6 Myths about Storing and Protecting CUI

Guidance for Safeguarding Controlled Unclassified Information

1. **If an enterprise handles CUI, the entire enterprise IT environment must be CMMC level 3 compliant**

   The documentation for the CMMC model v1.02 states that: "when implementing CMMC, a DIB contractor can **achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s)**, depending upon where the information to be protected is handled and stored."

   The DoD has approved the enclave model for CMMC compliance.

2. **Defense contractors must use Microsoft GCC High because many of the DoD agencies use it**

   Agencies within DoD do not typically rely on GCC High but instead use their own DoD-only cloud for storage and sharing of CUI.

   Further, the DoD has never required contractors to use a particular solution. To the contrary, the DoD has only stated that contractors must meet the compliance framework set out by the DoD for the protection of CUI within their own certification boundary and when flowing down CUI to subcontractors.

3. **Cloud Service Providers (CSPs) must be listed in the FedRAMP Marketplace to handle CUI**

   The FedRAMP Marketplace only includes service providers with an Authority to Operate (ATO) with the Federal government. These providers have been sponsored by a Federal agency and can provide services to those agencies. ATO is not required for providing cloud services to private enterprises supporting federal agencies.

   For service providers supporting private contractors to the DoD, the DFARS 7012 requirement is for FedRAMP Moderate baseline. Here is the excerpt from the DoD's 7012 document itself (252.204.7012 - b.2.ii.d):

   > If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident

> reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

DFARS does not stipulate that contractors use a CSP service authorized/approved by the FedRAMP ATO program. Instead, the standard simply requires contractors ensure that the CSP will process and store covered defense information to the same set of requirements.

4. **CSPs are required to accept DFARS 7012 flow downs.**

According to the DoD Procurement Toolbox’s Cybersecurity FAQs:

> The contractor does not normally ‘flow down’ the DFARS clause to the CSP but must ensure, when using a CSP as part of his covered contractor information system, that he can continue to meet the DFARS clause requirements, including the requirements in DFARS clause 252.204-7012 (c)-(g).

PreVeil supports our customers that accept the flow down of these DFARS requirements – something that commercial Microsoft O365 services will not do.

5. **If a DoD user sends a regular, unencrypted email with CUI to a defense contractor, that represents a data breach.**
   If a user sends a regular email with CUI to a contractor, it is typically termed a “Security Incident” for the subcontractor – not a breach. They escalate and log it internally and then engage in any clean-up of residual CUI content in the non-compliant email system These types of incidents will not prevent a contractor from bidding on future DoD contracts.

6. **Historically, proper marking of CUI has not been adhered to. As a result, subcontractors need to assume that all content could be CUI.**
   While proper marking has clearly been a problem in the past, the National Archives’ CUI marking initiative mandates proper marking of documents and email containing CUI starting Jan 2021. All CUI flowed down to contractors that are part of DoD programs that dictate CMMC compliance must use proper marking. If a subcontractor believes that an email or document received from a customer not marked as CUI is actually CUI, they should validate this with the sender’s organization.