Cyber Resilience Course

This 5-week online, 25 hour course is taught via Zoom, 6 – 8:30 pm, October 3 – November 4. Students will gain an understanding of important DOD cybersecurity requirements that will help keep their organization in good standing as a contractor with the federal government.

All course material is included in the registration fee. Students will have access to the electronic files through a cloud-based secure file sharing program.

COURSE OBJECTIVES

- Familiarize students to the DoD Cyber Security Requirement and Policies, specifically NIST 800-171 and variants, and the Cyber Maturity Model Certification (CMMC).
- Present students the essential controls for protecting their organization's networks and systems while mapping which potential CMMC level they can achieve.
- Provide students the important concepts such as Risk Management, Configuration Management, Incident Response and Insider Threats.
- Provide students the resources, reference materials and tools to develop a Systems Security Plan and Plan of Action and Milestones for their organizations.

COURSE AGENDA

Week 1/Module 1

- NIST 800-171 and Its Variants and Other Tools and Resources
- Fundamentals of Developing a System Security Plan, Plan of Action and Milestones (POA&M), and Applying NIST 18r1 (POA&M)

Week 1/Module 2

- Assessing Security Requirements for Controlled Unclassified Information (NIST 800-171A)
- The DoD Assessment Methodology

Week 2/Module 3

- DoD Security Policies and the reasons for increasing Cyber Security
- DFARS 7010, 7012, 7019, 7020 and 7021, and Working Knowledge of CDI, CUI, and FCI

Week 2/Module 4

- Cyber Security Policies and Best Practices
- Configuration Management

Week 3/Module 5

- Understanding Network Architectures
- Introduction to the Risk Management Framework

Week 3/Module 6

- Network Surveillance and Monitoring Tools
- WireShark and The OSI Layer

Week 4/Module 7

- Cloud Computing Best Practices
- Understanding Advanced Persistent Threat (APT)

Week 4/Module 8

- Critical evaluation criteria for hiring cybersecurity professionals and Managed Service Providers (MSPs) to monitor and interact with their networks.
- Understanding the fundamentals of Ransomware Attacks.

Week 5/Module 9

- Incident Reporting
- Developing and Incident Response Policy and Plan

Week 5/Module 10

- Cyber Maturity Model Certifications (CMMC 1.02, June 2020) and CMMC Accreditation Board
- Understanding Insider Threat

ABOUT THE INSTRUCTORS

TONY LOPEZ

Dr. Tony Lopez is the VP of Business of Operations and CISO at INDUS Technology, Inc. in San Diego, California, where he leads all IT/IS related activities and business operation for the company. Dr. Lopez has led the INDUS' program to meet NIST 800-171 requirements and was asked by the San Diego Chapter of NDIA Small Business Committee to lead a Task Force to study the impact NIST 800-171 on small businesses within the Defense Industrial Base. The Task Force, in cooperation with NDIA National has recently launched a national survey to gather data to help the Task Force better understand the impacts of NIST 800-171. Dr. Lopez also over sees business development activities at INDUS and information security matters. Other recent experience includes Director of Instructional Systems and Technology at the Navy Center for Information Technology, under contract to ANTIN Engineering, and Program Manager of NASA's SOLAR E-Learning Program under contract to High Technology Solutions, Inc.

Dr. Lopez has also been an adjunct Faculty over 16 years, teaching at the University of Phoenix San Diego Campus in the Information Systems and Technology Department. He has also taught at Business and IT related courses at California State University at San Marcos, Southwestern College Chula Vista, and Central Texas College, Navy Campus. Dr. Lopez' educational background includes a Bachelor's degree in Mechanical Engineering and Technology from California State University San Luis Obispo, an MBA from University of Phoenix, San Diego, and a PhD in Business Administration, with concentration in Computer Science, from California Southern University, Irvine.

LARISA BRETON

Larisa Breton is President of FullCircle Communications. Her company provides cyber security 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 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 an Adjunct Faculty at the University of Alaska Southeast where she holds a Digital Faculty Fellowship.