Defense Cybersecurity Assurance Program Seminar Agenda

0830 Registration/Check-in Continental Breakfast available

Pre-registered attendees can sign-in, network with other attendees/cyber resource providers and enjoy a light breakfast.
If space is available, walk-up attendees will be accommodated.

0900 Sponsor Welcome Main classroom

Purdue MEP, PTAC and the site sponsor will welcome the attendees and stress the importance of raising the cyber-health of the DoD supply chain. Conduct resource provider introductions.

0915 Agenda Review Main classroom

Purdue MEP will review the seminar agenda.

- ***Attendees should attend Track 1** to learn about the DoD cyber contracting regulations, get an overview of the NIST cybersecurity controls, learn about free self-assessment tools/resources and get an introduction to cyber providers who can help them.*
- ***Attendees should attend Track 2 if** they have started a System Security Plan (SSP), developed a Plan of Action and Milestones (POA&M) to close gaps to NIST SP 800-171 and they have an Incident Response Plan (IRP). The leader of this group will answer detailed questions regarding NIST 800-171 controls and describe how those controls can be met at your business.*

At this point the groups split, Track 1 attendees remain in the main classroom and Track 2 attendees go to the break-out room.

Track 1

0930 Safeguarding Covered Defense Information and Cyber Incident Reporting (DFARs 252.204-7012)

*The Defense Federal Acquisition Regulation Supplement, or **DFARS**, has been working to encourage DoD contractors to proactively comply with certain frameworks in order to achieve this goal. Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is the latest mandatory addition. Review DFARs 252.204-7012.*

1000 Protecting Controlled Unclassified Information on Nonfederal Systems and Organizations (NIST SP 800-171 rev 1)

Provide an overview of NIST 800-171. The protection of Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its assigned missions and business operations.

1100 Cyber self-assessment resources overview

For businesses that have the time and IT expertise, there are free tools and cyber self-assessment guides that can be referenced. This session will provide an overview of some of these resources. e.g. NIST SP 800-171A, NIST Handbook 162

1130 Workforce training resources Guest presenter

Different size organizations cope with different cybersecurity problems, but all have employees who are the weak link in their IT security. The challenges of creating and running an awareness program, as well as the cost, vary depending on the number of employees. This session will introduce the attendees to low-cost effective solutions for small business.

1200 Working lunch Cyber workforce focus groups

Grab your lunch!

These focus groups will work toward understanding what the cyber workforce needs are, what is driving those needs, and what the industry perceives as possible solutions to address these needs. We want to hear the perspective of cyber resource providers and small-to-medium businesses.

1pm Cyber Assessment Process TCC

Purdue MEP and TCC Solutions have developed a process to evaluate the current cyber-health of a company compared to the NIST 800-171 standard. This session will review that process, the notional timeline and the deliverables.

1:30pm Cloud Storage/Processing Lifeline Data Centers

This session will discuss the potential advantages to your business of moving a portion of your IT infrastructure to the cloud.

2pm Multifactor Authentication Guest presenter

MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint).

2:30pm Risk Management Mike Yoder, Gallagher

The activity of identifying what information requires what level of protection, and then implementing and monitoring that protection, is called "risk management." This session will review simple steps for creating a risk-based information security program to help you manage risk.

Track 1 and Track 2 combined

3pm Audits/Future DoD Cyber Reqs Mako

Starting in September 2020, every DoD contractor will need a Cybersecurity Maturity Model Certification (CMMC) to bid on any DoD proposal/work on any DoD contract. This session will review cybersecurity audits in general, and discuss the CMMC implementation.

3:30pm Wrap-up

Address any last questions.

A short review of the day and recommended next steps.

Track 2

In parallel with Track 1, the Track 2 attendees will cover specific NIST SP 800-171 rev 1 (Protecting Controlled Unclassified Information on Nonfederal Systems and Organizations) cybersecurity controls in detail. You should bring your SSP, POA&M, IRP, IT infrastructure diagrams, etc. to this session. You will have the ability to engage the seminar leader in detail about your specific network.

Seminar #1 (November 2019, Bloomington) will cover:

(Although the cybersecurity control families to be reviewed at each seminar are programmed below, the seminar leader has the flexibility to modify the information that is reviewed so that it matches the interest/needs of the attendees. The Track 2 goal that we are trying to achieve is a detailed, systematic review of NIST SP 800-171 over the course of one year.)

3.1 Access Control

Access is the ability to make use of any system resource. Access control is the process of granting or denying requests to:

- *use information,*
- *use information processing services, and*
- *enter company facilities.*

Examples of access control security requirements include account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination.

3.3 Audit/Accountability

Companies should create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity and ensure that the actions of users can be uniquely traced to those users so they can be held accountable.

Seminar #2 (April 2020, Indianapolis) will cover:

3.4 Configuration Management

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC). Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a change control board. It allows the entire system to be reviewed to help ensure that a change made on one system does not have adverse effects on another system.

3.5 Identification and Authentication

For most systems, identification and authentication is often the first line of defense. Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system. Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system.

3.6 Incident Response

Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be lessened by having standard operating procedures that can be followed in the event of an incident. Examples of incident response requirements include: incident response training, incident response testing, incident handling, incident monitoring, and incident reporting. Companies should establish an operational incident handling capability for company systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and track, document, and report incidents to company management and/or authorities.

Seminar #3 (May 2020, South Bend, Elkhart or Fort Wayne) will cover:

3.8 Media Protection

Media protection is a requirement that addresses the defense of system media, which can be described as both digital and non-digital. Examples of digital media include: diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Examples of non-digital media include paper or microfilm. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed.

3.9 Personnel Security

Users play a vital role in protecting a system as many important issues in information security involve users, designers, implementers, and managers. How these individuals interact with the system and the level of access they need to do their jobs can also impact the system's security posture. Almost no system can be secured without properly addressing these aspects of personnel security. Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources.

3.10 Physical Protection

Examples of physical and environmental requirements include: physical access authorizations, physical access control, monitoring physical access, emergency shutoff, emergency power, emergency lighting, alternate work site, information leakage, and asset monitoring and tracking. Companies should limit physical access to systems, equipment, and the respective operating environments to authorized individuals, protect the physical plant and support infrastructure for systems, provide supporting utilities for systems, protect systems against environmental hazards, and provide appropriate environmental controls in facilities containing systems.