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

Cybersecurity: Why is it Important?

Module 1

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:

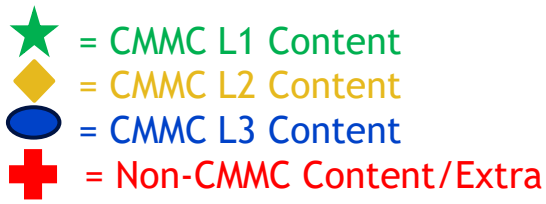
- What is Cybersecurity?
- CIA Triad
- Why it is important?
- Are your IT environments protected? Is your information protected?
- Module Summary

The objectives of this module are:

- Provide understanding of the importance of cybersecurity;
- Provide understanding of the CIS Triad; and
- Provide understanding of who is at risk.

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

What is Cybersecurity?

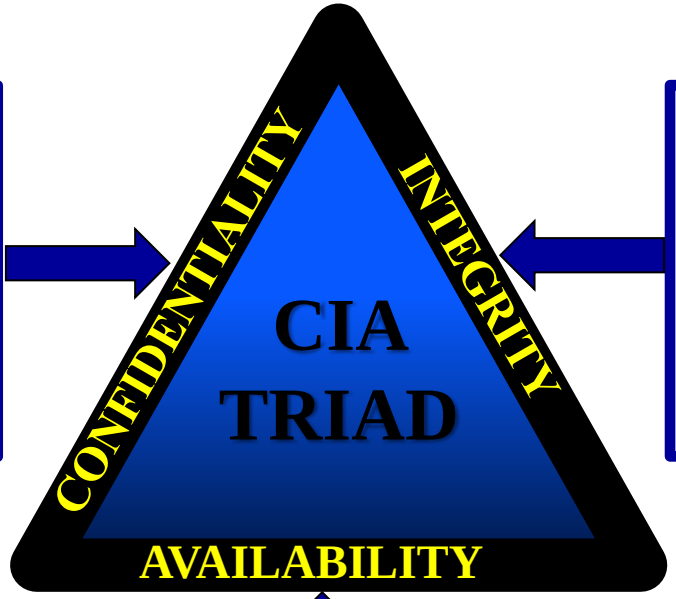
- All the tools we use and actions we take to keep computers, networks, and information **safe and available** for those who need it, and unavailable for those who should not have it.
- That means **protecting** hardware, software, people, and data from everything from cyber attacks to earthquakes.

Cybersecurity is about keeping our information technology (IT) resources secure (confidential, available, and unaltered).

CIA Triad

Confidentiality

Ensuring information is only made available to, or shared with, authorized individuals.



Integrity

Ensuring information is protected against unauthorized modification or destruction.

Availability

Ensuring timely and reliable access to, and use of, information.

CyberAssist

Why is it Important?

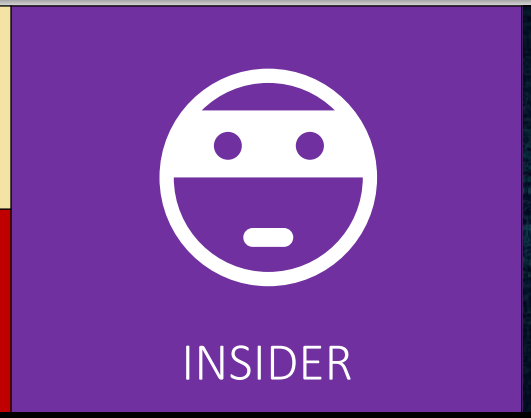
Evolving Threats

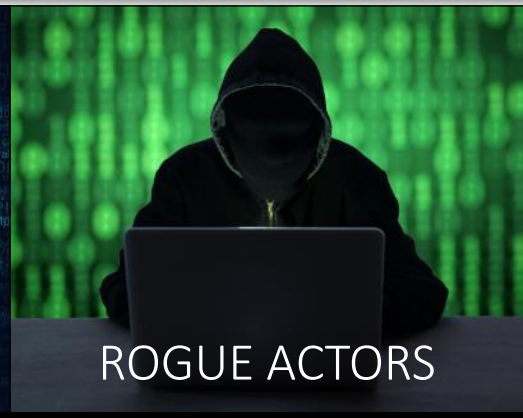
Increasing Potential Impact

Increasingly Unstable Threats

ADVANCED PERSISTENT THREATS (APT)

BROADBASED & CRIMINAL





The Only Constant is Change

Cybersecurity attacks continue to increase in frequency and sophistication for the Aerospace and Defense industry

Are your IT environments protected? Is your information secure?

As a DIB Partner, now is the time to understand your cybersecurity posture so that you can make sound, risk-based decisions about investing in cybersecurity protections.

- Identify and secure information through cybersecurity best practices.
- Understand and identify your risks and the types of cyber threats and vulnerabilities that affect your business.

By understanding the threats and vulnerabilities that affect your business, the business owners can make sound, risk-based decisions about investing in cybersecurity protection.

Module Summary

- Cybersecurity is about keeping our digital data, systems, and activities secure (confidential, available, and unaltered)
- Cybersecurity attacks continue to increase in frequency and sophistication for the Aerospace and Defense industry and supply chain
- Everyone is at risk when it comes to cyber attacks, but small businesses are more likely targets because of perceived limited resources to protect the business and its infrastructure
- For questions on the content, please send them to Contact Us - DIB SCC CyberAssist.

Next: Module 2 - Cybersecurity Maturity Model Certification (Level 2)