Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cyber Training

Cyber/Cybersecurity Maturity Model Certification (CMMC) v2.0

CyberAssist

Agenda

- Module 1: Cybersecurity: Why it is Important?
- Module 2: Cybersecurity Maturity Model Certification
- Module 3: Assessment Process - Interim
- Module 4: Incident Reporting
- Module 5: Cybersecurity Best Practices
- Module 6: Risk Management
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- CMMC Domains
- Survey

Incident Reporting

Module 4

Disclaimer and Overview

Note: CMMC is still going through the rule-making process and certain aspects and requirements may change. Refer to the *Resources Guide* provided in this training for the most updated information.

- The intent of this training is to build awareness for Defense Industrial Base (DIB) suppliers of the likely requirements of the Cybersecurity Maturity Model Certification (CMMC) and their obligation to meet FAR 52.204-21 (basic cyber hygiene) and DFARS 252.204-7012 (specialized data handling and protection requirements).
- This training is self-paced and intended for a range of roles and responsibilities including, but not limited to, executives, project managers and technical staff from organizations seeking certification (OSC) and need to comply with CMMC. Currently, CMMC does not apply to any contractor.
- Note: Completion of this training DOES NOT certify your organization. This training is intended for the purposes of providing awareness of the subjects outlined above.
- The DIB Sector Coordinating Council (SCC) Supply Chain Task Force does not take responsibility for suppliers' certification by the CMMC 3rd Party Assessment Organization (C3PAO).
- This training focuses on U.S. regulations and industry best practices:
  - U.S. Department of Defense (DoD) Chief Information Officer (CIO) Cybersecurity Maturity Model Certification (CMMC) Information
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - DIB SCC Supply Chain Task Force – CyberAssist website

Module Topics and Objectives

Helpful Hint:
Refer to the Resource Guide for a Glossary and Acronym Guide

Topics covered in this module:

- Common Cyber Incidents
- Cyber Incident Reporting Tips
- Cyber Incident Reporting – CMMC Level 2

The objectives of this module are:

- Provide understanding of common cyber incidents; and
- Provide understanding of cyber incident reporting tips.

A legend has been provided to assist with determining the content that you will need to know for each of the CMMC levels and what is additional content that will assist your organization with your cybersecurity posture. The corresponding symbol will be located at the top left corner of the slide.

Content Legend

CyberAssist

Cyber Incident Reporting

Our customers count on our products and services to support their mission each and every time. This includes timely reporting if information is compromised or exposed to unauthorized parties.

Cyber incident reporting is the process of reporting any actual or potential cyber incidents to the appropriate authority or organization.

Common Cyber and Security Incidents

The most common types of cyber and security incidents include:

- social engineering (e.g., phishing email)
- emailing sensitive information to unauthorized people
- unauthorized access to sensitive information from outside the organization (e.g., via compromised account credentials)
- lost laptops and mobile devices
- insider threats
- malware / ransomware

Cyber Incident Reporting Tips

Report all cyber incidents… even if reporting is not mandatory.

- Prompt reporting of actual and suspected security incidents can help prevent or limit the severity of an incident

Report incidents in a timely manner to avoid harm to your company's reputation and resources

- Comply with contract requirements for prompt incident reporting (e.g., 72 hours after discovery)
- Notify stakeholder points of contact per contract requirements (typically the buyer or subcontract manager / administrator)
- Follow any specific internal reporting requirements for your organization

Security incidents may include loss, theft, misuse, tampering, corruption, unauthorized disclosure of information, or when an individual violates controls intended to limit their access to information.

Cyber Incident Reporting – CMMC Level 2

- Organizations seeking to achieve CMMC Level 2, to be eligible for DoD subcontracts involving CUI should be aware…
  - Contracts involving CUI invoke DFARS 252.204-7012 with mandatory cyber incident reporting requirements
  - Report incidents to DoD (DIBNet site) within 72 hours of discovery
  - A Medium Assurance Certificate is required to report a cyber incident, applying to the DIB CS Program is not a prerequisite to report
  - DoD DIBNet and DFARS 252.204-7012 provide detailed guidance on required actions following a cyber incident

Ensure regulatory reporting requirements are understood when advancing to CMMC Level 2 (managing CUI)

Next: Module 5 - Cybersecurity Best Practices