevate your subcontractors' cybersecurity and help them meet DFARS, NIST and CMMC Level 3 requirements for securely communicating CUI throughout your supply chain.
- An SSP template that gives subcontractors a significant head start on their required SSPs, saving them time and money and expediting their compliance journeys.
- Coordinated access to the deep expertise of PreVeil's partner community. Those partners—expert in DFARS, NIST, CMMC and PreVeil—will support your subcontractors' compliance efforts and, likewise, help you meet the challenges and responsibilities for securing your supply chain that the DFARS Interim Rule has placed squarely on your shoulders.

Contact PreVeil to learn more.

About PreVeil

PreVeil makes encryption usable for everyday business. PreVeil's encrypted email works with existing apps like Outlook or Gmail, letting users keep their regular email addresses. PreVeil Drive works like DropBox for file sharing, but with far better security. All messages and documents are encrypted end-to-end, which means that no one other than intended recipients can read or scan them—not even PreVeil. PreVeil is designed for both small teams and large enterprises. Visit www.preveil.com to learn more.

PREVEIL

March 2021