PREVEIL

Securing the defense supply chain

How to achieve secure and compliant communication with your subcontractors

Executive Summary

CYBERTHIEVES TARGET American trade secrets and leadership in the medical, scientific, technological, military and commercial realms. Estimates of intellectual property losses in the overall US economy range between $225 - $600 billion *annually*.[1] The Defense Industrial Base (DIB)—a complex supply chain comprised of 300,000 primes and subcontractors—is not immune to such theft, the majority of which is conducted by nation state adversaries.[2]

To better defend the DIB's vast attack surface, the Department of Defense (DoD) is focused on supply chain risk management. Indeed, Katie Arrington, DoD's chief information security officer for the Undersecretary of Defense for Acquisition and Sustainment, recently identified securing the supply chain as one of her top three priorities for 2021.[3] As part of that effort, the DoD's DFARS Interim Rule holds primes responsible for the security of their supply chains. That responsibility extends throughout *all* levels of the supply chain—not just to contractors' direct suppliers.

This brief outlines the challenges primes and other contractors face in securing their supply chains, and describes key requirements of secure supply chain communications platforms, including:

- Uncompromised security, ideally grounded in modern principles of Zero Trust security and end-to-end encryption
- Data visibility and access control throughout the supply chain
- Compliance with federal regulations, including DFARS, NIST and CMMC
- Ease of deployment and configuration
- Simplicity of use
- Cost effectiveness

Securing your supply chain is complex but need not be overwhelming. PreVeil's end-to-end encrypted file sharing and email messaging tools offer pragmatic solutions for meeting each of these key requirements for communicating simply and securely with your subcontractors, as described herein.

This brief serves as a companion piece to an earlier PreVeil brief, *Securing the defense supply chain: Helping your subcontractors comply with DFARS, NIST and CMMC*. It is our hope that, taken together, the briefs offer the guidance and tools that primes and other contractors need to achieve a high level of confidence in the security of their supply chains.

1 See: *The Report of the Commission on the Theft of American Intellectual Property*, Feb. 2017.
2 See: *Cost and Sources of Global Intellectual Property Theft Include China and the U.S.*, July 2020.
3 Arrington's top three priorities for 2021 are Zero Trust, supply chain security, and DevSecOps. See keynote speech given at CyberEd.io 2021 Virtual Cybersecurity Summit.

The challenge: Secure and compliant communication throughout your supply chain

To get their work done, primes and subcontractors throughout the DIB need to collaborate, which means communicating and sharing sensitive files containing work plans, designs, and other CUI, FCI and ITAR data. Cybercriminals know that prime defense contractors are well protected—and that the cybersecurity capabilities of subcontractors vary widely. Attackers save themselves time and effort by going after the subcontractors, typically six or seven levels down the supply chain from their primes.

The upshot is that from a cybersecurity perspective, subcontractors are the Achilles heel of the DIB's supply chain. In light of that reality, primes need to figure out how to collaborate with their subcontractors in a secure and compliant environment.

From a cybersecurity perspective, subcontractors are the Achilles heel of the DIB's supply chain.

Enhancing the security of your supply chain is not only good business, but also helps achieve compliance with the DFARS Interim Rule mandate that holds primes and other contractors responsible for the security of their supply chains. This responsibility extends throughout all levels of the supply chain—that is, not just to contractors' direct suppliers, but through every layer down to the smallest supplier at the bottom of the chain. It's those suppliers that are most likely to have the fewest cybersecurity resources.

Larry Volz (Ret), Global CIO and SVP at Pratt & Whitney, describes the challenge this way: "When a Prime wins a defense contract, we need to immediately begin communicating with subcontractors throughout our supply chain to get the job started. From the get-go, we need to be able to email our suppliers and share files simply, securely, and in compliance with all DoD regulations."

Equally important, access to all the files containing CUI and FCI needs to be permanently shut down once the project is complete. This final task is too often neglected, and forgotten files from long-completed projects are frequently compromised by attacks on subcontractors.

Consider this illustrative case:

> In early 2015, a global defense technology firm needed to share hundreds of sensitive design files with a supplier. It did so securely, using the best cybersecurity controls available at the time. The work got done and the relationship with the supplier ended well, but the files were forgotten. Five years later the supplier's vulnerabilities were exploited by hackers—who were unable to penetrate the prime's network—and the old files were exfiltrated and released publicly. The prime was held responsible by the Department of Defense for the breach.

Of course, challenges with securing your supply chain extend beyond sharing and unsharing files. 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.

Varying levels of resources and cybersecurity sophistication throughout the supply chain make it all too easy for hackers to steal passwords, compromise administrators, breach servers, and employ the many techniques they have at their disposal to go after weak links. The massive SolarWinds and Microsoft Exchange breaches offer stark evidence of the uneven playing field that often pits small suppliers against well-funded and highly sophisticated attackers.

While world class security solutions are available to help level the playing field, too often they are beyond the reach of small suppliers because of cost and the difficulties associated with their deployment, configuration and use.

PreVeil solves the DIB supply chain security problem

PreVeil understands the challenges primes face in securing their supply chain and is designed to overcome them. PreVeil is a highly secure end-to-end encrypted email and file sharing platform that meets each of the key requirements for securing your supply chain communications, as described below.

Uncompromised security

PreVeil Drive and Email solutions are grounded in *end-to-end encryption*,[4] 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 by remotely logging into accounts with stolen passwords, nor by using a compromised administrator's credentials.

PreVeil is built on a modern *Zero Trust cybersecurity model*, which the NSA strongly recommended the entirety of the DoD and the DIB adopt in its February 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

4 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.

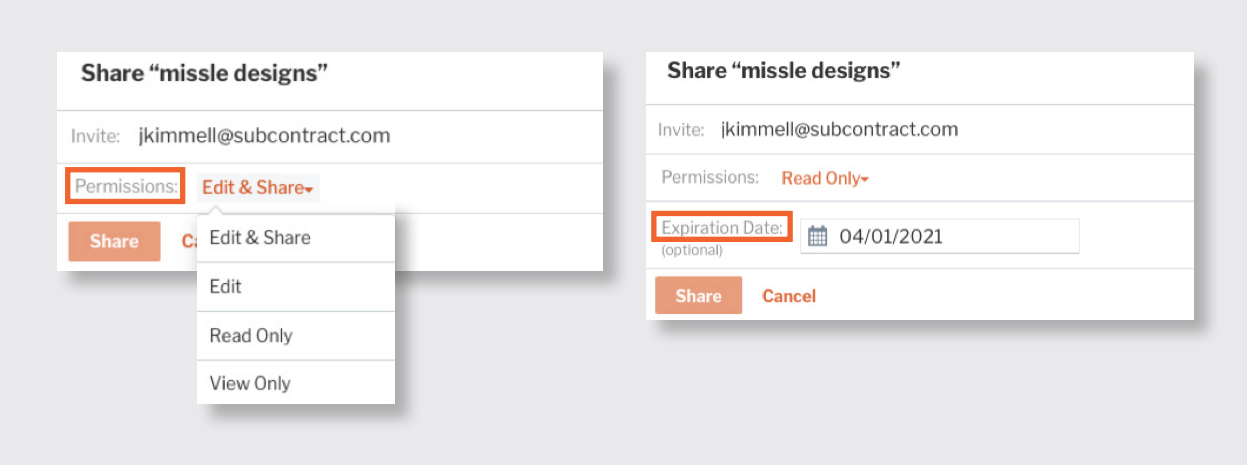
anomalous or malicious activity."[5] With PreVeil, any user—whether from inside or outside your organization—needs to be cryptographically authenticated, and the flow of CUI can be restricted to just trusted partners and suppliers.

Data visibility and access control

PreVeil Drive offers *data visibility and access control* by making it just as easy to unshare files and folders as it is to share them. For example, when a subcontractor is no longer involved with a project, 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. Permission options for shared files range from access for collaboratively editing and sharing the documents, to view only, which prevents the shared information from being downloaded at all.

Figure 1 below shows how files can be shared with different permissions and expirations, allowing the highest levels of control over their contents.

Figure 1: Sharing files—permissions and expirations



PreVeil also allows contractors' visibility into their data down to the smallest supplier at the bottom of their supply chain, and access control 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.

Compliance with federal regulations, including DFARS, NIST and CMMC

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 security environment.

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

PreVeil is FedRAMP Baseline Moderate Equivalent, stores all data on Amazon Web Services GovCloud, which is FedRAMP High, ands uses FIPS 140-2 validated encryption algorithms.

Given that the DFARS Interim Rule places responsibility for subcontractors' compliance squarely on the shoulders of their contractors, helping your suppliers expedite their compliance journey is good business. The companion piece to this brief, *Securing the defense supply chain: Helping your subcontractors comply with DFARS, NIST and CMMC*, describes PreVeil's comprehensive three-step approach to meeting this challenge.

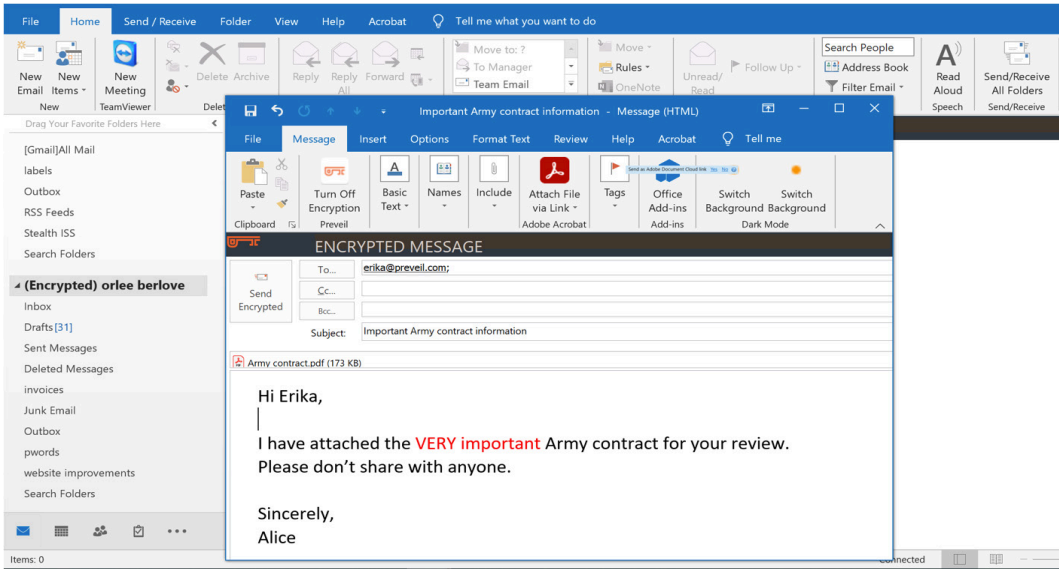
CASE STUDY:
NIST 800-171 COMPLIANCE

DIBCAC (the Defense Industrial Base Cybersecurity Assessment Center) recently conducted a thorough audit of an SMB subcontractor using DoD's exhaustive Assessment Methodology. The SMB, which uses O365, was able to keep that system and simply overlay PreVeil in a matter of hours to help address the majority of NIST 800-171 controls. The SMB scored a remarkable 106 of 110 on the audit, and clearly is well on its way toward CMMC Level 3 compliance as well.

Ease and simplicity of deployment, configuration and use

PreVeil Drive and Email deploy easily as an overlay system, without requiring any changes to existing file and email O365, Exchange or Gmail servers. Thus, *deployment and configuration are simple and inexpensive* for your subcontractors. Even so, if security is difficult to apply, it won't be used. PreVeil was created with this principle in mind so that your subcontractors can and will raise their cybersecurity and compliance levels. 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, and users can keep their regular email address, as shown in Figure 2 below.

Figure 2: Seamless integration of PreVeil Email into Gmail



Cost effectiveness

Finally, PreVeil is *cost effective*. It need be deployed only to employees handling CUI, whereas alternatives require deployment across entire organizations. 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 supply chain continuity.

In short, PreVeil offers state-of-the-art solutions that allow seamless, secure, and encrypted file sharing and email messaging to support collaboration throughout your supply chain. Moreover, PreVeil is accessible to even your smallest suppliers with the fewest cybersecurity resources, and so helps level the cybersecurity playing field.

PREVEIL USE CASE:
SHARING AND UNSHARING FILES WITH A SUBCONTRACTOR

In April 2020, a large global aerospace and defense technology firm needed to share 8,300 sensitive designs with a supplier. The prime installed PreVeil and told its supplier to do the same, which it did for free in less than an hour. The prime simply dragged and dropped the design files into a PreVeil Drive folder and shared it with their supplier quickly and easily over end-to-end encrypted PreVeil Email. The file sharing and communications met all relevant federal cybersecurity regulations, and allowed the prime to proceed securely and without disruption to its supply chain. Moreover, upon sharing, the prime time-limited the files so that the supplier's access to them expired on the end date of the supplier's subcontract.

Conclusion

PreVeil understands the challenges that primes and other contractors face as they strive to meet their responsibility for securing their supply chains. Our two-part series (of which this brief is part two) is designed to help you meet those challenges.

PreVeil's first brief, *Securing the defense supply chain: Helping your subcontractors comply with DFARS, NIST and CMMC*, presents a unique three-step solution to help you accelerate your subcontractors' efforts to raise their cybersecurity levels and achieve compliance with DFARS, NIST and CMMC.

This brief is designed to help primes and other contractors communicate throughout their supply chain in a secure and compliant environment. It presents PreVeil Drive and Email—built on modern cybersecurity principles and grounded in end-to-end encryption—as solutions that allow secure, compliant file sharing and email messaging to support collaboration throughout your supply chain.

It is our hope that this series offers the guidance and tools you need to achieve a high level of confidence in the security of your supply chain and, in so doing, empowers you to stay focused on improving your competitive position in the Defense Industrial Base.

To learn more about PreVeil, visit preveil.com/contact or call us directly at (857) 353-6480.

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

April 2021