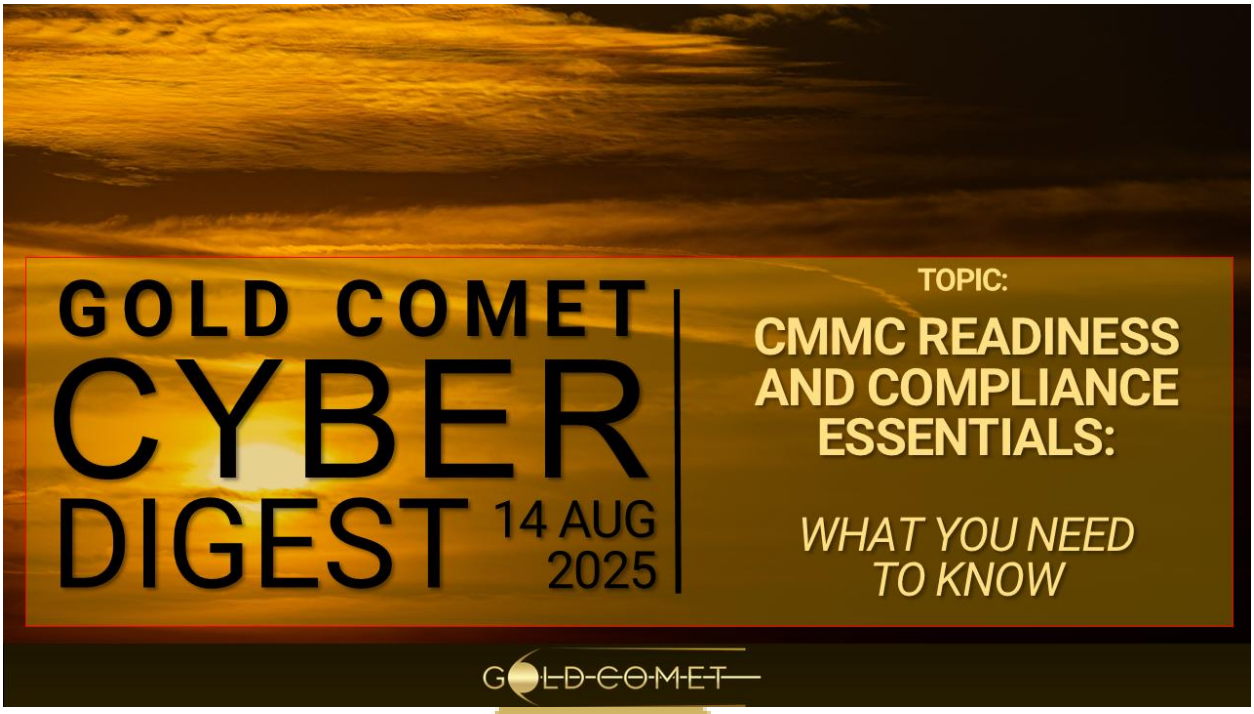

Welcome to the first issue of Gold Comet's Cyber Digest! Twice a month here on the Gold Comet blog, we'll be posting on cybersecurity topics and critical issues of interest to the cybersecurity administration community of decision-makers. Feel free to share this digest (in its entirety) with your colleagues and share your comments on these postings. You can download a copy – see the link below. We look forward to continuing to be a leading resource for secure data management information. This August 2025 issue will focus on CMMC Compliance – it's changing contract life in the DIB!

1. Why CMMC Compliance Matters (and What's New)

It's been nearly two years since the U.S. Department of Defense rolled out **CMMC 2.0**, and many contractors and subcontractors in the Defense Industrial Base (DIB) are still scrambling to meet even **Level 2** requirements. Now more than ever, contractors and subcontractors, especially those in regulated industries, must demonstrate clear compliance. Missing certification can mean inability to qualify for bids, revocation of existing contracts, or fines from DFARS violations. Recent actions by the DoD are raising the stakes.

2. Recent Developments in CMMC and Compliance

- **DoD Preparing for Level 3 Introductions:** The DoD has reaffirmed 2026 for Level 3 rollout, with expectations for foundational cybersecurity hygiene to be complete by early 2026. While Level 2 remains the most common target, the rise in sensitive data requirements is paving the way for Level 3 demands, including proactive detection and automated incident response. **Level 2 requirements are now showing up in DoD solicitations as mandatory.**

- **CISA "Compliance Readiness Alerts:"** DoD suppliers are being notified to prioritize encrypted file sharing, identity controls, and audit trails to avoid breaches and supply chain disruptions.

- **Ongoing DFARS Clarifications:** Updates emphasize that contractors must ensure both file transfers ***and storage*** meet NIST 800-171 standards. This includes email/messaging, and cloud links, which are all now under scrutiny.

- **Assessment Failures:** Over 300 companies have failed to pass recent third-party assessments due to documentation and system control gaps.

3. CMMC Certification Essentials: What, Why, and the Levels

- **Level 1 (Foundational):** Basic safeguarding practices, primarily focused on handling Federal Contract Information (FCI), such as passwords and low level access controls.

- **Level 2 (Advanced):** The standard level required for managing Controlled Unclassified Information (CUI). Requires implementation of NIST 800-171 controls across 14 domains including access, encryption, incident response, and audit logging.

- **Level 3 (Expert):** Still emerging. Builds on Level 2 with advanced cybersecurity hygiene, organizational maturity, and sophisticated threat intelligence integration.

4. Steps to Prepare for CMMC Readiness

1. **Classify Your Data**
   Understand the difference between FCI and CUI. Run a quick audit to determine where and how your data files, cloud drives, emails and other messaging are stored.

2. **Build Your SSP (System Security Plan)**
   Document how your systems implement each NIST 800-171 control. Map it out on a spreadsheet and make sure it's accurate.

3. **Create Your POA&M (Plan of Action & Milestones)**
   For any control you can't fully meet immediately, define the gap, responsible owner, remediation path, and timeline to resolve.

4. **Enforce Access Controls and Encryption**
   Ensure that sensitive files are encrypted at rest and in transit, and that access is based on user roles and need to know.

5. **Enable Continuous Monitoring & Audit Trails**
   Log file access and messaging events. Regularly review for unauthorized downloads or

access attempts, and policy violations.

6. **Test and Update Regularly**
   Conduct tabletop exercises around "what if" breach scenarios. Update your POA&M and SSP quarterly or whenever your tech stack changes.

5. Top 5 CMMC Readiness Pitfalls in 2025

Organizations continue to face issues in these critical areas:

1. **Insecure File Sharing Practices**
   Many still use FTP, Dropbox, or shared drives that lack encryption at rest and in transit.

2. **Unmonitored Messaging Channels**
   Internal communication platforms such as Teams, Slack, and commonly used email applications often don't meet auditability or confidentiality requirements.

3. **Over-Reliance on IT to Manage Compliance**
   Executives often assume the IT team "has it covered," even when no formal SSP (System Security Plan) is in place.

4. **Third-Party Vulnerabilities**
   Lack of vendor compliance monitoring can cause downstream risk inheritance.

5. **No Centralized Control or Reporting**
   Many organizations lack a singular view of how data is being accessed, stored, or shared.

Case Study: Aerospace Subcontractor, Mid-Tier Defense Vendor

- **Situation:** A mid-tier aerospace subcontractor lost a contract because they shared CUI over unsecured cloud links. Their storage and messaging lacked audit visibility and encryption—despite believing they were "secure enough."
- **Outcome:** After failing a DoD audit, they engaged a secure collaboration platform aligned with Zero Trust. Within 60 days, they implemented encrypted storage, messaging, and audit logging, passed their recertification, and got their contract back.
- **Lesson:** Compliance isn't a checkbox- It's continuous, latent risk mitigation.

6. How Gold Comet Supports CMMC Compliance

- **End-to-end Encryption** – Protects CUI during storage and sharing, addressing NIST access and encryption controls.
- **Role-based Access & Zero Trust** – Ensures only authorized users can view sensitive data.
- **Immutable Audit Trails** – Bullets through NIST and DFARS logging requirements with real-time visibility.

- **Built-in Compliance Documentation** – Export logs and summaries for your SSP and audit prep.

The Gold Comet platform is built for CMMC Data Management Compliance, designed from the ground up to align with CMMC, NIST, and DFARS requirements:

CMMC Requirement	Gold Comet Feature
Access Control (AC)	Role-based permissions with full object level encryption.
Audit and Accountability (AU)	Immutable activity logging and alerts.
System and Information Integrity (SI)	Closed-loop system prevents external malware injection.
Configuration Management (CM)	Admin-managed security defaults—users can't alter policies.
Media Protection (MP)	All data encrypted at rest & in transit—no third-party exposure.
Identification and Authentication (IA)	MFA + identity-first platform controls.

🔐 *NOTE: Gold Comet is not a C3PAO and does not provide certification, but we help you get compliant faster, with less operational burden.*

7. In the Next 30 Days …

If you haven't already started preparing, here's what you should do next:

Step 1: Reassess your current file sharing, data storage, and internal communication tools.

Step 2: Map each of them against CMMC 2.0 Level 2 controls.

Step 3: Identify tools that provide secure by default architecture, not patchwork policies.

Step 4: Request a demo of Gold Comet's secure collaboration suite or book a 30-minute no cost consultation call.

Step 5: Follow us on LinkedIn for weekly insights and new product and webinar announcements.

CLICK TO LEARN MORE ABOUT CMMC SUPPORT AND HaloCONNECT FOR ZERO TRUST COLLABORATION!

HaloCONNECT
Powered by Gold Comet

The Gold Comet™ Solution is a multi-patented, quantum-integrated data storage, data sharing and messaging platform designed on zero-trust principles and protectively housed within its own secure cloud environment. Our patented Object Level Encryption and FISMA high-rated, penetration-tested process provides users with the ultimate level of data integrity. The Gold Comet™ platform allows its users to securely store valuable information such as proprietary data, intellectual property, personnel records and PII, PHI and healthcare information, supply chain and legal records – virtually any information that needs to be protected from cyberthreat activity.