NISTCSF.COM

NIST Cybersecurity Framework Training Solutions

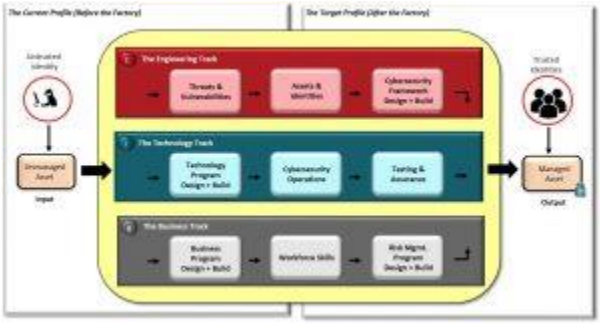
NISTCSF.COM

In May of 2017, President Trump issued Executive Order 13800 for "Strengthening The Cybersecurity of Federal Networks and Critical Infrastructure". Call to Actions included:

- Effective immediately, each agency head shall use The NIST Cybersecurity Framework to manage the agency's cybersecurity risk.
- Further, the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields to achieve our objectives in cyberspace.

NISTCSF.COM is a NIST Cybersecurity Framework (NCSF) workforce development program brought to you by UMass Lowell (UML) a NSA/DHS National Center of Academic Excellence in Cyber Defense Research (CAE-R). This innovative cybersecurity workforce development program is built around an NCSF Controls Factory™ model created by Larry Wilson, CISO in the university president's office to engineer, operate and manage the business risk of a NIST Cybersecurity Program. Since its inception, the program has been used to operationalize the NCSF across the university's five campuses plus several other universities and colleges throughout New England. More information about the program can be found here.

The NCSF Control Factory™ model helps enterprises organize the Engineering, Operations and Business Risk functions of an NCSF program. The model 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 cybersecurity risk profile and then over time adopt additional controls that will take it to a higher cybersecurity state. The factory approach allows for changes in the cybersecurity threat landscape, new vulnerabilities and the addition of improvements while still keeping a focus on the critical assets and identities.



The UML 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

The UML NIST Cybersecurity Framework workforce development program is built around a public private partnership where UML is partnering with the government, academia (public and private) and industry to deliver and continuously improve its NCSF content and Security Operations Training Center (SOTC) capabilities and services.

The UML accredited cybersecurity workforce development program is built around a Basic and Advanced NIST Cybersecurity Framework workforce developent model.

NIST Cybersecurity Basic Trainings

These programs teach candidates the fundamentals on how to operationalize the NIST Cybersecurity Framework across an enterprise and its supply chain using the UMass Lowell Controls Factory Model (CFM). The program also prepares candidates to sit for the certifications outlined in the NICE Cybersecurity Workforce Framework

Programs
- NIST Cybersecurity Framework Certification Training Based on the UMass Control Factory Model
- NIST Cybersecurity Industry Sector Certification Trainings (i.e., Healthcare, Energy etc.)
- NIST Cybersecurity Policy & Law Certification Trainings (i.e., 23 NYCRR 500, GDPR etc.)
- NICE Certification Trainings Aligned with the NICE Cybersecurity Workforce Framework
- NIST Cybersecurity Framework Simulation Trainings to Help Students Experience NCSF in Action

Credentials Earned
- Certifications, College Credits, Continuing Education Credits (PDU, CEU etc.)

Delivery Partners
- Private Training and Consulting Companies
- Non Profit Industry Associations
- Colleges & Universities

NIST Cybersecurity Advanced Trainings

These programs teach candidates the advanced hands-on skills required to work in a NIST CSF security operation (SOC) center and program. The training takes place in a fully functioning SOC which is delivering cost effective NCSF assessments, testing, monitoring and research services to business, government & academia

Programs
- NCSF-SOC Engineering Advanced Trainings
- NCSF-SOC Operations Advanced Trainings
- NCSF-SOC Business Risk Advanced Trainings
- NCSF-SOC Assessment Training
- NCSF-SOC Testing & Continuous Monitoring Training

Credentials Earned
- Digital Badges, Certifications, College Credits, Continuing Education Credits (PDU, CEU etc.)

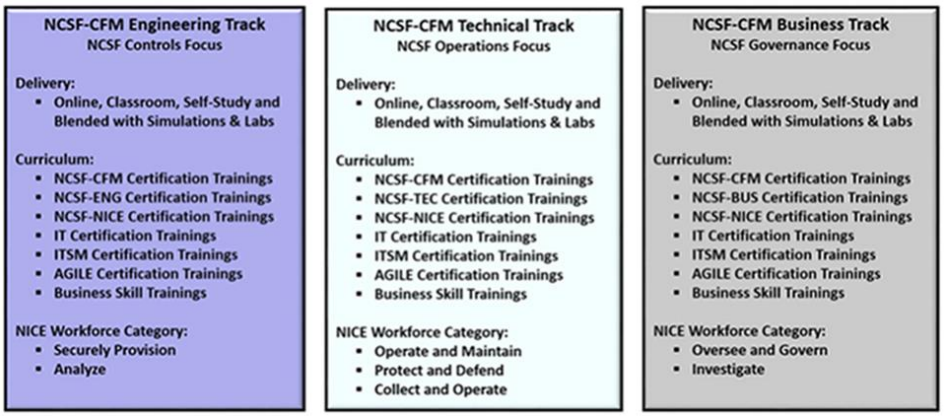
Delivery Partners
- Public Colleges & Universities
- Private Colleges & Universities
- Community Colleges
- Corporate Academies etc.

UML has contracted with itSM Solutions to build out and expand its program as itSM has years of experience in building accredited best practice training content and certification exam services. It is itSM's job to work with UML and other Academic, Government and Industry partners to expand the current program and to establish a continuing education program that will enable a lifelong learning partnership with the cybersecurity workforce. Today, itSM has established partnerships with Acquiros a U.S. based ISO 17024 certification body for accreditation and exam services, New Horizons Computer Learning Centers the world's largest independent IT training company with over 300 locations in 70 countries, PSA Security Networks the largest association of physical security manufacturers and installers in the world and Arvato Training & Education Services a global eCommerce platform and integrated eReader application which delivers interactive eBook and print versions of the UMass courseware anywhere in the world.

Listed below is a summary of the UML NIST Cybersecurity Framework (NCSF) / NICE workforce development program. Links to samples of UML's classroom and video content can be found below.

UML Program Summary

The UML NCSF workforce development program is built around three training tracks that teach individuals and organizations "how to" Engineer, Operate and Manage the Business Risk of a NIST Cybersecurity Framework (NCSF) Program. Each learning track aligns with the workforce categories outlined in the NICE Cybersecurity Workforce Framework. The university's goal is to get a NIST cybersecurity workforce up and running quickly in collaboration with government and industry and then continually improve it over time by leveraging the knowledge, skills and abilities the members of the collaborative bring to the program.



NCSF Certification Training Programs

The NCSF-CFM Foundation Certification Course, which is available via instructor-led sessions or online video, outlines current cybersecurity challenges and explains how organizations that implement an NCSF program can mitigate these challenges. This program is focused on candidates who need a basic understanding of the NCSF to perform their daily jobs as executives, business professionals or information technology professionals.

The NCSF-CFM Practitioner Certification Course, also available via instructor-led sessions or online video, details the current cybersecurity challenges plus teaches in depth the UML NCSF Control Factory

Model on how to engineer, operate and manage the business risk of a cybersecurity program based on the NIST Cybersecurity Framework. This program is focused on candidates who need a detailed understanding of the NCSF to perform their daily roles as cybersecurity engineers, operators and business professionals.

All programs come with a certificate of completion and continuing education credits, such as PDU and CEUs. Students who successfully complete the certification programs and meet university requirements may transfer credits and enroll in one of UMass Lowell's master's degree programs in information technology, such as network security or cybersecurity. Those interested in taking the courses may find that programs such as workforce development, the G.I. Bill, apprenticeships, internships, employers and others will fund their participation.

The NCSF NICE Certification Training Library, available via online video, prepares candidates for the IT (CompTIA, Cisco etc.) Information Security (ISC^2, ISACA, CompTIA etc.) and Best Practice (ITIL®, Cobit, AGILE etc.) certifications outlined in the NIST NICE Cybersecurity Workforce Framework (NCWF). All programs come with a certificate of completion college credits and continuing education credits, such as PDU and CEUs.

Security Operations Training Center (SOTC) – UML has developed a Security Operations Training Center (SOTC) model that enables students to receive advanced training and hands on cybersecurity experience while delivering NIST Cybersecurity assessment, testing and continuous monitoring services to businesses and governments not capable of doing it themselves. UML can help training partners set up a SOTC of its own or provide SOTC services from its training SOC in Massachusetts.

Future Programs - UML is planning to develop additional courses in partnership with industry experts, academia and the private industry that will enable NCSF practitioners to gain ongoing knowledge, skills and abilities in cybersecurity.

Evaluating the Print, Digital Book and Video Courseware

The NCSF Practitioner course digital book can be viewed here using the following login information User: preview@skillpipe.com PW: **courseware2017**

Chapter 8 of the NIST CSF Practitioner video course can be found at here

For more information please contact Rick Lemieux at 401-764-0720 or rick.leieux@itsmsolutions.com