ISI

CMMC AWARENESS CHECKLIST FOR FSOs

PURPOSE

This checklist helps Facility Security Officers (FSOs) understand their responsibilities and support their organization's compliance with the Cybersecurity Maturity Model Certification (CMMC), particularly where it intersects with industrial security and NISPOM obligations.

1. Understand the Framework

- ☐ Know what CMMC covers: protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
- ☐ Understand how CMMC aligns with NIST SP 800-171 controls.
- ☐ Recognize that CMMC applies to unclassified systems, not the classified networks under NISPOM.
- ☐ Review how CMMC 2.1 defines assessment levels (Level 1, 2, and 3) and which applies to your contracts.

2. Identify Where CUI Resides

- ☐ Work with program managers and IT staff to identify where CUI is stored, processed, or transmitted.
- ☐ Verify that CUI systems are segmented from classified or public networks.
- ☐ Ensure all personnel handling CUI are cleared, trained, and briefed appropriately.
- ☐ Confirm CUI is marked, stored, and destroyed according to DoD and contract guidance.

CMMC AWARENESS CHECKLIST FOR FSOs

3. Align Policies and Procedures

- [ ] Review company security policies to ensure CUI handling is explicitly addressed.
- [ ] Align insider threat, incident reporting, and physical access procedures with CMMC requirements.
- [ ] Verify that personnel and physical controls described in the System Security Plan (SSP) match current practice.
- [ ] Confirm your facility's Information System Security Manager (ISSM) and IT security leads are coordinating on both classified and CUI environments.

4. Support Assessment Readiness

- [ ] Know whether your company is pursuing self-assessment (Level 1) or third-party certification (Level 2+).
- [ ] Ensure security training includes a module on CUI handling and cyber hygiene.
- [ ] Support documentation readiness:
  - Security System Plan (SSP)
  - Plan of Actions and Milestones (POA&M)
  - Incident response plan
- [ ] Confirm that physical security controls—locks, access logs, and visitor procedures—support CMMC compliance.

5. Coordinate and Communicate

- [ ] Maintain communication with:
  - Compliance officers / CMMC lead
  - IT / cybersecurity team
  - Program management
  - DCSA representatives (for alignment between NISPOM and CMMC)
- [ ] Include CUI awareness in all security briefings and refresher trainings.
- [ ] Encourage reporting of potential cyber incidents involving CUI, not just classified information.

6. Monitor and Maintain

- [ ] Stay updated on DoD and DCSA guidance related to CMMC implementation.
- [ ] Track any policy or DFARS clause changes that introduce or update CMMC requirements.
- [ ] Periodically re-evaluate internal processes to ensure ongoing readiness.
- [ ] Document lessons learned from DCSA reviews and apply them to CMMC controls.

7. Key Takeaway

CMMC compliance is a team effort, but FSOs play a critical role in bridging physical, personnel, and information protection. By embedding CUI awareness into your security culture, you help ensure readiness for both DCSA assessments and CMMC audits.