PREVEIL

Securing the Defense Industrial Base Supply Chain

Executive Summary

THE PURPOSE OF THIS BRIEF is to help the Department of Defense contractors communicate securely, easily, and cost effectively—both internally and with their supply chain—and in so doing meet DoD's cybersecurity compliance requirements including DFARS 7012, NIST 800-171, ITAR, and soon, CMMC.

The Defense Industrial Base (DIB) is a complex supply chain comprised of 300,000 primes and subcontractors that need to share sensitive files and communicate securely to get their work done. Cybercriminals know that prime defense contractors are well protected—and that the cybersecurity capabilities of DIB subcontractors vary widely. Hackers save themselves time and effort by going after the subcontractors, typically six or seven levels down the supply chain from the primes.

The DoD is well aware of these tactics and so is focused on better defending the vast attack surface that the Defense Industrial Base (DIB) presents to adversaries. Clearly, it's in the best interests of prime contractors, too, to secure their supply chain so they can continue to do DoD work without disruption.

This brief outlines key considerations to keep in mind when assessing solutions to secure the supply chain, including:

- Uncompromised security
- Ease of deployment
- Simplicity of use
- Compliance with federal regulations, including CMMC
- Cost effectiveness

PreVeil's encrypted file sharing and email messaging tools support collaboration and address each of these key considerations for securing the supply chain, as described herein. PreVeil's world-class end-to-end encryption is based on MIT computer scientists' research on cybersecurity and applied cryptography.

PreVeil Drive and Email deploy easily in minutes with no impact on existing file and email servers, making configuration and deployment simple and inexpensive. PreVeil integrates seamlessly with Outlook and Gmail and so is easy to use. Further, PreVeil's security paradigm supports compliance with DFARS 7012, NIST 800-171, ITAR, and virtually all of the CMMC mandates related to the communication and storage of Controlled Unclassified Information (CUI) up and down the supply chain.

Best of all, PreVeil's supply chain solutions can be downloaded for free by subcontractors for encrypted file sharing of up to 100GB of data, and unlimited encrypted email messaging. This gives primes an unparalleled opportunity to help themselves and their suppliers comply with federal cybersecurity regulations—and likewise, protect and preserve their supply chain continuity.

Introduction

The Department of Defense (DoD) is taking a supply-chain risk-management approach to defending the vast attack surface that the Defense Industrial Base (DIB) presents to adversaries. Of the approximately 300,000 contractors in the DIB, only about 1% are primes; the remainder are subcontractors. Those subcontractors—which vary widely in terms of their size and cybersecurity capabilities—are the Achilles heel of the DIB's supply chain.

During a December 2019 DoD briefing, Ellen Lord, DoD's Undersecretary of Defense for Acquisition and Sustainment (OUSD A&S), explained that supply chain vulnerabilities are most prevalent six or seven levels down from prime contractors. Earlier, in September 2019, Katie Arrington, DoD's chief information security officer for the OUSD A&S, put it this way: "Adversaries aren't going after a Lockheed Martin, at the top prime level, they're going after small business…that's the most vulnerable [link in the supply chain]."

Lord and Arrington have it right. Indeed, as reported in April 2020, 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 the U.S. prime defense contractors are well protected, and they save themselves time and effort by going after their subcontractors.

Five key considerations for securing the DIB supply chain

Five straightforward considerations should be top of mind when considering alternative solutions for securing your supply chain:

1. ***Security***. Implement the highest level of data security needed, including the ability to control information several levels down the supply chain.
2. ***Deployment***. Ensure ease of deployment, so that suppliers can easily install the solution in IT environments that often vary widely from supplier to supplier.
3. ***Simplicity.*** Ensure frictionless ease of use, so that sharing information is as easy as with basic consumer-level email and file sharing systems.
4. ***Compliance***. Regulations governing the DoD's supply chain include among others DFARS 7012, NIST 800-171 and, soon, CMMC.
5. ***Cost effectiveness***. Affordability matters, and flows from easy, low-touch deployment and use - without compromising security.

PreVeil solves the DIB supply chain cybersecurity problem

The key considerations outlined above for how best to secure the DIB supply chain need not be overwhelming. Cybersecurity research at leading universities has led to critical advances in applied cryptography. These new technologies will enable your company to enhance its own cybersecurity, as well as that of the subcontractors in your supply chain.

The brief descriptions of PreVeil's security features and products that follow demonstrate how PreVeil's supply chain solutions leverage technical advances to offer secure file sharing and encrypted email messaging to support collaboration—and address each key consideration for securing the DIB supply chain.

Key consideration no. 1: Security

PreVeil's security architecture is based on MIT computer scientists' research on cybersecurity and applied cryptography. It leverages a fundamentally better security paradigm, grounded in world-class end-to-end encryption. End-to-end encryption is based on the principle of zero trust, that is, any user—whether from inside or outside your organization's networks—needs to be authenticated. Too often, the default of traditional solutions is to trust anyone who's communicating from within the network. That gives hackers who've made their way in, through any of a wide range of techniques, legitimacy and free rein within your network.

End-to-end encryption is the widely-acknowledged gold standard for protecting email and file sharing. Indeed, in response to concerns about the work that U.S. government employees and military personnel are doing from home during the coronavirus pandemic, the National Security Agency (NSA) recently issued guidance about the use of collaboration services for telework—which also describes the communications that happen between primes and their subcontractors at almost any time. The NSA's top recommendation is that such collaboration services use end-to-end encryption.

PreVeil's end-to-end encryption ensures that data—files and emails—is encrypted on any device an internal employee or subcontractor may use, and never decrypted anywhere other than on the recipient's device. Only the sender and the recipient can ever read the information being shared—and no one else. Data is never decrypted on any server or gateway anywhere; if attackers successfully breach a server, all they will get is useless gibberish.

Further, PreVeil doesn't depend on passwords, but instead authenticates users via strong cryptographic keys that are automatically created and stored on users' devices—and never in a central key server, eliminating central points of attack. And as described below, PreVeil's Trusted Community and Approval Group features, along with the ability to unshare files, all strengthen controls of access to sensitive information.

Finally, PreVeil runs on Amazon Web Services (AWS) GovCloud, which does not have the ability to access decrypted user data.

Key considerations nos. 2 and 3: Ease of deployment and simplicity for the user

PreVeil deploys easily because it seamlessly integrates with familiar Mac and PC applications. And PreVeil is easy for end users to adopt because it works with the tools they already use. PreVeil Drive's file sharing works like OneDrive and is integrated with the Windows File Explorer and Mac Finder. PreVeil Email integrates with Outlook, Gmail, or Apple Mail clients.

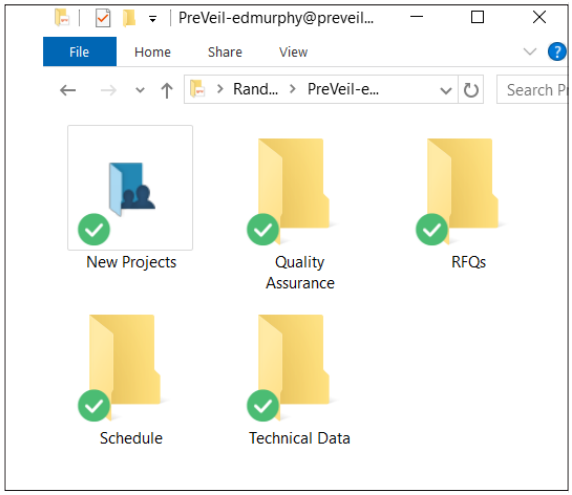
The following descriptions of PreVeil's supply chain solutions illustrate these and other features.

PreVeil Drive

PreVeil Drive works like OneDrive for file sharing, but with far better security. But unlike OneDrive—or Box, Google Drive, and DropBox—which always have access to your data, only you and the people with whom you've explicitly shared files can decrypt them. Any changes to files made on users' devices are automatically synched to encrypted versions of those files stored in PreVeil's cloud-based service, AWS GovCloud.

PreVeil Drive users easily create folders for sharing data internally or with subcontractors. PreVeil Drive is easy to use and automatically integrates with Windows File Explorer and Mac Finder. It's available for Windows, Mac and, with PreVeil's mobile app, for iPads and smartphones as well.

PreVeil Drive: Sharing and storing files



Easy to unshare and control access

Importantly, PreVeil Drive makes 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.

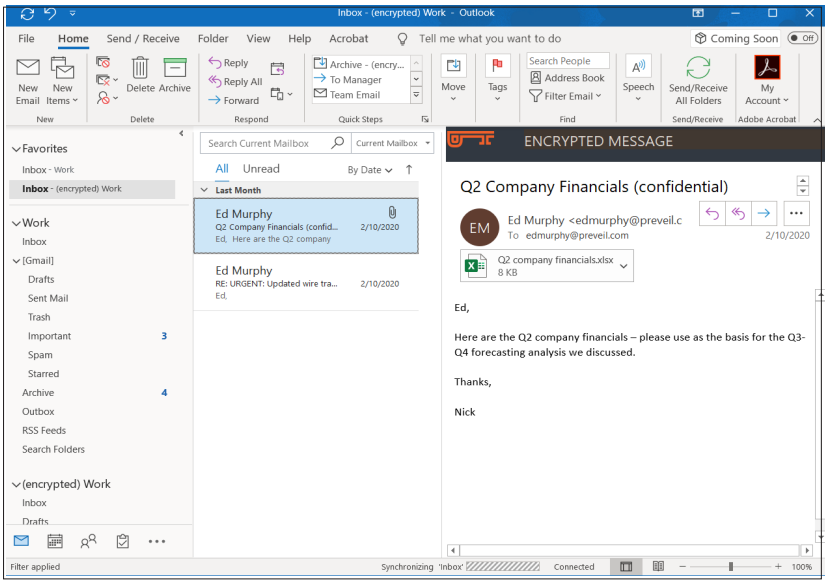
PreVeil also allows administrators to control access down to a device level. If a user's computer or phone has been lost or stolen, for example, the missing device can be locked to prevent further PreVeil access.

PreVeil Drive: Easy to unshare files and folders

PreVeil Email

PreVeil Email lets your employees and subcontractors communicate via end-to-end encrypted emails using their existing email addresses. It seamlessly integrates with mail clients such as Outlook, Gmail, and Apple Mail, and works on browsers and mobile devices as well. When PreVeil Email is used with Outlook, Gmail, or Apple Mail, the installation process automatically creates a new set of mailboxes for encrypted email messaging. Messages in these new mailboxes are encrypted and stored on PreVeil's servers. There are no changes to the mailboxes already in your employees' and subcontractors' mail programs, and there is no impact on the servers that store your regular, unsecure messages.

PreVeil Email: Encrypted inbox in Outlook



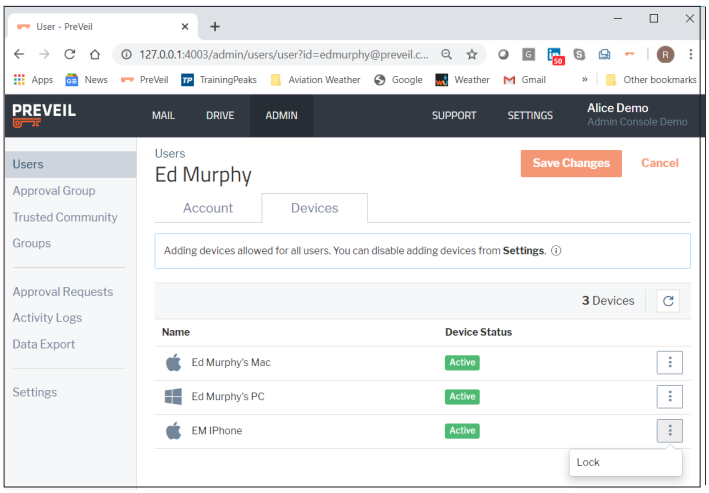
Trusted Communities

For both Drive and Email, PreVeil's Trusted Communities allow administrators to restrict communications to whitelisted domains and email addresses. This ensures that only members of a trusted community can exchange emails and files—virtually eliminating phishing and spoofing attacks.

Admin Console and Approval Groups

Using PreVeil's Admin Console, IT administrators can create, modify and delete users and groups, as well as set data and recovery policies both internally and that extend beyond their organizational boundaries to include subcontractors as well. Device management controls let admins disable lost or stolen devices quickly. Even though all files and emails are encrypted, admins have the tools they need to manage and access their organization's data and that which they've shared with their subcontractors. They can view activity logs and decrypt and export user data only with permission from a PreVeil Approval Group, a feature that prevents admins from becoming central points of attack. In essence, trust is distributed amongst approvers instead of being centralized with one admin.

Admin console: Device management controls



Key consideration no. 4: Compliance with federal regulations

PreVeil provides the foundation for compliance with federal regulations governing CUI. Specifically, PreVeil's Drive and Email solutions support compliance with:

- Current DoD regulations related to handling, storing or processing emails or files containing CUI, including DFARS 7012 and NIST 800-171. [1]
- The State Department's most up-to-date regulations requiring end-to-end encryption for communications governed by ITAR (International Traffic in Arms Regulations).
- CMMC level 3 mandates related to handling, storing or processing emails or files containing CUI, for primes and their subcontractors.[2]

1 Federal regulations mandate that any company that manufactures, exports or brokers defense-related articles, defense services, or is involved with related technical data must be ITAR compliant.

2 For complete details, PreVeil's CMMC white paper, which provides a high-level overview of the CMMC framework and its key components, also includes an extensive PreVeil CMMC Level 3 Compliance Matrix, a table that lists each of the required capabilities for CMMC Level 3 and indicates which requirements PreVeil meets.

Additionally, as described above, PreVeil's supply chain tools support compliance with the NSA's recent cybersecurity guidance for collaboration services for telework—which also describes the communications that happen between primes and their subcontractors at almost any time. The NSA's top recommendation is that such collaboration services use end-to-end encryption.

Key consideration no. 5: Cost effectiveness

PreVeil Drive and Email are a fraction of the cost of alternatives for several reasons:

- PreVeil's cost per user per month is significantly lower than alternatives.
- PreVeil need be deployed only to employees handling sensitive files and, data, whereas alternatives require deployment across an entire organization.
- PreVeil does not impact existing file and email servers, and so configuration and deployment are simple and, likewise, inexpensive.
- PreVeil's straightforward, light-touch solutions help avoid expensive CMMC consultant engagements, which are par for the course for some alternatives.

Best of all, PreVeil can be downloaded for free by your subcontractors for encrypted file sharing up to 100GB of data with each of them, along with unlimited encrypted email messaging, all at no cost. For example, if a prime needs to share manufacturing designs with dozens of its subcontractors, those subcontractors can download PreVeil for free in minutes and receive the design files via PreVeil's end-to-end encryption solutions, which meet all relevant federal cybersecurity regulations and preserve the supply chain.

PreVeil Case Study

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.

Table 1: PreVeil vs. alternatives

	PreVeil	Microsoft GCC High	Box Gov	On-Prem
Product	Email & files	Email & files	Files only	Email & files
Cybersecurity compliance architecture	Requires no reconfiguration, integrates seamlessly with email and file sharing tools already in use	Requires extensive and specialized compliance configuration	Requires extensive and specialized compliance configuration	Burden of architecting a secure and compliant on-prem platform
Security				
Encryption	End-to-end encryption	Optional key server (central point of attack)	Optional key server (central point of attack)	Security varies widely, requires in-house IT staff to manage patching and related security maintenance
Authentication	Key-based authentication	Password vulnerability	Password vulnerability	
Admin Control	Admin Approval Groups	Admin vulnerability	Admin vulnerability	
Whitelisting	Trusted Communities	None—vulnerable to phishing and spoofing		
Drive deployment	No impact to existing file servers Only users handling CUI need to deploy	Rip and replace file servers Typically must be deployed to 100% of organization	N/A	Varies widely
Email deployment	No impact to existing email servers Only users handling CUI need to deploy	Rip and replace email servers Typically must be deployed to 100% of organization	N/A	Varies widely
Business impact	Easily deploys in a matter of hours Easy to use	Months-long company-wide migration Retraining for all employees	Substantial upfront implementation effort Complex configuration and administration	Stresses capabilities of often small IT teams Reduces IT availability for critical business projects
Financial burden	Fraction of the cost vs. alternatives, and subcontractors can use for free (up to 100GB for file sharing; unlimited emailing) No major consulting contracts for implementation	Significant upfront migration fees License fees 2-3x O365, required for all employees	Set up and add-on modules required Expensive annual licensing	Hardware and software costs, IT person hours, and ongoing maintenance

Conclusion

DoD contractors need to exchange files and communicate securely both internally and with their suppliers. PreVeil offers world-class end-to-end encryption that enables secure collaboration throughout the supply chain. PreVeil Drive and Email are easy to deploy and simple to use, as they integrate seamlessly with the file sharing and email tools you already use—with no impact on your existing file and email servers.

PreVeil's light-touch solutions support compliance with DFARS 7012, NIST 800-171, ITAR and virtually all of the CMMC mandates related to the handling of CUI—for both primes and their subcontractors. PreVeil's FedRamp certification will be completed later in 2020.

To further support the DIB supply chain, PreVeil is free for the subcontractors of primes that install PreVeil. Primes and their suppliers can use PreVeil Drive for up to 100GB of encrypted file sharing, and PreVeil Email for unlimited encrypted email messaging.

But better security at low cost isn't enough: if security is difficult to use, it won't be used. To be effective, security must be as frictionless as possible. PreVeil was created with this principle in mind to help your organization achieve its security objectives and, likewise, to help secure the DIB supply chain.

To learn more about PreVeil, visit us at www.preveil.com/contact/.

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.

Additional copies of this paper can be downloaded at www. preveil.com/supply-chain-whitepaper.

PREVEIL

June 2020 v1