ENTERPRISE SECURITY OPERATIONS | DCSA CUI PROGRAM OFFICE

A ROADMAP TO CUI COMPLIANCE

CONTROLLED UNCLASSIFIED INFORMATION

Developing a Foundational CUI Program

This roadmap will assist industry in developing a Controlled Unclassified Information (CUI) program and provides 11 key areas which industry can focus on to become compliant with CUI requirements.

Conduct Initial Self-Assessment | **Information System (IS) Security Controls Familiarization** | **CMMC Requirements and Level Identification** | **Conduct Full Assessment**

Customer Engagement | **Safeguarding & Access** | **SPP Development**

Identifying Key Personnel | **CUI Training** | **Policy Documents** | **Contract Identification**

BUILDING THE FOUNDATION OF A CUI PROGRAM

1. Identifying Key Personnel
- Senior Management
- Facility Security Officer
- Information Technology (IT) Manager/ISSM
- Insider Threat Program Senior Official
- Network Engineers
- Program Managers
- Contracting and Acquisition Professionals

2. CUI Training
- 11 CUI training requirements
- CDSE courses
- Required annually (DOD)

3. DOD Policy
- DODI 5200.48
- NIST SPs
- CUI Policy

4. Contract Identification
- DD Form 254 review
- Review contracts
- Review legacy information

5. Customer Engagement
- Review SCGs
- Engage customers
- Understand contractual requirements

6. Safeguarding & Access
- How is it stored?
- Who has access?
- Long term storage
- Access hours
- Encryption requirements
- Decontrol and destruction
- Leveraging resources

7. SSP Development
- Facility security procedures
- Facility CUI contacts
- Information system security policies
- Contractual-specific guidance
- Safeguarding and Marking
- Reporting

8. Conduct Initial Self-Assessment
- Review results
- Correct findings
- Identify opportunities
- Make improvements

9. IS Controls
- NIST SP 800-171
- NIST SP 800-172

10. CMMC 2.0 Implementation (https://www.acq.osd.mil/cmmc/index.html)
- Implemented through the acquisition and contracting process.
- Requires compliance with CMMC as a condition of contract award.
- CMMC level will be specified in the solicitation & RFIs, if utilized.
- Key features identified in the CMMC Model Structure.
  - LVL 3 Expert (110+ NIST SP 800-172 Controls); USG-led Triennial Assessments
  - LVL 2 Advanced (110 NIST SP 800-171 Controls); Self-Assessments or Triennial Third-Party Assessments
  - LVL 1 Foundational (17 NIST SP 800-171 Controls); Annual Self-Assessments

11. Conduct Full Assessment
- Evaluate program
- Report findings to management
- Mitigate findings
- Identify program improvements
- Enhance program