

# PreVeil for Aerospace & Defense

## *DoD Cybersecurity Standards: No Longer Optional*

### Shift from Self-Assessments to 3<sup>rd</sup> Party Audits

Beginning in 2020, the DoD's cybersecurity enforcement model will drastically change:

- Cybersecurity Maturity Model Certification (CMMC) audits required of all suppliers
- Certified cybersecurity audit results required to participate in RFPs
- Significant business risk for contractors who fail to comply

### DoD Cybersecurity Compliance Standards are Expanding

Contractors are required to meet the CMMC level established by the contract officer.

CMMC levels include:

- **Level 1:** Basic Hygiene. Required of all 300,000 DoD contractors.
- **Level 3:** Good Cyber Hygiene. Required of all A&D contractors handling CUI.
- **Level 4-5:** Proactive to Advanced Cyber Hygiene. Required for critical programs.

---

## PreVeil Helps A&D Suppliers Accelerate Cybersecurity Compliance

### Securing CUI Against Breaches

- **End-to-end encryption:** Protects CUI in email and files at all times
- **Cryptographic authentication:** Eliminates common credential attacks
- **Trusted Communities:** Enables contractors to control the flow of CUI

### Easy to Deploy and Use

- **Ease-of-use:** Native integration with Outlook, Gmail, File Explorer, mobile
- **Minimal business disruption:** No changes to existing IT infrastructure
- **Compliant data storage:** Encrypted data resides on AWS GovCloud or on-prem

### Cost Effective

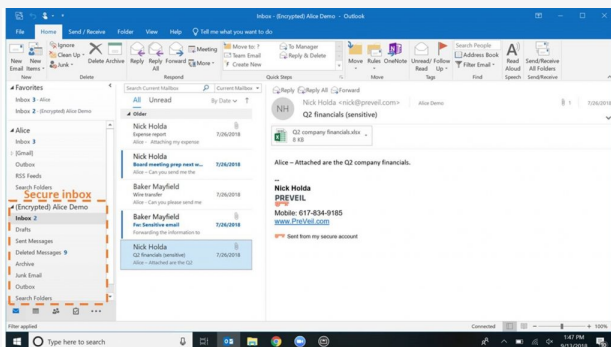
- **Affordable pricing model:** Significantly less expensive than alternatives
- **No setup fees:** Zero implementation and configuration fees
- **Limit licensing fees:** Only pay for users that need to touch CUI

# Securing CUI for Aerospace & Defense Companies

PreVeil is a highly secure email and file sharing service that provides Aerospace & Defense suppliers with an out-of-band communication channel that leverages a fundamentally better security paradigm. PreVeil's end-to-end encryption architecture (born out of MIT research) ensures email and file contents stay protected even when networks/servers are breached, employee passwords are stolen, and IT Administrator accounts are compromised.

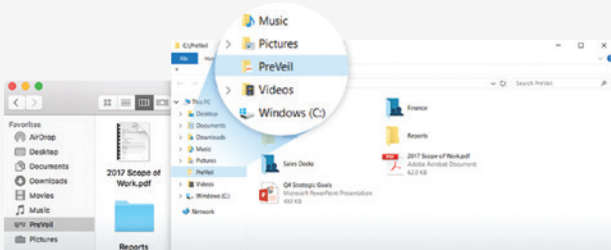
## PreVeil's secure email & file sharing service is seamlessly integrated for end users

**PreVeil Email ("Trusted Mailbox")** Delivers a highly secure, complementary mailbox right next to users' ordinary mailbox (using their same email address). Users get to keep using Outlook, Mac Mail, Gmail, iOS, and Android just like they do today.



## PreVeil Drive

Users can easily store, sync, and share sensitive files containing DoD CUI – internally and with 3rd parties – protected with end-to-end encryption.



## Admin Console

Provision and manage user accounts, access corporate data when required, and monitor logs. Optional integration with Active Directory.

## PreVeil was built from the ground up using a fundamentally better security paradigm

### Data stays encrypted all the time

End-to-end encryption protects data even when servers and networks are breached.



### Users authenticate via device-based keys

Encryption keys stored transparently on user devices are required to access sensitive data



### Protection against catastrophic IT Admin breach

Patented Approval Groups™ enable privileged access without granting any one admin keys to the kingdom.



**Trusted Communities** Enables you to control flow of CUI and other sensitive information, and isolate users from phishing and spoofing.



*...all combined with incredible Ease of Use*