itSM Solutions®
IT Best Practice Training Programs

UMASS University of Massachusetts

NISTCSF.COM

NIST Cybersecurity Framework Training Solutions

Response to National Institute of Standards and Technology Cybersecurity Workforce RFI

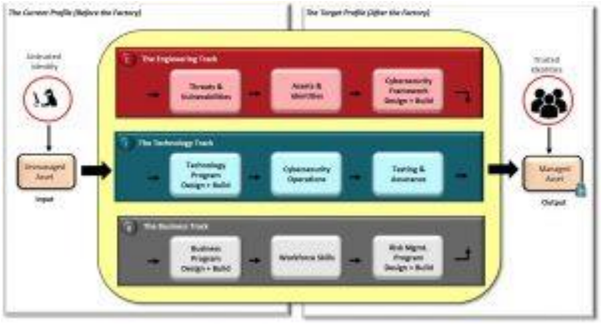
General Information

1. Are you involved in cybersecurity workforce education or training (*e.g.,*curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? *Note:* Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

NISTCSF.COM

NISTCSF.COM is a NIST Cybersecurity Framework (NCSF) workforce development program brought to you by UMass Lowell 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 Current Profile (Before the Factory)
The Target Profile (After the Factory)
Untrusted Identity
Unmanaged Asset
Input
The Engineering Track
Threats & Vulnerabilities
Assets & Identities
Cybersecurity Framework Design + Build
The Technology Track
Technology Program Design + Build
Cybersecurity Operations
Testing & Assurance
The Business Track
Business Program Design + Build
Workforce Skills
Risk Mgmt Program Design + Build
Trusted Identities
Managed Asset
Output

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

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

The UMass accredited cybersecurity workforce enablement program is built around the following six pillars.

- NIST Cybersecurity Framework Certification Training Based on the UMass Control Factory Model
- NIST Cybersecurity Framework Simulation Trainings to Help Students See Cybersecurity in Action
- NICE Certification Trainings Aligned with the NICE Cybersecurity Workforce Framework
- NIST Cybersecurity Association & Critical Sector Specific Trainings (i.e., Healthcare, Energy etc.)
- NIST Cybersecurity Policy & Law Specific Trainings (i.e., 23 NYCRR 500, GDPR etc.)
- NIST Cybersecurity Hands-On Training Delivered in UMass Security Operations Training Centers

UMass 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 UMass and other Academic, Government and Private 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, we have partnership agreements in place with Acquiros a U.S. based ISO 17024 examination institute 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 and PSA Security Networks the largest association of physical security manufacturers and installers in the world.

Listed below is a summary of the UMass NIST Cybersecurity Framework (NCSF) / NICE workforce development program. A copy of our corporate presentation and links to our classroom and video content are included below.

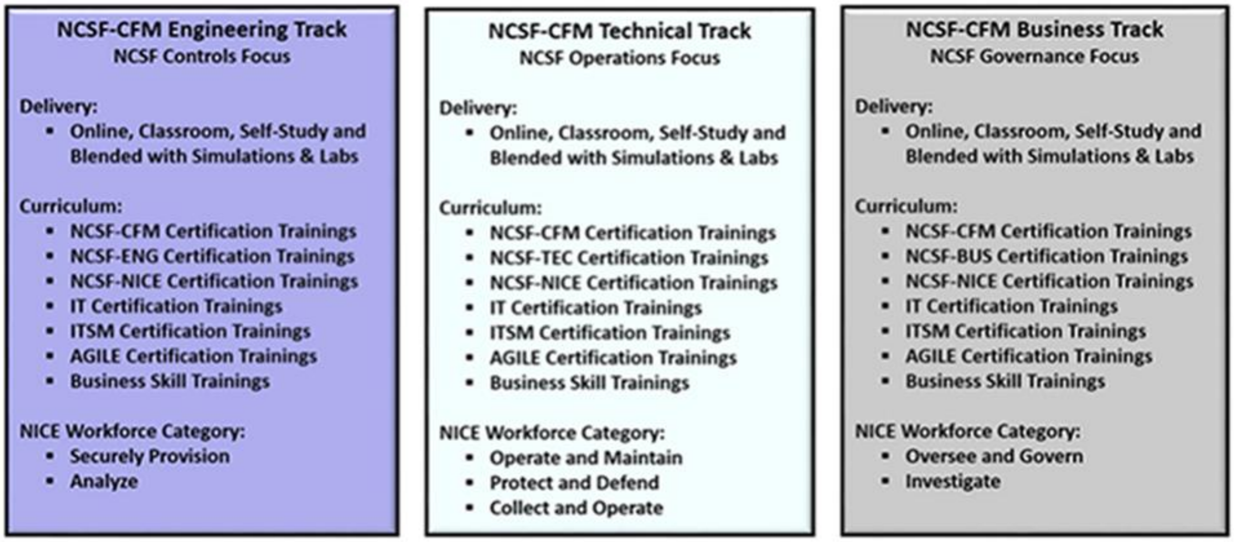
UMass Program Summary

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.

The itSM/UMass 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 partnership with government and industry and then continually improve it over time in partnership with academia and the other organizations across the globe.



NCSF-CFM Engineering Track
NCSF Controls Focus

Delivery:
- Online, Classroom, Self-Study and Blended with Simulations & Labs

Curriculum:
- NCSF-CFM Certification Trainings
- NCSF-ENG Certification Trainings
- NCSF-NICE Certification Trainings
- IT Certification Trainings
- ITSM Certification Trainings
- AGILE Certification Trainings
- Business Skill Trainings

NICE Workforce Category:
- Securely Provision
- Analyze

NCSF-CFM Technical Track
NCSF Operations Focus

Delivery:
- Online, Classroom, Self-Study and Blended with Simulations & Labs

Curriculum:
- NCSF-CFM Certification Trainings
- NCSF-TEC Certification Trainings
- NCSF-NICE Certification Trainings
- IT Certification Trainings
- ITSM Certification Trainings
- AGILE Certification Trainings
- Business Skill Trainings

NICE Workforce Category:
- Operate and Maintain
- Protect and Defend
- Collect and Operate

NCSF-CFM Business Track
NCSF Governance Focus

Delivery:
- Online, Classroom, Self-Study and Blended with Simulations & Labs

Curriculum:
- NCSF-CFM Certification Trainings
- NCSF-BUS Certification Trainings
- NCSF-NICE Certification Trainings
- IT Certification Trainings
- ITSM Certification Trainings
- AGILE Certification Trainings
- Business Skill Trainings

NICE Workforce Category:
- Oversee and Govern
- Investigate

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 UMass Lowell NCSF Control Factory Methodology on how to engineer, operate and manage the business governance 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 (ISC², 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) – UMass 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. UMass can help training partners set up a SOTC of its own or provide SOTC services from its training SOC in Massachusetts.

Additional Programs created in partnership with industry experts, academia and private training organizations across the globe - UMass is planning to develop additional courses in partnership with industry experts, academia and the private industry that will enable NCSF practitioners to gain additional 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

NISTCSF.COM Presentation

Our NISTCSF presentation can be found here

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Unfortunately, very little at this moment. The cybersecurity space is disorganized and dysfunctional because it was never considered core and mission critical to companies plus there was no framework to build around. The NIST CSF helps address the what and why and its up to academia and private industry to teach the how in the context of a cybersecurity lifecycle and continual improvement. Current cybersecurity workforce development programs (i.e., certifications) are a mile wide and an inch deep and pretty much specialist focused. What's needed are trainings for engineers, operations and business risk & professionals all working together to design, manage and improve a NIST CSF program across an enterprise and its supply chain. The networking and PC industry had this same problem back in the eighties. I wrote an article called One Hundred Thousand+ Cybersecurity Professionals Trained & Certified by 2020 *back in December of 2016 on how we can learn from the past to solve the cybersecurity workforce issues we face today.*

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

I think the current NICE Cybersecurity Workforce Framework is an excellent starting point, however additional work need to be done in specific industry critical sectors as they need more than just the basic cybersecurity training designations. UMass has been working with key industry associations, sectors and technology companies to better understand the specific requirements of each industry so we can incorporate that content into our certification training programs

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Based on the hundreds of people I spoke with in the cybersecurity space the answer is no 95% of the time. Basically, policies are built around certifications and experience because once again there was no framework to operate or measure from.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors)?

They only know what they know and since there was no framework to measure against they do not know much. Most think the cybersecurity world is built around certifications and those who have experience with firewalls, access control systems and applications. Most are not looking at cybersecurity as an organizational capability which is what is has become. I wrote an article titled Organizational Change is Key to Online Cybersecurity & Service Management *that answers the question listed above.*

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

*The only one I know of that teaches the knowledge, skills and abilities in alignment with the NCSF is the UMass program described above. Here is an article that was written by OSHEAN (*www.oshean.org*) the Research and Education Network (REN) in Rhode Island that has been working with UMass and other organizations looking to launch effective NIST Cybersecurity Workforce Development program. The UMass cybersecurity workforce development program focuses on the following:*

- ***LEARNING** the theory on how to design, build, instrument, test, manage and improve an NCSF program*
- ***SEEING** cybersecurity in "Action" using in-class or online simulation and gamification programs*
- ***APPLYING** cybersecurity theory in a real-world environment using project based design and configuration labs designed to teach the practical skills associated with the engineering, technology and business dimensions of an NCSF program*
- ***EXPERIENCING** NCSF by working in a state sponsored security operations centers (SOC) designed to deliver affordable NCSF assessment, continuous monitoring and research data to local governments, small to medium size businesses and academia*
- ***PREPARING** candidates to pass the IT, Cybersecurity and Industry Specific work and specialty role certifications outlined in the NCWF*

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The wrong picture is being painted about the workforce we need. We don't need to recruit only new people (university thinking) we need to recruit a combination of people from all walks of life (veterans, *unemployed, employed, exceptional rookies etc.). I wrote an article titled* Why Retired Military, Workforce Veterans and Exceptional Rookies Need to Be Part of Your Cybersecurity Team *that answers the question listed above*

7. How will advances in technology (*e.g.,* artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

It will affect it dramatically which is why the cybersecurity workforce needs to live beyond the walls of IT. One of our biggest fears is that of Industrial and Building Control systems as everything has or will have a cyber connection on it. To kick things off in this space UMass has signed a partnership PSA Security Networks the largest association of physical security manufacturers and installers in the world. We are working with its manufacturers and integrators to help the learn the KSA's to integrate NIST cybersecurity best practices into everything they do. We are also in discussions with the Control System Cyber Security Association International (CS^{2}AI) Established by and for the community of professionals defending ICS, IIoT, Industry 4.0, etc., (CS)^{2}AI is a network of individuals dedicated to the growth and expansion of career and educational opportunities for everyone involved with these critical infrastructure systems.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

I wrote an article titled NIST Cybersecurity Education Centers (NCEC) *that answers the question listed above. I also wrote another article titled* NIST Cybersecurity Framework (NCSF) - What's Missing? *that focuses on what missing from the NIST Cybersecurity Framework in order to make it useful and effective. The UMass Controls Factory was created to address the "What's Missing" aspects of the framework.*

ii. iii. iV. and V At the state or local level, including school systems, private sector, education and training providers and technology providers?

The UMass NIST Cybersecurity Workforce Development program is built around a public private partnership where UMass is looking to partner with the government (Federal, State and Local), academia (public and private) and private industry to deliver and continuously improve its NCSF content and Security Operations Training Center (SOTC) capabilities and services