NISTCSF.COM

NIST/NICE Cybersecurity Workforce Framework
Training & Certification Programs

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

Introduction

In February 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which called on the Department of Commerce's National Institute of Standards and Technology (NIST) to develop a voluntary risk-based Cybersecurity Framework for the nation's critical infrastructure—that is, a set of industry standards and best practices to help organizations identify, assess, and manage cybersecurity risks. These 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. NIST issued the resulting Framework in February 2014. The framework has now been adopted by commercial enterprises and 28 other countries across the world as its cybersecurity standard.

Our training initiative is tied too Imperative #4 of the recently released Presidential Cybersecurity commission report to build cybersecurity workforce capabilities across the nation's critical infrastructure sectors.

Currently, the cybersecurity sector is understaffed despite high demand, and the Commission predicts that the economy will need 100,000 new cyber-sector employees by 2020. To meet that demand, the Commission is advocating Federal, State and Local grants, apprenticeship programs, rotational programs, early education, and support for college students and businesses investing in this field. They are also promoting the use of H1B monies companies pay to bring in help from overseas to fund this program as well.

All trainings will be aligned to the recently released NICE Cybersecurity Workforce Framework (NCWF). The National Initiative for Cybersecurity Education (NICE), 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) in addition to helping organizations educate, recruit, train and retain a qualified cybersecurity workforce, the NCWF will serve as a building block for the development of cybersecurity training standards and career planning.

In January of 2017, Federal agencies will soon be using the NCWF to identify and qualify their cybersecurity workforce and integrators (physical and cybersecurity) as called for by the Federal Cybersecurity Workforce Assessment in the Cybersecurity Act of 2015.

NISTCSF.COM

NISTCSF.COM is a NIST/NICE cybersecurity workforce development solution brought to you by itSM Solutions LLC and Larry Wilson the CISO in the UMASS President's office.

The NISTCSF.COM program is centered around a Controls Factory Methodology (CFM) created by an award winning CISO on how to Design, Build, Test and Manage a cybersecurity program based on the NIST Cybersecurity framework. The CFM approach has already been adopted by many universities across New England.

Funding sources for these programs will include Workforce Development, GI Bill, Apprenticeship, Internship, Human Resource and other funding programs set up for the unemployed, underemployed, retired veterans and employed workers for continuing education purposes.

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

– SANS Person who made a difference in Cybersecurity, 2013
– ISE (Information Security Executives) Finalist for Executive of the Year for North America, 2013
– ISE Information Security Program of the Year for Higher Education & Government Category, 2013
– Security Magazine most influential cyber security professionals in North America, 2016

Training content for this program can be licensed as print or digital book for instructor led classroom or virtual classroom delivery or as ⬚video's for an online self-paced training solution. All programs come with a university certificate of completion plus continuing education (PDU, CEU's etc.) and college credits.

The NISTCSF.COM program is built around a three tier training model.

NCSF Certification Training Programs

These programs will teach candidates how to design, build, test and manage a cybersecurity program based on the NIST Cybersecurity Framework (NCSF) and Larry's " NCSF Controls Factory Methodology"

The **NCSF 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: Instructor Led Classroom or Virtual Classroom, Self Paced Video
Number of Hours: 8 (1 Day)
Credentials or Certificate Attained: Certificate of Completion, PDU's, CEU's, College Credits
Course Description & Outline: Can be found here

The **NCSF Practitioners Course** explains in detail current security challenges, and how organizations design, build, test and manage a comprehensive Cybersecurity and 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: Instructor Led Classroom or Virtual Classroom, Self Paced Video

Number of Hours: 24 (3 days)
Credentials or Certificate Attained: Certificate of Completion, PDU's, CEU's, College Credits
Course Description & Outline: Can be found here
NIST/NICE Work & Specialty Role Certification Training Programs

These programs will teach candidates the knowledge they need to prepare for the IT and cybersecurity certifications outlined in NIST 800-181 the NICE Cybersecurity Workforce Framework (NCWF) and DoD 8140 Cyberspace Workforce Management Policy directive.

NIST Specification 800-181 provides guidance about the work and specialty roles associated with a cybersecurity program along with describing the knowledge, skills, abilities required for each role.

Terminology from the NCWF has already been incorporated into two new online resources for the cybersecurity field: the CyberSeek jobs map graphically displays the nation's cybersecurity job demand and availability; and the Career Pathway, which can help students or job seekers new to the field develop cybersecurity career plans.

itSM's careeracademy.com certification training portal enables students be trained to sit for up to 25 NCWF work and specialty area professional certifications in Cybersecurity from CompTIA, ISACA, ISC², Mile2 and others.

Location of Training: Online
Means of Instruction: Self Paced Video
Number of Hours: Varies based on Program Selected
Credentials or Certificate Attained: Certificate of Completion, PDU's, CEU, College Credits
Course Description & Outline: Can be found here
Credentials or Certificate Attained: Certificate of Completion
Course Description & Outline: Can be found here

NCSF Lab Programs (Coming Soon)

These programs will deliver an online cybersecurity lab where candidates can apply in a real world environment the knowledge, skills and abilities they learned in the classroom or online classroom.

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: Certificate of Completion, PDU's CEU's, College Credits
Course Description & Outline: Coming Soon