Defense Supply Chain Cyber Resilience Labs

Schedule

This 5-week, 25-hour course is taught via Zoom on Wednesdays & Fridays from 8:00 am to 10:30 am PST. Begins March 10th and goes to April 9th.

Instructors

Dr. Tony Lopez (INDUS Technology) and Ms. Larisa Breton (FullCircle Communications)

Overview

This course aims to help each participant to learn the fundamentals of creating a DFARS 7012 and NIST 800-171 compliant System Security Plan (with related Plan of Action and Milestones) that will help them understand and better prepare for Cyber Maturity Model Certification (CMMC) requirements. It is important to note that Systems Security Plans (SSP) and related Plans of Action and Milestones (POA&M) are very detailed documents which require the development of policies, physical actions to secure systems, and careful planning. Participants will learn all about this in this course. However, participants should keep in mind that they should not expect to have a plan completed in 5 weeks of instruction, if one does not already exist. Participants are welcome to work on a plan-in-progress, if their company has begun the process.

The course has been designed to engage participants in hands-on activities, providing them with working time and one-on-one instructor guidance to successfully complete each core segment of the program. Participants are encouraged to assemble their course outputs into the initial forming elements of an SSP for their organization, with any identified remedial issues to be included in their POA&M. The instructors encourage participants to share their SSPs and provide comments and guidance on their progress. In addition, participants are provided with all of the critical references, resources and guidance to assist them in developing a well-formatted SSP and POA&M in MS Word for their own corporate use, as well as additional reporting artifacts (for example, such as the DHS CERT reporting tool), all course materials for their future use and reference, and a signed Certificate of Completion.

Learning Objectives

- Introduce participants to DoD Cyber Security Requirements and Policies, specifically NIST 800-171 and variants, and the Cyber Maturity Model Certification (CMMC).
- Introduce participants to essential controls for protecting their organization's networks and systems, and to map which potential CMMC level they can achieve.
- Introduce participants to important concepts for Cyber Security such as Risk Management, Configuration Management, Incident Response and Insider Threat.
- Provide resources, reference materials and tools to assist participants to develop a Systems Security Plan and Plan of Action and Milestones for their Organizations.

About the Instructors

Dr. Tony Lopez: Dr. Lopez is a Vice President and Chief Information Security Officer at INDUS Technology, Inc. and is responsible for the development and implementation of both INDUS' NIST 800-171and INDUS' Internal Threat Program, so he has firsthand knowledge of the NIST 800-171, DFARS 7012 and the Cyber Maturity Model Certification requirements and what it takes to meet these requirements. Having been an adjunct faculty to various universities in San Diego, Dr. Lopez is very experienced working with participants with a very wide ranges of knowledge in IT and Cyber, and teaching/learning group facilitation. Dr. Lopez has over 25 years working in the Defense Industry and for Federal Agencies, 16 of these as Director of Information Systems INDUS Technology and today Vice President of Operations and CISO. Other recent experience includes Director of Instructional Systems and Technology at the Navy Center for Information Technology and Program Manager of NASA's SOLAR e-Learning Program. Dr. Lopez's education includes a bachelor's degree from Cal State San Luis Obispo in Mechanical Engineering, a Master's Degree in Business Administration from University of Phoenix and a Ph.D. from Cal Southern University in Business Administration with concentration in Computer Science.

Ms. Larisa Breton: Ms. Breton is President of FullCircle Communications. Her company provides cybersecurity and engineering support services to the DoD, City of Los Angeles, City of San Francisco, and other entities. Ms. Breton earned her Masters' degree in Safety and Security Leadership from The George Washington University and has been a leading small-business SME on the DFARS 7012 regulations, publishing in CTO Vision, and providing policy advisory directly to DoD as well as to the IEEE at their Quality, Reliability and Security international conference. She has trained Procurement Technical Assistance Center counsellors and also has trained San Diego small businesses on how to meet DFARS 7012 requirements. Ms. Breton sits on the NIST NICE Workforce Management and K-12 Committees and participates in the DoD/DHS/MITRE Software Supply Chain Risk Management working group and other security forums. Ms. Breton has an extensive history with digital engagement including performing digital media and portfolio management for General Motors Cyberworks. She is Adjunct Faculty at the University of Alaska Southeast, teaching industrial control system cybersecurity, where she holds a Digital Faculty Fellowship.

Target Audience

The course is intended for all contractors and subcontractors working in the DoD supply chain.

Course Content (25-hour course)

Module 1 / NIST 800-171 and Systems Security Plan

- Introduction to NIST 800-171 and Its Variants.
- Fundamentals of Developing a Systems Security Plan, Plan of Action & Milestones, and Applying NIST - 18r1.

Module 2 / Assessing Operations and DoD Assessment Methodology

- Assessing Operations NIST 800-171A
- DoD Assessment Methodology

Module 3 / DoD Policies, CDI and CUI

- DoD Policies Reasons for increasing Cyber Security
- DFARS 252.204-7012/7010 and Working Knowledge of CDI and CUI

Module 4 / Best Practices and Configuration Management

- Industry Best Practices for Cyber Security Policies
- Configuration Management

Module 5 / Network Architecture and Risk Management Framework

- Understanding Network Architectures
- Introduction to the Risk Management Framework

Module 6 / Monitoring Tools and Fundamentals of Risk Management

- Network Surveillance/Monitoring Tools Shodan/WireShark Framework
- Fundamentals of Risk Management

Module 7 / Cloud Computing and Persistent Threat

- Importance of Cloud Computing
- Advanced Persistent Threat and The Importance of NIST 800-172

Module 8 / Hiring Professionals and FIPS 199

- Hiring Cyber Security Professionals and Management Service Providers (MSPs)
- FIPS 199 Categorizing Information Systems

Module 9 / Reporting and Developing Incident Response Plan

- Reporting Incidents
- Developing and Incident Response Policy and Plan

Module 10 / CMMC and Insider Threat

- Cyber Maturity Model Certification (CMMC) and the CMMC Accreditation Body.
- Fundamentals of Insider Threat

Link to course:

https://elcamino.coursestorm.com/category/defense-supply-chain-cyber-resilience-labs