



# **NISTCSF.COM**

## **NIST 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

## NISTCSF.COM – NIST/NICE Cybersecurity Workforce Training Solutions

### 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 individual career planning.

**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.

It is our intent to stand up a series of NIST Cybersecurity Workforce Framework education centers across the nation (and eventually the globe) in partnership with other universities, tech schools, high schools, associations, integrators, governments and enterprise institutions.

## NISTCSF.COM

**NISTCSF.COM** is a NIST/NICE Cybersecurity Workforce Framework (NCWF) training program brought to you by itSM Solutions LLC and Larry Wilson the CISO in the UMASS President's office.

Training content is available as print, digital book which can be delivered in a classroom or v-classroom by a qualified instructor or as a turnkey self-paced video training solution. All programs come with a certificate of completion plus continuing education (PDU, CPE's etc.) and college credits.

The program and its author have won the following 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

It is our goal to partner with universities, tech schools, high schools, trade associations, integrators, governments and enterprise to bring this cybersecurity training solution to the global market.

## NCWF Training Program Overview

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

**The first tier teaches organizations the knowledge, skills and abilities (KSA) to design, build, test and manage a Cybersecurity program based on [Executive Order 13636 the NIST Cybersecurity Framework \(NCSF\)](#).** 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:** 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](#)

### **NCSF Practitioner Certification Training**

The 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](#)

***Phase 2 of the program based on [Executive Order 13636 the NIST Cybersecurity Framework \(NCSF\)](#) will include four workshops and labs that will provide practitioners the practical experience they will need to become productive cybersecurity employee's upon graduation. Programs include:***

### **NCSF Practitioner Engineering Workshop and Lab**

This workshop will include the design requirements and build specifications based on the 22 Framework Categories and 5 Core Functions of the NIST Cybersecurity Framework. The "Lecture-based" Workshop will be supplemented with a "Hands-on" workshop in partnership with vendors providing solutions for the operationalizing of the NIST CSF across an enterprise and its supply chain.

**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

### **NCSF Practitioner Technology Workshop and Lab**

This workshop will include the design requirements and build specifications based on the 20 Critical Security Controls. The “Lecture-based” Workshop will be supplemented with a “Hands-on” lab in partnership with vendors providing solutions for the management and monitoring of the 20 critical controls.

**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

### **NCSF Practitioner Business Security Workshop and Lab**

This workshop will be based on the ISO 27002 or NIST 800-171 standards. This workshop includes the design requirements and build specifications based on either ISO 27002 or NIST 800-171. The lecture based workshop will be supplemented by a hands on lab developed for this lecture – since this program is more about business controls and not technical controls the hands-on component is more or less practice exercises and case studies.

**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

### **NCSF Practitioner Business Risk Workshop and Lab**

This workshop will be based on the Baldrige Excellence Framework and the FAIR Institute Cyber Risk methodology. This program will also include lab exercises.

**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

The second tier teaches organizations the knowledge, skills and abilities (KSA) to prepare for the work role and specialty certifications outlined in the [NIST 800-161 the NICE Cybersecurity Workforce Framework](#). Programs include:

#### **NICE Work Role or Specialty Certification Training Library**

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, ISC<sup>2</sup>, 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](#)

The third tier teaches employees the knowledge, skills and abilities (KSA) to practice good cyber behavior when working online. Programs include:

#### **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

**Course Description & Outline:** Can be found [here](#)