NISTCSF.COM

NIST Cybersecurity Framework
Workforce Development & Certification Program

Rick Lemieux
itSM Solutions LLC
31 South Talbert Blvd. #295
Lexington, NC 27292
USA
401-764-0720
Fax – 401 764-0747

NISTCSF.COM – NIST Cybersecurity Workforce Training Solutions

Introduction

In May of 2017, President Trump issued an Executive Order for "STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE," which hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

Two key provisions of the executive order include:

- Effective immediately, each agency head shall use ***The Framework for Improving Critical Infrastructure Cybersecurity*** **(the Framework) developed by the National Institute of Standards and Technology**, or any successor document, to manage the agency's cybersecurity risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) within 90 days of the date of this order.
- Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

The itSM Solutions UMass Lowell **NISTCSF.COM workforce development program** is designed to help federal agencies and private industry learn the knowledge, skills and abilities to operationalize the NIST Cybersecurity Framework across an enterprise and its supply chain.

All NISTCSF.COM trainings are aligned with the recently released NICE Cybersecurity Workforce Framework (NCWF). The NCWF framework, led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. It's recently released special publication 800-181 - the NIST/NICE Cybersecurity Workforce Framework (NCWF) serves as a building block for the development of cybersecurity training standards and individual career planning.

It is NISTCSF.COM intent to stand up NIST Cybersecurity Workforce Development and Continuous Monitoring centers across the country in partnership with government, academia and private industry to meet the cybersecurity workforce development needs outlined in President Trumps executive order.

NISTCSF.COM

NISTCSF.COM is a NIST Cybersecurity Framework (NCSF) workforce development solution brought to you by itSM Solutions LLC and UMass Lowell a NSA/DHS National Center of Academic Excellence in Cyber Defense Research (CAE-R).

The program is built around a controls factory model created by the university's chief information security officer that teaches organizations how to design, build, test, maintain and continually improve a cybersecurity program based on the NIST Cybersecurity Framework (NCSF).

The UMass Lowell program and its author have won the following industry awards:

• Security Magazine's Most Influential People in Security, 2016
• SANS People Who Made a Difference in Cybersecurity Award, 2013
• Information Security Executive (ISE) nominee for Executive of the Year for North America, 2013
• ISE North America Project Award Winner I for the Academic and Public Sector Category, 2013

NCWF Training Program Overview

The NISTCSF.COM program is built around a four phase training model.

Phase 1 of the NCSF workforce development program teaches organizations the knowledge, skills and abilities (KSA) to design, build, test, manage and continually improve a NIST Cybersecurity Framework program based on the UMass Lowell NCSF Controls Factory Model™

The program is based on a cybersecurity "controls factory" methodology created by Larry Wilson the CISO in the UMASS President's office. The program consists of certification training and hands-on lab where students learn the practical skills they will need to become productive cybersecurity professionals upon graduation.

The controls factory methodology is designed to teach cybersecurity organizations how to organize the engineering, technical and business functions of a NIST cyber security program. The program is completely adaptable which means that each of the modules can easily be updated, replaced or modified with minimal impact on the overall solution. Organizations are free to choose the minimum set of controls its need to improve its framework profile and then over time incrementally adopt other controls that will take it to its identified target state. The factory approach allows for changes in the cybersecurity threat landscape, new vulnerabilities and the addition of incremental improvements while still keeping a focus on the critical assets and identities. Programs include:

NCSF Foundation Certification Training

The Foundations Course outlines current security challenges and explains how organizations who implement a NIST Cybersecurity Program can mitigate these risks. This program prepares students to function successfully in NICE entry level work role positions.

Location of Training: Onsite or Online
Means of Instruction: Classroom, Virtual Classroom, Self Paced Video
Number of Hours: 16 (2 Day)
Credentials or Certificate Attained: Certification, PDU's, CEU's, College Credits

NCSF Practitioner Certification Training

The Practitioners Course explains in detail current security challenges, and how organizations design, build, test, manage and improve a Cybersecurity Risk Management Program based on the NIST Cybersecurity Framework. This program prepares students to function successfully in NICE entry, mid and advanced level work role positions plus acquire the knowledge and skills to

advance to the specialty roles (ethical hacker, vulnerability assessment manager etc.) outlined in the NICE framework.

Location of Training: Onsite or Online
Means of Instruction: Classroom, Virtual Classroom or Self Paced Video
Number of Hours: 30 (4 days)
Credentials or Certificate Attained: Certification, PDU's, CEU's, College Credits

Phase 2 of the NCSF workforce development program includes cybersecurity project and security operations center (SOC) programs that will teach NCSF Practitioners the hands on skills they need to work in a NCSF program.

NCSF Engineering Workshop and Lab
This "lecture-based" workshop will be supplemented with "hands on" project based labs designed to teach candidates how to perform assessments and create project plans based on the NIST Cybersecurity Framework.

Location of Training: Onsite or Online
Means of Instruction: Instructor Led Classroom or Virtual Classroom, Self Paced Video
Number of Hours: To Be Determined
Credentials or Certificate Attained: Digital Badge, PDU's CEU's, College Credits

NCSF Technology Workshop and Lab
This "lecture-based" workshop will be supplemented with a "hands-on" project based labs that will teach candidates how to select, configure and utilize the technologies associated with a NIST Cybersecurity Framework Security Operations Center (SOC)
Location of Training: Onsite or Online
Means of Instruction: Instructor Led Classroom or Virtual Classroom, Self Paced Video
Number of Hours: To Be Determined
Credentials or Certificate Attained: Digital Badge, PDU's CEU's, College Credits
Course Description & Outline: Coming Soon

NCSF Business Workshop and Lab
This "lecture-based workshop will be supplemented with "hands-on" project based labs that will teach candidates how to adopt ISO 27002 or NIST 800-171 standards in a NIST Cybersecurity program.

Location of Training: Onsite or Online
Means of Instruction: Instructor Led Classroom or Virtual Classroom, Self Paced Video
Number of Hours: To Be Determined
Credentials or Certificate Attained: Digital Badge, PDU's CEU's, College Credits

Phase three of the NCSF workforce development program prepares candidates to sit for the work role and specialty certifications outlined in the NIST 800-161 the NICE Cybersecurity Workforce Framework.

NICE Work Role or Specialty Certification Training Library

itSM's certification training portal prepares candidates to sit for up to 192 NCWF IT, Cybersecurity and Business Skill professional certifications.

Location of Training: Online
Means of Instruction: Self Paced Video
Number of Hours: Varies based on Program Selected
Credentials or Certificate Attained: Certification, PDU's, CEU, College Credits

Phase four of the NCSF workforce development program teaches employees the knowledge, skills and abilities (KSA) to practice good cyber behavior when working online.

Employee Cybersecurity Awareness Training

RESILIA™ Employee Awareness Training Programs cover topics in phishing, social engineering, online safety, social media, BYOD (Bring Your Own Device), removable media, password safety, personal information, information handling and remote and mobile working. Programs are delivered as online games, simulations and animations. Student assessment testing and reporting tools are available with this program.

Location of Training: Online
Means of Instruction: Games, Animations and Simulations
Number of Hours: Varies based on Program Selected
Credentials or Certificate Attained: Certificate of Completion