PREVEIL

PreVeil's End-to-End Encryption Enables ITAR Compliance

The U.S. State Department has recently taken action that recognizes that technological advances in cybersecurity can simplify ITAR compliance without compromising national security goals. Newly-revised International Traffic in Arms Regulations (ITAR) now allow for the exchange or sharing of unclassified defense-related technical data provided that:

- the technical data is end-to-end encrypted; and
- no cloud services provider has access to keys, network access codes, or passwords that enable decryption.

Unclassified defense-related technical data is information and software required for all aspects of a defense article's life cycle—from design through operation, maintenance and modification.

Specifically, the new rule, effective March 25, 2020, states that unclassified defense-related technical data secured using end-to-end encryption that meets standards specified in FIPS Publication 140-2 is no longer considered an ITAR-controlled export and, likewise, is free of the rules governing those exports.

Previously, organizations subject to ITAR's export rules have had to use complex and expensive servers and software that was difficult to deploy, maintain and administer. Now they will be able to simplify and cost-effectively streamline their internal data storage and sharing practices by moving unclassified defense-related technical data into the cloud—provided that data is end-to-end encrypted, and can only be decrypted by the intended recipient and never by a provider.

The new ITAR guidelines also make it much easier to comply with requirements when employees travel to and or access ITAR-restricted data while in foreign countries. Previously they had to file a lot of paperwork and get special licensing for those employees to access ITAR data abroad. With the new carveout, they are freed of the burden of compliance overhead and it is much easier for their employees operating oversees to do their job.

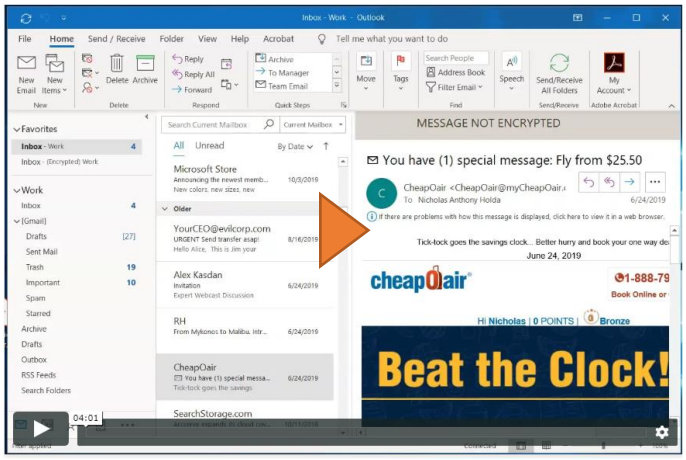
PreVeil Email and Drive meet ITAR standards

PreVeil's security architecture is grounded in world-class end-to-end encryption that meets ITAR standards. It's based on MIT computer scientists' research in cybersecurity and applied cryptography. With PreVeil, email, files and data are only ever encrypted and decrypted on a user's device. Information is never decrypted on any server anywhere. If attackers breach a server, all they will get is useless gibberish because the server never sees plaintext data. PreVeil captures every email and file sharing transaction that contains ITAR data in immutable logs that support ITAR compliance and enterprise security standards.

PreVeil complies with the second critical component of the new ITAR standards—that no cloud services provider has access to keys, network access codes, or passwords that enable decryption—because PreVeil doesn't have any access to user keys, ever. Private keys are stored on user devices. Keys stored on the server are encrypted, ensuring an attacker can never access them.

PreVeil Email lets your employees send and receive encrypted emails containing data subject to ITAR using their existing email address. It integrates seamlessly with Outlook and Gmail clients, as shown in screen shot below, and works on browsers and mobile devices. The installation process automatically creates a new set of mailboxes for your encrypted messages. Messages in these new mailboxes are encrypted and ITAR compliant. There are no changes to the mailboxes already in your mail program and no impact on the servers that store your regular, unsecure messages.

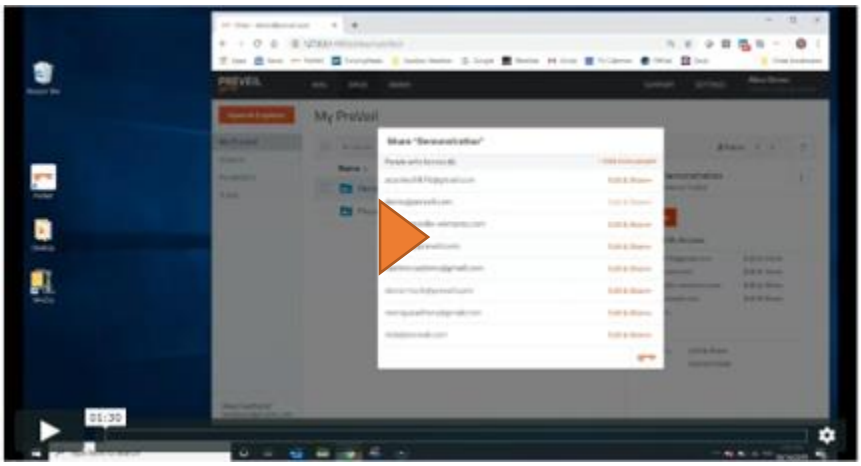
Preveil Email: Video demonstration



PreVeil Drive enables end-to-end encrypted file sharing and storage of data subject to ITAR. Users can access files stored on PreVeil Drive from any of their devices, or share files with other users who have the appropriate access permissions through PreVeil's Trusted Communities.

PreVeil Drive is easy to use and functions like Dropbox, Google Drive or OneDrive, as shown in the screen shot below. But unlike those alternatives, which allow the server to access your decrypted data, with PreVeil Drive only you and the people with whom you've explicitly shared files can decrypt them. In accordance with the new ITAR ruling, PreVeil servers store only encrypted data and have no ability to access keys to decrypt it. PreVeil Drive automatically integrates with Windows File Explorer and Mac Finder and has no impact on your existing file servers. It's available for Windows, Mac and, with PreVeil's mobile app, for smartphones, iPads and tablets.

Preveil Drive: Video demonstration



PreVeil's advanced key management

PreVeil's key management system meets ITAR standards by eliminating key servers and the central points of attack they present. PreVeil enables sharing, storage and revocation of encrypted data from user devices while hiding the complexities of key management, as the process occurs automatically. On the other hand, some encryption systems centralize the storage of decryption keys in a key server. Doing so undermines the benefits of encryption because attackers can focus their efforts on penetrating the key server, which if successful would ultimately compromise all of the encrypted data. That's why the new ITAR rule specifies that companies will be held liable if "access information"—such as decryption keys, network access codes, and passwords—is used by unauthorized persons to receive unencrypted technical data. PreVeil eliminates that possibility.

Elimination of passwords

PreVeil also eliminates passwords, another common point of vulnerability. Instead of relying on passwords, PreVeil authenticates users via strong cryptographic keys that are automatically created and stored on users' devices. Replacing passwords with cryptographic keys shuts down the many significant security risks that flow from phishing and password-guessing attacks, including the use of compromised passwords for unauthorized access and malicious activity. And again, because the keys are stored are user's devices, hackers cannot remotely log into user accounts.

In short, PreVeil offers an elegant solution to help your company comply with ITAR's new end-to-end encryption rule.

Keep in mind, too, that PreVeil's email and file sharing service is a fraction of the cost of alternatives: And as explained above, PreVeil's low touch on your existing infrastructure makes configuration and deployment simple and inexpensive.

PreVeil leverages a fundamentally better security paradigm to help companies achieve compliance with ITAR. But better security 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 so that all your security objectives will be met.

To learn more about PreVeil, contact us

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/itar-whitepaper.

June 2020 v1