CYBERSECURITY EDUCATORS:

EXPLORING THE CYBERSECURITY MATURITY MODEL CERTIFICATION

NCyTE CENTER

OCTOBER 28 -29, 2020 - 8:00am - 3:30pm (Pacific)
REGISTER NOW AT
www.ncyte.net/cmmc-workshop

WHAT IS CMMC? WHAT CYBERSECURITY EDUCATORS NEED TO KNOW:

Significant compromises of sensitive U.S. defense information on vendor computer networks have prompted new rules and requirements. Soon over 300,000 new and existing DoD contractors seeking new contracts with the Department of Defense (DoD) must meet requirements announced January 1, 2020. The model is design to protect our nationals DoD supply chain from cyber criminals and state sponsored attacks. This requirement, the Cybersecurity Maturity Model Certification (CMMC), is a unified standard for implementing cybersecurity across the companies included in the defense industrial base (DIB).

Contractors continue to be responsible for implementing critical cybersecurity requirements, but the CMMC also requires third-party assessments. Community Colleges across the nation can assist these contractors prepare for these sweeping changes.

ATTEND THE NCYTE CENTER 2-DAY CMMC WORKSHOP

NCyTE Center will present a 2-day virtual workshop on CMMC requirements for college faculty and small business IT personnel. This Cybersecurity Maturity Model Certification (CMMC) workshop will provides an overview of how to prepare for future certification, including its requirements, impact and importance for contractors working with the Department of Defense. Funded by a grant from the National Science Foundation, the course is free but limited to 20 attendees.

John Sands, PI and Director of the Center for Systems Security and Information Assurance (CSSIA) and professor at Moraine Valley Community College in Chicago will present the course. An Instructor Guidebook, Student Guidebook, training resources, and a Canvas course package will be available to attendees.

WHO SHOULD ATTEND?

- Full-time cybersecurity faculty at community colleges, technical colleges, and universities seeking to better prepare students for the workforce with CMMC certification.
- Small business IT and cybersecurity personnel at DIB businesses pursuing CMMC certification to compete for DoD contracts. (Acceptance on a space-available basis.)

The National Cybersecurity Training & Education Center (NCyTE) is a consortium of colleges, universities, high schools, and industry partners working together to grow and strengthen our nation's cybersecurity workforce. Currently funded as a national resource center by a National Science Foundation Advanced Technological Education (NSF-ATE) grant, NCyTE is administered by Whatcom Community College in Bellingham, WA. Visit www.ncyte.net.

FOR MORE INFORMATION, CONTACT TBol@whatcom.edu

WHO MUST COMPLY?

- Contractors, Suppliers, Small Businesses, Vendors: CMMC certification will eventually be required of all DOD contractors including suppliers at all tiers of the supply chain.

- Third-Party Assessors: The CMMC Accreditation Body (CMMC-AB) developed procedures to certify third party assessment organizations (CP3AO) to evaluate companies' CMMC levels.

MATURITY LEVELS ADDRESSED AS PART OF NCYTE WORKSHOP:

The Office of the Under Secretary of Defense combined several cybersecurity standards and best practices and mapped these controls and processes across several maturity levels. Each level will progressively mandate higher technical requirements and assessment—Level 1 through Level 5. Each Maturity Level will be covered in this workshop.

LEVEL 1:

A company must perform "basic cyber hygiene" practices, such as using antivirus software or ensuring employees change passwords regularly to protect Federal Contract Information (FCI). FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government." It does not include public information or certain transactional information.

LEVEL 2:

A company must document certain "intermediate cyber hygiene" practices to begin to protect any Controlled Unclassified Information (CUI) through implementation of some of the US Department of Commerce National Institute of Standards and Technology's (NIST's) Special Publication 800-171 Revision 2 (NIST 800-171 r2) security requirements. CUI is "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls," but does not include certain classified information.

LEVEL 3:

A company must have an institutionalized management plan to implement "good cyber hygiene" practices to safeguard CUI, including all the NIST 800-171 r2 security requirements as well as additional standards.

LEVEL 4:

A company must have implemented processes for reviewing and measuring the effectiveness of practices as well as established additional enhanced practices detect and respond to changing tactics, techniques and procedures of advanced persistent threats (APTs). An APT is defined as an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors.

LEVEL 5:

A company must have standardized and optimized processes in place across the organization and additional enhanced practices that provide more sophisticated capabilities to detect and respond to APTs.