Streamline CMMC Compliance with Egnyte

Background
After a major change to CMMC 2.0 by the Department of Defense (DoD). CMMC transitioned from five total compliance levels to three. Level 2 of the new model is now 100% aligned to the National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171). Additionally, the DoD provides guiding principles as referred to in the CMMC Assessment Guide Level 2, Version 2.0, from December 2021.

CMMC is designed to provide assurance to the DoD that a Defense Industrial Base (DIB) contractor can adequately protect Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for the information flow down to its subcontractors in a multi-tiered supply chain.

A contractor can achieve a CMMC certification for an entire enterprise network, for specified segments, or for a specific enclave, depending on how their assessment is scoped. Prior to conducting a CMMC assessment, the contractor must specify the CMMC assessment scope. The assessment scope informs which assets will be assessed within the contractor’s environment.

Penalties for Non-Compliance to DFARS Cybersecurity Requirements
The DoD issued a memo in June 2022 that directed Contracting Officers to enforce penalties on DoD contractors who fail to comply with DFARS Clauses 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) on certain contracts. Currently, DFARS 7012 mandates DIB orgs to self-attest to NIST 800-171 compliance, while DFARS 7019 makes those scores available to DoD officials. As a result, you need to begin compliance now.

Why Egnyte
Egnyte provides a Cloud-based, Secure Data Enclave to help reduce your assessment environment scope and streamline the assessment journey.

The enclave is:
- **Secure:** With inherited controls from EgnyteGov’s SaaS environment and Google Cloud Platform (GCP) Services’ - FedRAMP High data center infrastructure.
- **Fast:** Provisioning of 30 Egnyte Platform Configuration settings and associated documentation explicitly satisfies related CMMC / NIST 800 171 practice area and control objectives.
- **Assessment Management-Friendly:** Maintenance of the compliance journey via the Assessment Dashboard with management and access controls, record-keeping, and insights.
- **Trusted:** An experienced support team is in your corner, with deep technical knowledge of CMMC.
- **Cost-Effective:** Purchase only what you need, for the users who need it.
The Egnyte Solution

Egnyte for CMMC provides organizations that handle CUI with a secure environment for file sharing and collaboration, along with intelligent self-assessment and control documentation tools that support ongoing compliance. The unified solution is a cost-effective way to streamline the time to compliance and increase productivity for teams who manage CUI.

Gather
- Auto-tagging of CMMC files
- Discovery and classification of CUI data in targeted repositories
- Advanced metadata labeling

Control
- Technically-isolated, fully-managed CMMC enclave (with configured controls and a secure infrastructure)
- Controlled sharing framework for internal and external users
- Threat management to detect and mitigate potential attacks

Audit
- Auto-populated CMMC artifacts and audit response
- Built-in assessment dashboard and tools to complete and measure your compliance journey
- Monitoring of all data sources for CMMC files

Take the Next Steps with a CMMC Workshop
- Meet with Egnyte’s CMMC Subject Matter Experts
- Gain insights into your CMMC / DoD contract requirements (for Prime and Sub-Contractors, etc.)
- Discuss your current state of CMMC certification and your compliance journey
- Walk through the Egnyte for CMMC solution
- Discuss how Egnyte for CMMC’s capabilities will meet your needs

For more information about CMMC Compliance, take an Egnyte Product Tour or visit egnyte.com/solutions/cmmc-compliance.