Cyber Security Assessment Training 800-171 and CMMC Readiness

NIST 800 -171 and CMMC (Cybersecurity Maturity Model Certification) affects any manufacturer who works with controlled unclassified information (CUI) from certain government agencies, most notably the Department of Defense (DoD), the General Services Administration (GSA) and NASA.

Mass MEP 's training for members of the DoD's Supply Chain to self asses their compliance with the NIST 800-171 will provide the senior management and staff of a company the tools to self asses their enterprises compliance with all 14 points of NIST 800-171 regulation which will prepare the client for CMMC readiness.

Training teaches the participants how to self-assess the 14 elements of their Compliance

- Access Control (AC)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Incident Response (IR)
- Media Protection (MP)
- Physical Protection (PE)
- Risk Management (RM)
- Situational Awareness (SA)
- System and Information Integrity (SI)
- Asset Management (AM)
- Awareness & Training (AT)
- Identification & Authorization (IA)
- Maintenance (MA)
- Personnel Security (PS)
- Recovery (RE)
- Security Assessment (CA)
- System and Communications Protection (SC)

Participants will learn how to identify gaps in the way they store and transmit Confidential Unclassified Information (CUI). Participants will learn to identify where their sensitive information is and how it is accessed and by who is it accessed. They will also learn how to develop a policy about access protocols including who and how access is granted.

The benefits of this training will be that senior management teams will be regularly able to assess and reassess areas that have improved or need improvement. The financial benefits will be identifying weaknesses before they create situations that could lead to non- compliance or loss of data.

This training will greatly enhance the skills of trainee by virtue of its ability to be generically applied to any business or industry in the DoD Supply Chain that may need compliance with these regulations.

This training will greatly enhance the skills of trainee by virtue of its ability to be generically applied to any business or industry in the DoD Supply Chain that may need compliance with these regulations.

The Training will consist of five sessions of 8 hours each in length or 40 hours total. The sessions will include:

- Access, Awareness, Audit & Accountability
- Configuration, Identification, Authentication,
- Incident Response, Maintenance, Protection, Personnel Security
- Physical Protection, Risk Assessment, Security Assessment
- Communication Protection System & Integration Integrity

The Training will be taught by NIST Certified training specialists with Strong Facilitation Skills

What is the Cyber Security Assessment Training?

NIST 800-171 is a framework that specifies how your information systems and policies need to be setup in order to protect Controlled Unclassified Information (CUI). This Assessment Training will provide the orientation necessary for a company's internal staff to determine gaps in their information system security that put their Confidential Unclassified Information (CUI's) information at risk. The CMMC is a certification audit that will be performed by a registered auditing firm as decided by the DoD. Note: the audit process is not included as part of this proposal.

Why do you need the Cyber Security Assessment Training?

If a company has contracts with the United States Department of Defense (DoD) or is a subcontractor to a prime contractor with DoD contracts, your organization must be compliant with NIST SP 800-171. This is a requirement that is stipulated in the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.

DFARS focus on two things: safeguarding Covered Defense Information (CDI), and reporting cyber incidents.

About Our Process

Mass MEP will train participants on each of the fourteen NIST 800-171 elements, teach participants how to identify gaps and how to develop an implementation plan to help bring them into compliance, preparing them for the necessary CMMC audit process.