PreVeil for CMMC Compliance

What is CMMC?

The CMMC measures a company's ability to protect FCI (Federal Contract Information) and CUI (Controlled Unclassified Information). It outlines five levels of cybersecurity maturity required to work on DoD projects, ranging from basic cyber hygiene practices at Level 1 to highly sensitive practices and processes at Level 5.

What does it mean for my business?

The biggest change from previous practice is the shift from self-assessment of cybersecurity compliance to required external audits. All contractors wishing to work with the DoD must be certified by a CMMC Third Party Assessment Organization (C3PAO) at the CMMC maturity level appropriate to their DoD work.

Companies that work with or generate CUI will need to achieve CMMC Level 3 at a minimum.

How do I get started?

1. Perform a baseline of current cybersecurity hygiene.
2. Identify gaps between your organization's current capabilities and the requirements for the CMMC maturity level you seek to achieve.
3. Develop a plan to help guide you toward closing gaps and implementing needed IT systems and processes.

Why companies choose PreVeil?

Defense companies must protect CUI within their company and within their supply chain. PreVeil delivers exceptional security that is easy to deploy and use, is highly affordable and supports CMMC Level 3 compliance.

| Business impact	PreVeil	Microsoft GCC High
CUI Protection	End-to-end encryption for email and files. Purpose built to protect against modern cyber attacks.	Vulnerable to modern attacks. Relies on antiquated security model.
Deployment	Only needs to be deployed to users handling CUI. No changes to existing IT infrastructure.	Company-wide implementation. High risk of business disruption.
Economics	Simple, all inclusive user license fee for subset of users.	Expensive. Requires several product suites + $30-50k initial setup fees.
Compliance	Enables DFARS 7012, NIST 800-171, and ITAR compliance out of the box.	When custom configured, enables compliance on virtually all relevant controls.

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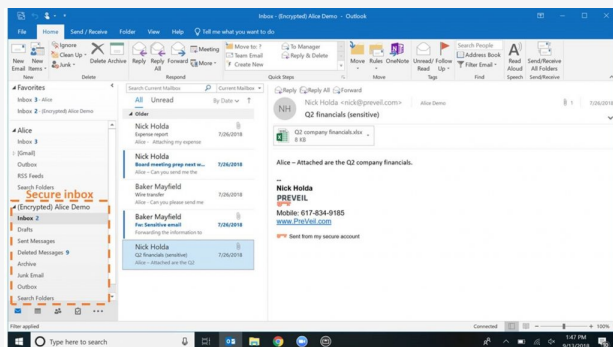
PreVeil Drive
Users can easily store, sync, and share sensitive files containing DoD CUI – internally and with 3rd parties – protected with end-to-end encryption.

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 isulate users from phishing and spoofing.

...all combined with incredible Ease of Use