March 2017

WORKING GROUP 7
Cybersecurity Workforce

Final Report – Cybersecurity Workforce Development Best Practices Recommendations

Table of Contents

1 Executive Summary

Cybersecurity refers to the technologies and techniques used to protect information and systems from being stolen, compromised or attacked. This includes unauthorized or criminal use of electronic data, attacks on networks and computers, and viruses and malicious codes. Cybersecurity is a national priority and critical to the well-being of all organizations.[1]

Over the past five years, cyberattacks have been on the rise in frequency and impact. Headline grabbing attacks at Sony Pictures exposed copyright content, company confidential data and personal privacy information that forced Sony to shut down their online services for weeks. The Ashley Madison data breach resulted in the exposure and public posting of some very personal data. And, the Office of Personnel Management was the target of a persistent breach that compromised tens of millions of records of personal information related to current and past federal workers including security clearance information.

However, it is not just data that is being stolen. Researchers demonstrated the ease with which they were able to wirelessly exploit and gain control of the steering, brakes and transmission of a Jeep Cherokee. Recently, suspected state sponsored cyberattacks in the Ukraine caused a six hour power outage for some 80,000 customers. This sophisticated and highly coordinated attack combined Telephone Denial of Service (TDOS), hacked control systems, and compromised monitoring to attack the critical infrastructure while "blinding" the utility operator from detecting the problem. It is believed to be the first critical infrastructure attack of its kind and underscores the national security implications of cybersecurity.

Anticipating the potential kinetic impacts of a cyberattack on critical infrastructure, President Obama released Executive Order 13636, Improving Critical Infrastructure Cybersecurity, citing the need for improving cybersecurity in response to the repeated cyber intrusions into critical infrastructure.[2] The cornerstone of this order is the enhancement of security and resilience of critical infrastructure through the voluntary, collaborative efforts of federal agencies and commercial industry.

Cybersecurity professionals have unique skills, are in short supply, and are vital to our nation's security. As a result, competition for talent is fierce and establishing a strong team is essential. This requires organizations to tailor how they plan for their cybersecurity workforce so they have the right people in the right positions. In the White House Executive Order 13636, Improving Critical Infrastructure Cybersecurity, the President assigned the Department of Homeland Security (DHS) the leadership role to work with Federal Agencies and sector specific regulators to help ensure we have skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders. One of the results of this mission, is the collaborative effort with the National Initiative for Cybersecurity Education (NICE) that resulted in the development of the National Cybersecurity Workforce Framework (NCWF).[3]

---

[1] Cybersecurity Workforce Development Toolkit, How to Build a Strong Cybersecurity Workforce, https://niccs.us-cert.gov/

[2] Executive Order 13636 dated February 12, 2013

[3] In November, NIST released for comment an update in partnership between NICE and DHS that changes the nomenclature back to the NICE Cybersecurity Workforce Framework

The mission of the Communications Security, Reliability and Interoperability Council (CSRIC or Council) is to provide recommendations to the Federal Communications Commission (FCC) to ensure, among other things, optimal security and reliability of communications systems.[4] Furthermore, the Council's recommendations specifically address the prevention and remediation of detrimental cyber events. Working Group 7 of the CSRIC V is specifically chartered to provide recommendations for the CSRIC's consideration regarding any actions the FCC should take to promote improvements in cybersecurity workforce development. [5]

The CSRIC V Working Group 7 has been tasked to examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field.

Specifically, this working group will leverage existing work in this context to enhance the volume and quality of the workforce, including[6]:

(1) demonstrating the application of the National Cybersecurity Workforce Framework (NCWF) to the common and specialized work roles with in the communications sector;
(2) identifying any gaps or improvements in the NCWF for evolving work roles or skill sets that should be included in sector members' workforce planning; and
(3) identifying, developing, and recommending best practices and implementation thereof to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. In this respect, the working group should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

This Final Report builds upon the Interim Report that specifically addressed the demonstration of the applicability of the NCWF to the Communications Sector and the identification of gaps or improvements to the NCWF. Further, it documents the approach that the Working Group 7 applied to identify, develop and recommend best practices for consideration by the CSRIC V membership for inclusion in the Final Report. In order to manage the scale of the task, Working Group 7 chose to segment the information gathering and analysis process with targeted findings specific to each segment. We then identified best practices based on our analysis for each segment for consideration. This Final Report presents those Best Practices deemed to be most appropriate and impactful for consideration by the CSRIC V as recommendations to the FCC and the Communications Industry as a whole.

[4] Charter of the FCC's Communications Security, Reliability and Interoperability Council
[5] CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016
[6] The FCC CSRIC Working Group Description references the NICE CWF; Working Group 7 has opted to refer to this framework using the April 2014 NICCS designation of the National Cybersecurity Workforce Framework (NCWF) for external consistency

The National Cybersecurity Workforce Framework (NCWF)[7] provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Competencies, and KSAs.

1. **Categories** are common major functions regardless of job titles or other occupational terms.
2. **Specialty Areas** are common types of cybersecurity work which are grouped with similar areas under a specific Category.
3. **Competencies** are areas of expertise required for the successful performance of a job function; these are defined in the framework through the association of specific KSAs.
4. **Knowledge, Skills and Abilities (KSAs)** are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training experience, education, or training.

Working Group 7 (WG7) leveraged the prior NCWF analysis and process completed by the Financial Sector as a best practice to accelerate our task of evaluating the NCWF. The summary conclusions are that the NCWF is a viable, flexible framework that can and should be applied to the Communications Sector for Cybersecurity Workforce Development Planning. Building on this finding by the Working Group members, we proceeded to complete the initial evaluation of the "building blocks" – Categories, Specialty Areas, Competencies, and KSAs – for gaps and improvements that should be included in the application of this dataset to the Communications Sector. Our work product is attached to this Final Report as Appendices 1 and 2. It was also delivered to the FCC as a working database in Microsoft Excel format for unrestricted use.

We recognize that cybersecurity workforce development is undergoing rapid change and evolution. This Final Report provides a lexicon that can be used to articulate the specific Workforce needs of the Communications Sector for roles involving cybersecurity. However, it is a static dataset and needs to evolve as the NCWF matures and Cybersecurity Workforce Development Planning gains maturity in our respective organizations. As part of the Final Report, WG7 provides specific recommendations for consideration by CSRIC on a process for adaptation and improvement of the sector specific dataset.

2 Introduction

In February of 2013, the White House released Executive Order 13636, Improving Critical Infrastructure Cybersecurity, citing the need for improving cybersecurity in response to the repeated cyber intrusions into critical infrastructure.[8] The cornerstone of this order is the enhancement of security and resilience of critical infrastructure through the voluntary, collaborative efforts of federal agencies and commercial industry.

The Executive Order assigned the National Institute of Standards and Technology (NIST) to develop a flexible cybersecurity framework for critical infrastructure protection that could be adapted to meet the specific needs of individual sectors. The Order also calls for the Department of Homeland Security (DHS) to provide technical assistance to agencies in the development of their cybersecurity workforce and programs.

[7] https://niccs.us-cert.gov/training/tc/framework
[8] Executive Order 13636 dated February 12, 2013

A national effort to draft a Cybersecurity Workforce Framework began in 2010 with more than 20 Federal Departments and Agencies contributing to the initial drafting process. A draft of the National Cybersecurity Workforce Framework was posted for public comments in September 2011 in conjunction with the Second Annual NICE Conference[9] hosted by NIST. The National Cybersecurity Workforce Framework (NCWF) version 1.0 was posted in April 2013 to the National Initiative for Cybersecurity Education (NICE) website. Subsequently, DHS began to work on updating the NCWF by seeking input from across the private sector, academia, and government. NCWF version 2.0 was posted by DHS to its cybersecurity workforce portal in April 2014. DOD, DHS, and the NICE program office at NIST developed an updated draft special publication of the NCWF released by NIST for public comments in November of 2016 that adds cyber work roles and the associated Knowledge, Skills, Abilities (KSAs) into a national cyber workforce framework.[10]

The Executive Order further calls for the sector specific government agencies to engage in a consultative process with DHS and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure in a voluntary and collaborative partnership. The mission of the Communications Security, Reliability and Interoperability Council (CSRIC) is to provide recommendations to the Federal Communications Commission (FCC) to ensure, among other things, optimal security and reliability of communications systems.[11] Furthermore, the Council's recommendations specifically address the prevention and remediation of detrimental cyber events. Working Group 7 of the CSRIC V is specifically chartered to provide recommendations for the CSRIC's consideration regarding any actions the FCC should take to promote improvements in cybersecurity workforce development.[12]

A joint survey published by ISACA and the RSA Conference in 2015 indicated that over 80% of corporations expected a cyberattack in the current calendar year. The same report estimated that 35% of corporations are unable to fill their open positions with qualified cybersecurity personnel. Furthermore, less than half of the corporations surveyed believed that their current security teams had the necessary skills and tools to enable them to detect and respond to complex incidents. According to a report published in October of 2015, "Securing our Future: Closing the Cybersecurity Talent Gap", jointly published by Raytheon and the National Cyber Security Alliance (NCSA), there were almost 240,000 job postings for cybersecurity-related job openings in 2014, a 91 percent increase from 2010. More recently, Symantec estimated the number at 300,000. Regardless of the source, it is painfully clear that industry is still not closing the cybersecurity workforce gap.

The National Cybersecurity Workforce Framework (NCWF)[13] provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Competencies, and KSAs.

[9] http://csrc.nist.gov/nice/Sept2011-workshop/index.html
[10] http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf
[11] Charter of the FCC's Communications Security, Reliability and Interoperability Council
[12] CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016
[13] https://niccs.us-cert.gov/training/tc/framework

1. **Categories** are common major functions regardless of job titles or other occupational terms. The National Initiative for Cybersecurity Careers and Studies (NICCS) published NCWF includes seven Categories: Securely Provision, Operate and Maintain, Collect and Operate, Analyze, Protect and Defend, Oversight and Development, and Investigate.
2. **Specialty Areas** are common types of cybersecurity work which are grouped with similar areas under a specific Category. The NCWF defines 31 Specialty Areas.
3. **Competencies** are areas of expertise required for the successful performance of a job function; these are defined in the framework through the association of specific KSAs. NICCS identifies 65 Competencies.
4. **Knowledge, Skills and Abilities (KSAs)** are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training experience, education, or training. Knowledge is a body of information applied directly to the performance of a function. Skill is an observable competence to perform a learned psychomotor act. Ability is competence to perform an observable behavior or a behavior that results in an observable product. The NCWF defines 369 KSAs that can be each associated with one or more Specialty Areas.

By using these basic building blocks to provide a common language to speak about cyber roles and jobs, the NCWF helps to define professional requirements in cybersecurity regardless of organizational structure or job titles. It has been developed largely with input from the Federal Government and is currently being refined by the nation's cybersecurity stakeholders, including academia, professional, and non-profit organizations, and private industry. It is meant to be flexible and organizations are encouraged to use it as a general guide to fit their specific needs. Some examples include:

- Standardize how positions are managed and described by populating position descriptions with Tasks and KSAs from the Workforce Framework.
- Incorporate Tasks and KSAs into job advertisements to attract candidates who can perform needed job functions.
- Develop career paths that outline the Tasks and KSAs staff need to perform to progress to the next level.

While some of the NCWF is based on Federal Government programs, any organization can customize it as needed. A more comprehensive overview of the NCWF is available at the National Initiative for Cybersecurity Careers and Studies (NICCS).[14]

[14] The Draft NIST Special Publication 800-181 that updates the NCWF includes the addition of Work Roles to the components used to organize roles and responsibilities resulting in the following updated common set of components:

- **Categories** – A high-level grouping of common cybersecurity functions;
- **Specialty Areas** – Distinct areas of cybersecurity work;
- **Work roles** – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks;
- **Tasks** – Specific work activities that could be assigned to the professional working in one of the NCWF's Work Roles; and
- **Knowledge, Skills, and Abilities (KSAs)** – Attributes required to perform Tasks, demonstrated through relevant experience or performance-based education and training.

2.1 CSRIC Structure

Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4, Communications Infrastructure Resiliency		Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Evolving 911 Services	Working Group 2: Emergency Alerting Platform	Working Group 3: Emergency Alert System	Working Group 4A: Submarine Cable Resiliency	Working Group 4B: Network Timing Single Source Risk Reduction	Working Group 5: Cybersecurity Information Sharing	Working Group 6: Secure Hardware and Software – Security by Design	Working Group 7: Cybersecurity Workforce	Working Group 8: Priority Services	Working Group 9: WiFi Security	Working Group 10: Legacy Systems and Services Risk Reduction

Table 1 - Working Group Structure

2.2 Working Group 7 Team Members

Working Group 7 consists of the members listed below:

Name	Company
Bill Boni (Co-Chair)	T-Mobile
Drew Morin (Co-Chair)	T-Mobile
Bill Newhouse	NICE Program Office at NIST
Quentin Sa'Lay	Comcast NBC Universal
Barbara Endicott-Popovsky	University of Washington
Frank Cicio	IQ4 representing Cybersecurity Workforce Alliance
Kim Keever	Cox
Upendra Chivukula	State of New Jersey
Kathrina Hardy	Verizon
Philip Linse	CenturyLink
Chris Boyer	AT&T Services
Erik Wallace	Comtech
Jay English	Department of Homeland Security
Andrew Fry	University of Washington
Mike Geller	Cisco Systems
Kazuhiro Gomi	NTT America
Scott Haas	IID Security Central
Shinichi Hirata	NTT Corporation
John Hoag	Case Western Reserve University
Masato Kimura	NTT Corporation
Steve Mace	NCTA
Shawn Matthews	PacOpticNetworks
Daishi Sakakibara	NTT Corporation
Matthew Straeb	Alert FM
Nobumitsu Takeuchi	NTT Corporation
Kathy Whitbeck	Nsight
Shinichi Yokohama	NTT Corporation

Table 2 - List of Working Group Members

3 Background

A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure. There is a well-documented shortage of general cybersecurity experts; however, there is an even more acute shortage of qualified cybersecurity experts who also have an understanding of the unique challenges to critical infrastructure. As the cybersecurity threat and technology environment evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain and continuously improve the necessary cybersecurity practices

within critical infrastructure environments.

To address this accelerating gap, the Federal government established the National Initiative for Cybersecurity Education (NICE). NICE is led by NIST as a collaborative effort involving Federal, academic, and industry partners with the mission to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. Various efforts, including NICE, seek to accelerate learning and skills development, nurture a diverse learning community, and guide career development and workforce planning. Organizations must understand their current and future cybersecurity workforce needs, and develop hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems delivering critical infrastructure services.[15]

3.1 Cybersecurity Workforce Planning[16]

Workforce planning is a systematic way for organizations to determine future human capital requirements (demand), identify current human capital capabilities (supply), and design and implement strategies to transition the current workforce to the desired future work state. Best in class workforce planning is designed in a repeatable and reliable fashion, highlighting risks and forecasting needs over time.

Effective workforce planning highlights potential risk areas associated with aligning the workforce to work requirements. Applied correctly, workforce planning allows organizations to adjust resources to meet future workloads, patterns of work, and fundamental changes in how work is accomplished. A workforce planning approach must fit the needs of a specific organization and account for unique characteristics of the cybersecurity profession.

Leading practice workforce planning consists of three components:

- Process: Establishing an integrated and consistent means of diagnosing workforce needs and risks. This includes a defined model, data, and analytics.
- Strategy: Providing a direct line of sight between business and workforce requirements. This includes a shared vision, governance, and continuous monitoring or performance.
- Infrastructure: Supporting execution of an effective and repeatable workforce planning process. This includes a healthy workforce of people, collaboration across levels and enabling technology.

Using a Workforce Planning Process, such as the example provided below, an organization can conduct a cybersecurity workforce and workload analysis, enabling it to identify current and future needs and potential gaps which may impact an organization's ability to meet goals and objectives.

[15] http://csrc.nist.gov/nice/
[16] https://niccs.us-cert.gov/careers/workforce-planning

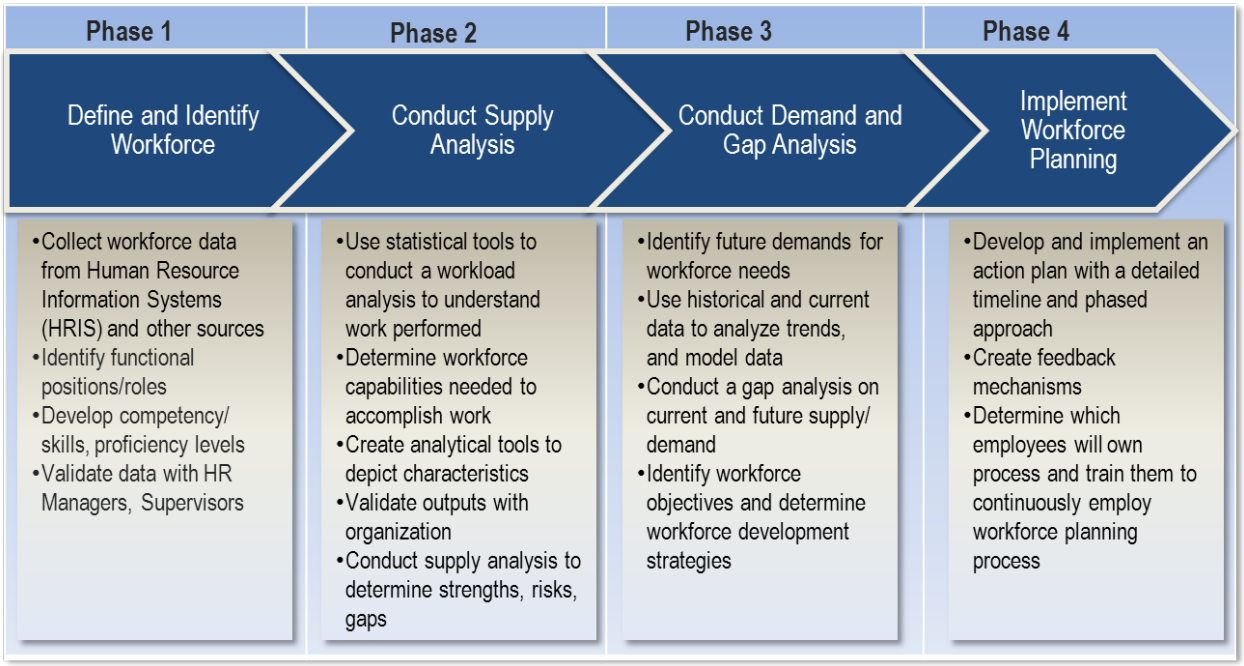


Figure 1 – Example Workforce Planning Process

Additionally, cybersecurity workforce planning requires a shared vision and performance management. A shared vision provides a common language and taxonomy to define cybersecurity workload and workforce allowing agile response to emerging technology and new threats. Performance management is also key to evaluating cybersecurity professionals' skills within specific technology-based specialties. The National Cybersecurity Workforce Framework provides additional support to organizations in considering this critical aspect of cybersecurity workforce planning.

One of the most important aspects of workforce planning is identifying the workforce and workload requirements that impact the nature of the work performed. Workload and workforce requirements are the unique characteristics that make one profession different from another, and may change how workforce planning is executed for that workload or workforce. DHS found unique workload and workforce requirements specifically important to cybersecurity.

Workload Requirements:

- Surge Capacity– the need to expand resources and capabilities in response to prolonged demand.
- Fast-paced– the need to sustain multiple work streams occurring rapidly.
- Transformative– the need to adapt to fundamental changes to technology, processes, and threats.
- High Complexity– the need to employ a large number of intricate technologies and concepts.

Workforce Requirements:

- Agile– the ability to shift between roles or needs should a threat warrant different support.
- Multi-functional– the ability to maintain and execute a variety of activities at any given time.
- Dynamic– the ability to provide for constant learning to effectively approach new endeavors and problems.
- Flexible– the ability to move into new roles or environments quickly to increase knowledge and skills.
- Informal– the ability to work in a nontraditional environment.

Coupled with workforce planning best practices, these requirements help identify workforce planning needs as they apply to cybersecurity.

DHS recommends cybersecurity workforce planning use a two-pronged approach. As outlined above organizations should use workforce planning to identify cybersecurity skills, proficiency gaps and workload. Organizations should develop an approach that integrates best practices for workforce planning specific to cybersecurity with the seven categories of the National Cybersecurity Workforce Framework—providing a standardized and categorized way from which to build this approach. Secondly, organizations should use a capability maturity model to apply the elements of best practice workforce planning to analyze their cybersecurity requirements and maturity needs.

3.2 The DHS Capability Maturity Model (CMM)

As the cybersecurity workforce continues to evolve, and organizations track and manage against the changing cybersecurity environment, understanding where current workforce planning capabilities lie and how to develop those capabilities has become increasingly important. A capability maturity model (CMM) provides a structure for organizations to baseline current capabilities in cybersecurity workforce planning, setting a foundation and consistency of evaluation. It allows organizations to compare their capabilities to one another, and enables leaders to make better decisions about how to support progression and what cybersecurity human capital initiative investments to make.

DHS's CMM segments key activities into three main areas: 1) process and analytics, 2) integrated governance, and 3) skilled practitioners and enabling technology.

Process represents those activities associated with the actual steps an organization takes to perform workforce planning and how those steps are integrated with other important business processes throughout the organization. **Analytics** represents those activities associated with supply and demand data and the use of tools, models, and methods to perform workforce planning analysis.

Integrated governance represents those activities associated with establishing governance structures, developing and providing guidance, and driving decision-making. It is the building block to an organization's overall workforce planning strategy and vision as well as assignments of responsibility, promotion of integration, and issuing of planning guidance.

Skilled Practitioners represents the activities associated with establishing a professional cadre of workforce planners within an organization. **Enabling Technology** represents the activities associated with the accessibility and use of data systems.

3.3 Using the DHS Maturity Model

The DHS Cybersecurity Workforce Planning CMM has three maturity levels. These levels are limited, progressing, and optimizing. Limited is the most basic level, portraying a key activity area or segment of an organization's cybersecurity workforce planning capability that is in its infancy. This level of capability is at its start of development and may be represented by an organization having limited establishment of processes, lacking clear guidance or having little in terms of data and analysis methods. The progressing level describes a key activity area of some aspect of cybersecurity workforce planning which an organization has started to perform, commonly represented by an organization establishing some infrastructure to support workforce planning efforts. The final level of maturity, optimizing, depicts a key activity area or segment of cybersecurity workforce planning capability that has fully developed, such as one that is integrated with other business processes and can support different levels of workforce and workload analysis, the results of which drive short and long term decision making for the cybersecurity workforce.

It is important to note that organizations will have differing goals when it comes to the maturation of the cybersecurity workforce planning capability and that all organizations do not need to reach the optimizing state for all key areas. This decision should take into account many different variables. Leaders need to assess the impacts of: allocation of resources, implementation, timing, and return on their investments. Therefore, organizations should view their maturity rankings less as a grade or judgment and more as an indication of resources spent on workforce planning. Having a "limited" maturity level does not equate to "bad" workforce planning, but rather that the organization has not dedicated resources to partially or fully develop that aspect of the maturity model, and that there are extenuating circumstances for that outcome.

In order to use the model, organizations must have an accurate understanding of their current workforce planning capabilities as they relate to the three segment areas, with the ability to site specific evidence of conducting related activities. An organization's current capability is the springboard upon which to build further maturity, using the CMM to pinpoint necessary next steps and decision points for progression. DHS recommends a three-step process to using the CMM to determine an organization's current cybersecurity workforce planning capability and progress individual organizational maturity along the continuum:

- Gather data on qualitative CMM variables;
- Analyze data and determine current maturity levels by CMM key area; and
- Determine priority areas for increased maturity and develop action plans.

4 Objective, Scope, and Methodology[17]

4.1 Objective

The CSRIC V Working group 7 has been tasked to examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field.

4.2 Scope

Specifically, this working group leveraged existing work in the context to enhance the volume and quality of the workforce, including[18]:

- demonstrating the application of the National Cybersecurity Workforce Framework (NCWF) to the common and specialized work roles with in the communications sector;
- identifying any gaps or improvements in the NCWF for evolving work roles or skill sets that should be included in sector members' workforce planning;
- identifying, developing, and recommending best practices and implementation thereof to mitigate insider threats, including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities within the communications sector and particularly with respect to personnel having access to the most critical elements of the nation's communications network assets; and
- considering means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

4.3 Methodology

The approach that Working Group 7 (WG7) undertook to address the cybersecurity workforce development tasking assigned by CSRIC V was to address the basics of a common lexicon based on the National Cybersecurity Workforce Framework (NCWF) model first. Once these building blocks were completed, we undertook a survey of different stakeholders representing various segments of the communications sector to understand current best practices in cybersecurity workforce development. The resulting data was analyzed to produce recommendations that were approved by the Working Group membership for presentation to the CSRIC.

4.3.1 Evaluate National Cybersecurity Workforce Framework

As a starting point, we elected to begin by reviewing a similar work product completed by the Financial Sector in cooperation with the Cybersecurity Workforce Alliance (CWA). WG7 Members focused on defining the role profiles from an extended baseline of the NCWF Specialty Areas, Competencies, and KSAs instead of starting our work from scratch. WG7 leveraged the CWA data set and process developed in support of the Financial Sector as our

[17] CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016
[18] The FCC CSRIC Working Group Description references the NICE CWF; Working Group 7 has opted to refer to this framework using the NICCS designation of the National Cybersecurity Workforce Framework (NCWF) for external consistency

starting point. The CWA data set was the result of a similar sector specific assessment of the NCWF. Our approach was to leverage:

- the extended Workforce Profiles and Roles already developed for the Finance sector as a starting point, and
- the direct experience from CWA representatives in extending the taxonomy to address gaps or improvements.

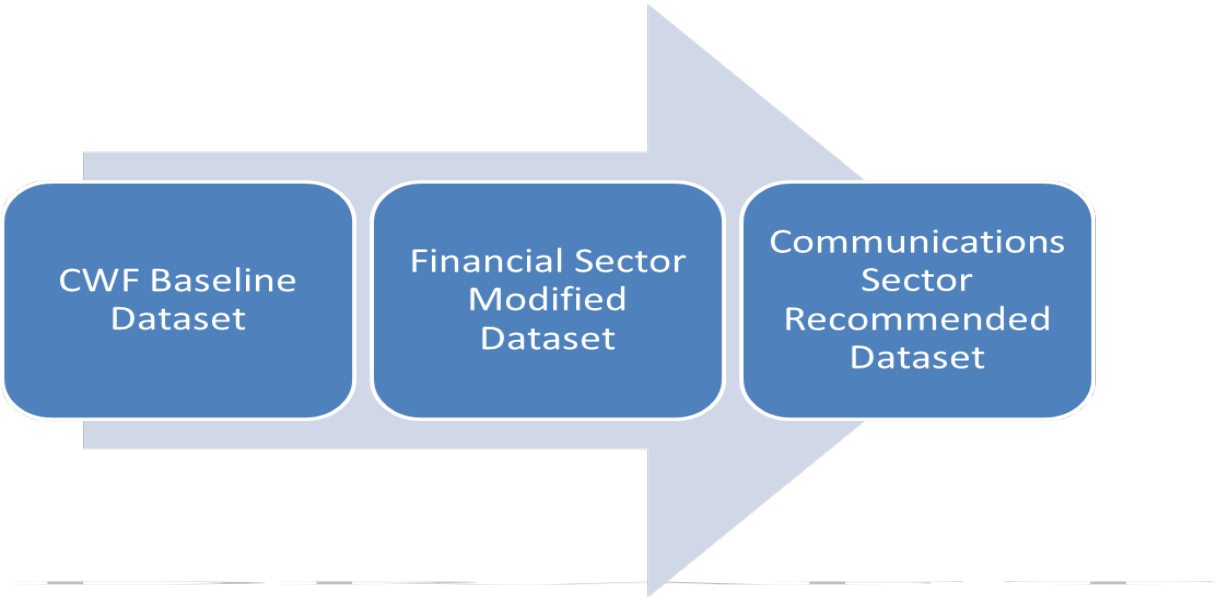


Figure 2 - NCWF Evaluation Process

The resulting taxonomy that was captured in the information base during the first part of the Gap Analysis is available to be shared across the communications sector. It is included in Appendices 1 and 2 to this Final Report.

4.3.1.1 Application of NCWF to the Communications Sector

The first task of the Working Group was to demonstrate the application of the National Cybersecurity Workforce Framework (NCWF) to the common and specialized work roles with in the Communications Sector. For each Category, Specialty Area, Competency, and KSA, the Working Group members were surveyed to assess specifically if the existing entry in the NCWF was applicable to the Communications Sector. As our Working Group including a diverse subset of the overall Communications Sector, Public Safety, Federal/Local Government, and Academia, an internal survey of the membership provided a broad assessment of the applicability of the NCWF to our sector. The inputs were then aggregated and reviewed by the Working Group as a whole. The recommendation from the membership was to be inclusive in our assessment of the NCWF – meaning that we did not remove any of the specific KSAs, Competencies, etc. in the data set we were provided even if the specific entry might not be directly applicable to a specific member of the sector. As a result, we were unanimous in our determination that the model is in fact applicable to the Communications sector and that the expansion of the component data by the Financial Sector was also applicable.

4.3.1.2 Identify Gaps and Improvements

After accepting the NCWF as an applicable structure to develop a common language to describe cybersecurity work, we proceeded to identify any gaps or improvements in the NCWF for evolving work roles or skill sets that should be included in sector members' workforce planning. Again, each of the Working Group members were tasked to review the KSAs, Competencies, Specialty Areas, and Categories for any gaps or modifications to better reflect the specific needs of their segment of the Communications Sector. This data was aggregated and distributed to the membership for final comment and approval. The resulting dataset detail is included in Appendices 1 and 2 to this report.

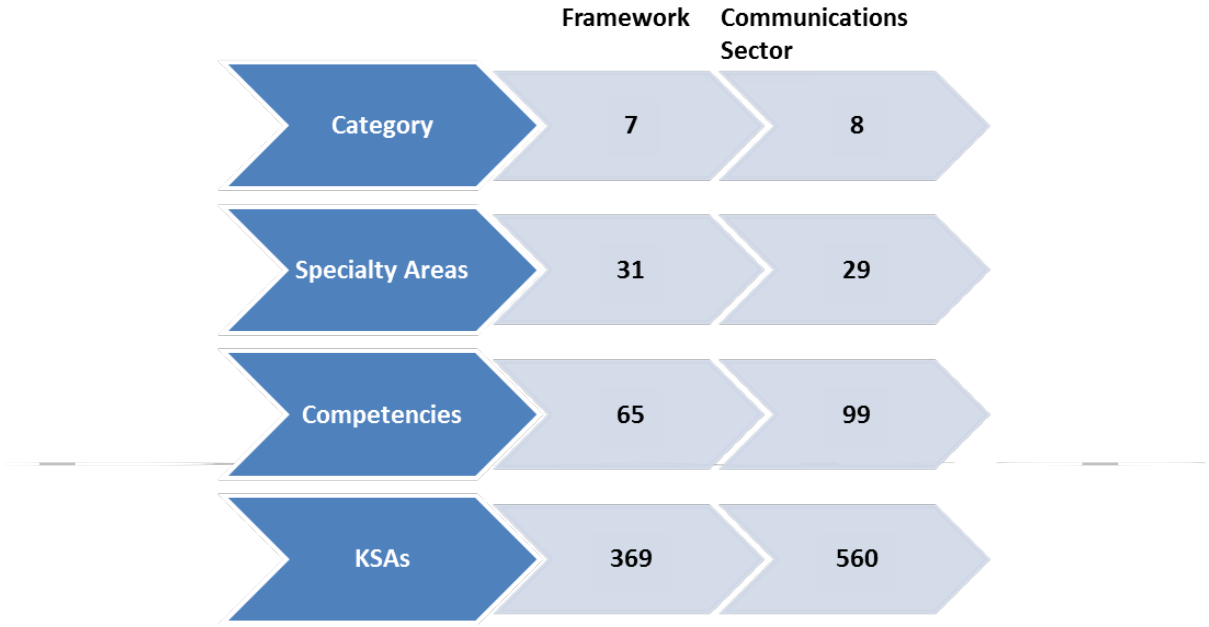


Figure 3 - Summary Data from NCWF Gap Identification

4.3.2 Identify, develop and recommend Best Practices

The second phase of the Working Group assignment is to identify, develop and recommend best practices and implementation thereof to mitigate insider threats within the communications sector including through scalable means to enhance transparency, accountability and validation of skills, knowledge and abilities, particularly with respect to personnel having access to the most critical elements of the nation's communications network assets. The approach we followed was to survey constituent members of the Communications Sector on their workforce planning programs as they related to cybersecurity and more specifically the National Cybersecurity Workforce Framework. We also gathered experiential data from outside the Communications Industry sector, specifically from Academia, Federal Government and State Government to provide insight into the best practices, policies and tools developed as a result of these different implementations of the NCWF.

4.3.2.1 Communications Industry

The Working Group members reviewed their current company internal workforce planning procedures and specifically, cybersecurity workforce development, to provide "sanitized" examples of best practices, policies, and tools that can be shared externally with the FCC and Communications Sector companies.

4.3.2.2 Academic Segment

There are current multiple Academic, Government and industry organizations reviewing cybersecurity education curriculum. These include the Association for Computing Machinery (ACM) and the NSA/DHS joint effort to designate National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD). The members of the Academic Segment have made it clear that there is a need to agree on a common core for cybersecurity curriculum that meets the needs of the education marketplace and takes into consideration the different types of institutions and their goals. WG7 cataloged various initiatives that are ongoing across the Academic community with the participation of industry and government to define cybersecurity education curriculum and the challenges they face.

In addition to the activities focused on curriculum development, the WG7 identified and reviewed various programs representing successful partnerships between Government, Industry and Academia to expand the talent pool available to seek education in areas of study that would prepare them to fill openings in the cybersecurity workforce. These programs vary across the communities served and the methods employed but they serve a common purpose in that they are encouraging more students to pursue academic studies in the disciplines necessary to support the growing demand. The result of this data gathering and analysis informed our findings to provide guidance to the CSRIC on recommendations for the FCC to enhance workforce development.

4.3.2.3 Public Safety

Public Safety networks are undergoing a transformational evolution from TDM networks to the Internet Protocol based Next Generation to support 911 emergency call handling. At the same time, FirstNet is anticipated to completely change the way First Responders will interact with each other and share data with local, regional and even Federal entities. The December 2015 FCC Task Force on Optimal PSAP Architecture report from Working Group 1 on cybersecurity was tasked

> "…to address the issues of increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy 9-1-1 environment, and develop recommendations for PSAP-specific cybersecurity practices based on the NIST Cybersecurity Framework and other foundational resources that include the results of Federal cybersecurity focused reports and activities of CSRIC and DHS; industry specific standards bodies such as NENA, APCO, and ATIS; and commercial industry best practices."[19]

This report included a discussion providing guidance on leveraging the NCWF for the development of training programs specific to the needs of the Public Safety segment. The

[19] Task Force on Optimal PSAP Architecture, Working Group 1, Optimal Cybersecurity Approach for PSAPs

Working Group reviewed this guidance to identify opportunities for and impediments to execution.

4.3.2.4 Financial Sector

Working Group 7 leveraged work done by the CWA in support of the Financial Sector as part of our review of the National Cybersecurity Workforce Framework. In this section, we review some of the lessons learned and practices from the Financial Sector as part of their initiative to tackle the cybersecurity workforce development gap. By leveraging the work already completed, and supporting their ongoing activities intended to inform the NCWF version 2.0 development of roles and related updates, WG7 intends to establish a recurring process for Communications Industry continuing participation in the evolution of the NCWF to assure our industry requirements are included in future publications of the guiding standards.

4.3.2.5 Federal Sector

The 2013 Executive Order on Critical Infrastructure Security assigns roles for the adoption of the cybersecurity framework for critical infrastructure protection[20] and specifically calls for the Department of Homeland Security to coordinate the provision of technical assistance to agencies on the development of their cybersecurity workforce.[21] The Working Group conducted a review of the DHS NICCS[22] available tools, practices, and policies for Cybersecurity Workforce Development[23] that have been leveraged by Federal Sector agencies. Further, WG7 reviewed guidance provided by the recent focus on workforce in both the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government[24] (October 2015), and the workforce aspects of the Cybersecurity National Action Plan (CNAP).[25]

Specific activities and programs within the Department of Defense, citing the emerging change in training focus from certification based to KSA focused metrics driven, representing best practices in cybersecurity training, were included in our review. Another notable program intended to inform best practices is the OPM Scholarship For Service program. WG7 members met with representatives from OPM to understand the specifics of the program. As a result of these activities, WG7 identified a number of example best practices currently in use by the Federal Sector that were assessed for applicability to the Communications Industry.

4.3.2.6 State Government Sector

The National Association of State Chief Information Officers (NASCIO) in partnership with Deloitte conducted a cybersecurity study in 2014 based on a comprehensive survey of State Chief Information Officers. Among the summary findings of the report, the cybersecurity workforce gap was specifically called out as a talent crisis:

[20] http://www.nist.gov/cyberframework/index.cfm
[21] Executive Order 13636 of February 12, 2013
[22] https://niccs.us-cert.gov/
[23] https://www.dhs.gov/topic/cybersecurity-education-career-development
[24] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf
[25] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

> "The skill sets needed for effective cybersecurity protection and monitoring are in heavy demand across all sectors. State CISOs are struggling to recruit and retain people with the right skills, and they will need to establish career growth paths and find creative ways to build their cybersecurity teams."[26]

In addition to the activities of national organizations, many State governments are pursuing programs meant to address the cybersecurity workforce development challenge. For example, the Workforce Development and Education Subcommittee of the State of California's Office of Emergency Services is currently pursuing a program to "develop a consistent definition and criteria for cybersecurity expertise to serve the State of California". The WG7 members also engaged with the NICE Working Group (NICEWG)[27] subgroups to leverage their extended reach across the Nation to identify state and local progress in areas of transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. The NICEWG has been established to provide a mechanism by which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.

The Working Group consolidated the information gathered from this sample of ongoing workforce development program activities in support of State government cybersecurity needs. The purpose here was not to create an exhaustive compendium, but rather to provide examples of active programs with the purpose of providing insights into current State actions, policies and tools to inform the CSRIC V members.

5 Findings

5.1 Analysis of the National Cybersecurity Workforce Framework

Development of a common framework for describing cybersecurity work enables employers to develop job descriptions that reflect the specific and critical knowledge, skills, and abilities with a consistent format and language. The development of this common lexicon enables the various constituents of the workforce planning supply chain to be more efficient in communicating specific requirements in a consistent and replicable manner. The end result is a convergence of efforts across a common framework to address the nation's cybersecurity workforce development requirements. This convergence requires a cooperative effort involving Academia, Government, and Industry to align on a common lexicon and framework. It does not require the mandate of a set of the same tools, curriculum, processes and policies. With that in mind, the CSRIC V Working Group 7, Workforce Development, focused on identifying and documenting the "building blocks" of a common lexicon and identifying current best practices for cybersecurity workforce development that can then be used by Industry, Academia, and Government to accelerate the development and implementation of their specific planning processes.

[26] 2014 Deloitte-NASCIO Cybersecurity Study – State governments at risk: Time to Move Forward, NASCIO Publications, October 2014
[27] http://csrc.nist.gov/nice/nicewg.html

5.1.1 Application of the National Cybersecurity Workforce Framework (NCWF) to the Communications Sector

In evaluating the value of the NCWF, we further agreed with the inputs from Government representatives based on the collective review from NIST, DHS and the Office of the Secretary of Defense (OSD) that the Cybersecurity Workforce Framework and the recently released draft cyber workforce special publication:

- Provides organizations with the common lexicon that categorize and describe cybersecurity work, as well as the knowledge, skills, and abilities required to perform tasks that constitute cybersecurity work;
- Improves communication among organizations to help identify, recruit, and develop cyber talent;
- Enables employers to standardize professional development, certifications, and training;
- Facilitates a more consistent, comparable, and repeatable approach to select and specify cybersecurity work roles for positions within organizations;
- Provides a stable yet flexible catalog of tasks, knowledge, skills and abilities for each cybersecurity work role to meet both the current and future needs based on changing threats, requirements, and technologies; and
- Enables academic institutions to align curricula to the Workforce Framework and teach the knowledge necessary for students to effectively join the cybersecurity workforce.

The Working Group 7 membership unanimously agreed that the NCWF is applicable to the Communications Sector. We then focused on the data elements in the NCWF to develop a sector specific dataset that would form the initial baseline for describing cybersecurity work.

5.1.2 Identify Gaps and Improvements in the NCWF

The majority of KSAs were found to be common across industry sectors. There were less than a half dozen KSAs that were deemed not applicable to the Communications Sector from the initial working data set developed for the financial sector by the CWA. Almost all of the KSAs reviewed by WG7 participants were common across their specific representative segment. We did find that Public Safety environment and Radio/Telecommunications technology specific KSAs were lacking in the initial data set reviewed and these were added by WG7.

The level of experience in a specific KSA can vary for roles within an organization. For example, entry level positions can be expected to understand the lexicon and execute routine tasks associated with a KSA under direction of more skilled leadership while Subject Matter Experts are expected to be able to apply KSAs in creative problem solving. As the specific nature of the roles required to staff a cybersecurity workforce vary greatly depending on the needs of the segment participants, this becomes a specific application of the dataset and is considered beyond the scope of the initial research conducted by this working group.

5.2 Findings Informed by Identification of Best Practices

As noted earlier in the methodology section, the Working Group gathered data from a diverse set of segments directly and indirectly related to the Communications Industry. The methods used for information gathering included interviews, data searches, presentations from Subject Matter Experts, review of internal business practices and workforce development programs, and

active participation in multiple organizations both public and private involved in addressing the cybersecurity workforce development challenge. Throughout this section on Findings, there are multiple referenced materials included in the Appendices to this document intended to further inform the reader concerning specific programs, tools, and strategies that formed the basis of the Best Practices and Recommendations of this Working Group. The first Subject Matter Expert presentation was provided by Benjamin Scribner of the Department of Homeland Security, National Cybersecurity Education & Awareness Branch (CE&A) and is included in Appendix 5. This presentation provides an excellent overview of the Workforce Development challenge and some of the Best Practices currently being employed by the Federal Government. The following sections describe the findings by each of the six segments the Working Group pursued to develop Recommendations and Best Practices for this final report.

5.3 Communications Industry

A balanced, holistic approach that contemplates investment in programs geared at younger students, cultivating the emerging workforce through curriculum development with colleges and universities, and training or re-training the existing workforce is key to successful workforce development for member organizations in the Communications Industry. The NICCS (National Initiative for Cybersecurity Careers and Studies) articulates four fundamental practices for developing a cybersecurity workforce as depicted in Figure 4 below.

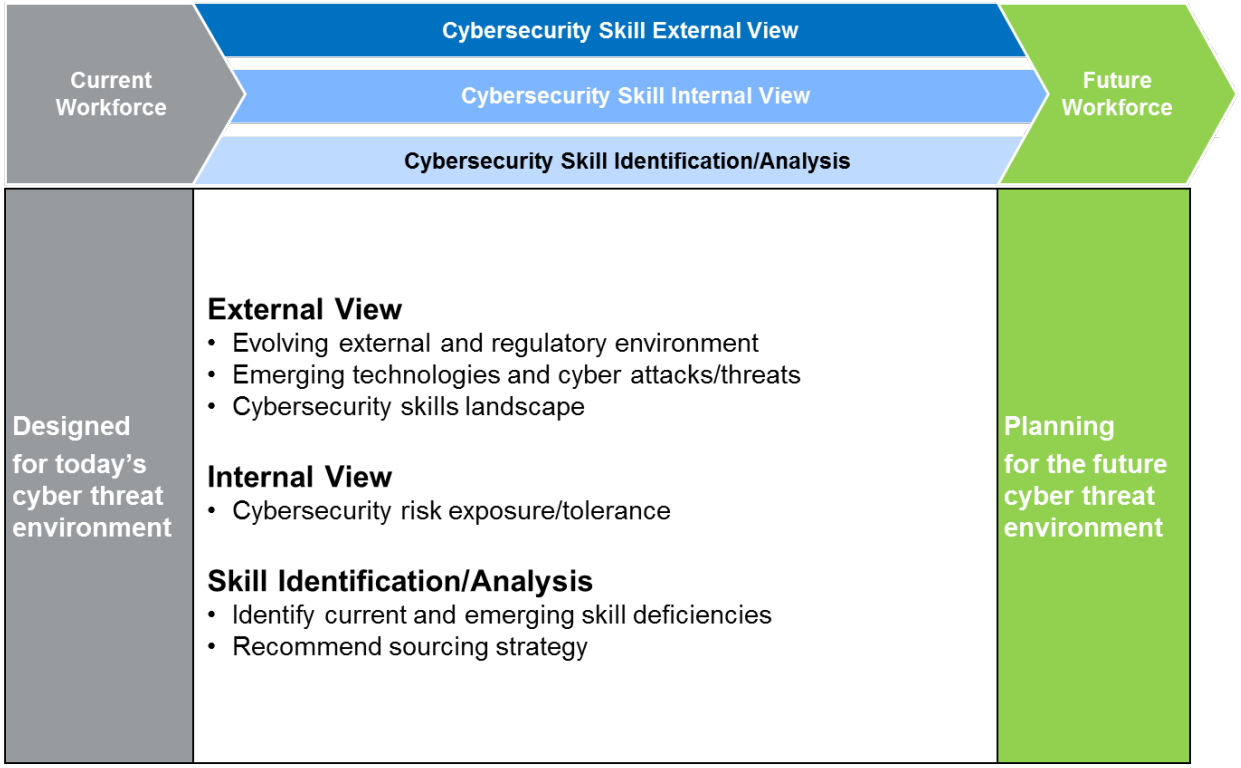


Figure 4 - Foundational Practices for Developing a Cybersecurity Workforce

Although variations did exist, we found that in general these practices are foundational and appear consistently in our findings:

- Understand workforce needs and skills gap;
- Hire the right people for clearly defined roles;
- Enhance employee skills once they enter the organization; and
- Create an environment and implement programs that retain top talent.

5.3.1 Benchmark the Organization

1. Organizational Structure
    a. Perform Gap analysis on organization
    b. Review organizational structure to confirm applicability
    c. Identify key drivers for business and how security needs to align
2. Develop Partnerships with the business
3. Identify Specialty Security Areas
4. Define Emerging Skills and Pivotal Roles - While all roles are important, pivotal roles are identified as roles that have significant impact the strategy and drive a disproportionate value to the organization.
    a. Long to recruit and develop
    b. More expensive to buy
    c. Difficult to retain due to high in demand skills and experiences.
5. Balance Technical versus Soft Skills – Technical skills have been the focus there is an importance for soft skills as well
    a. Business acumen
    b. People management
    c. Communication

5.3.2 Work Model

1. Work Growth – How does work grow and how and by whom is it being performed across the organization
    a. Identify how work grows and determine contribution based on level of worker
    b. Review expected contribution vs actual contribution of employees within a given level (Is work being performed at correct level)
2. Job Levels – Create proper job levels for the work being performed
    a. Utilize all levels for security roles
    b. Indicate specialized roles where only senior levels are used
3. Talent Movement - Pursue diverse talent through various sources
4. Career Management
    a. Create sustainable talent development strategy
    b. Re-think or build strategy for hires
    c. Create hybrid roles

d. Flexible work arrangements
e. Provide clarity on career paths

5.3.3 Examples of Currently Active Programs

Industry leaders have identified several programs they have put in place designed to find the best and the brightest minds in diverse fields of study to include security.

1. Campus to Career
    a. Internships and Co-ops
    b. Entry-level
    c. Leadership Development Programs
    d. Partnerships
2. Collaborate with learning institutions to create custom designed training /certificate programs that strengthen the workforce and build shareholder value.
3. Conferences and career fairs
4. Established solid relationships with certain universities for recruiting new graduates. We continue to explore new programs dedicated to cybersecurity degrees as the programs mature.
5. Recruit STEM degree graduates from universities in specific areas including cybersecurity into internal programs that rotate new hires through several cybersecurity roles in the company over the course of a few years, prior to permanent assignment in a specific role for the longer term. This gives new graduates a better picture over the company's cybersecurity efforts from many angles before deciding on a career path within the company.
6. Fund and support many different programs and events that engage the workforce at younger ages including Girls That Code, hack-a-thons and local programs designed to foster interest in STEM careers generally, and cybersecurity careers specifically in high school students.

5.3.4 Continuing education for workforce

By offering certifications in cybersecurity to existing employees through a partnership program with a college, corporations are able to "retool" the existing workforce. One example program offers a cybersecurity certificate to existing employees following completion of several progressively built courses including:

1. The foundations of cybersecurity
2. Network security
3. Mobile security
4. Emerging threats and defenses
5. Ethical hacking
6. Policy analysis and implementation

Though the development of an internal education program, one industry participant was able to offer many cybersecurity training courses and established a badging program to encourage

employees to develop their skills. They also offer industry standard training and fund industry certification testing through third parties.

1. For example, in 2016 they funded 78 people to take Certified Information Systems Security Professional (CISSP) training and the corresponding certification exam through a 3rd party.
2. They also funded 150 people to take one of three different GIAC training programs and the corresponding Global Information Assurance Certification (GIAC) certification exam through a 3rd party. The training classes they funded lead to the following certifications:
    a. GIAC Information Security Fundamentals (GISF)
    b. GIAC Security Essentials Certification (GSEC)
    c. GIAC Certified Enterprise Defender (GCED)

5.3.5 Combining skilled practitioners to address challenging positions

Data Scientists with security knowledge can be among the more difficult positions to fill. As a solution to this challenge, one company pairs a pure data scientist with a security analyst that will compensate for lack of people who can do both. In order to better fill this need in the future, the following programs were then designed to train and re-train employees in particular fields to broaden their skill into another:

a. A certification in Data Science through an online education resource
b. Online Master of Science in Data Science and Analytics through a university
c. A hybrid Online Master of Science in Data Science through a partnership with a university
d. Development of a nanodegree program in Data Analysis.

5.3.6 List of candidate best practices from Industry Findings

1. Foster an organizational culture that embraces cybersecurity throughout the organization, starting with the tone from the top executives. Cybersecurity professionals are passionate about the work they perform and need to feel connected with an organization that recognizes and values the need for an in-house cybersecurity workforce. (e.g., Cyber Savvy Program)
2. Engage with colleges and universities to support cybersecurity directed research (e.g., IIS UConn program), and internships. Fostering academic relationships strengthens the reputation of industry cybersecurity programs, provides valued intellectual capital and thought leadership, and can be a source for resource/skill gaps.
3. Develop engaging internship roles with clearly defined expectations/deliverables that provide value to the company and the individual. Ensure the intern has the opportunity to explore several cybersecurity functions within IIS, in addition to their internship role. Enabling the intern to appreciate the depth and breadth of the cybersecurity program will assist with recruiting for future interns and permanent roles.
4. Establish well-defined career paths with supporting job requirements and key competencies to support both technical and management roles. This element is critically important for recruiting and retention.

5. Ensure competitive pay aligned with experience. The shortage of cybersecurity resources is driving increased salaries for highly experienced individuals. Aligning to these external forces is critical for recruiting and retaining key roles. Periodic review of pay scales against these market forces is critical for ongoing retention of loyal staff members, whose salary positions tend to erode over time.
6. Foster personal development through conferences, external training, on-the-job or cross training, job shadowing, innovation labs and stretch assignments. Encourage the staff to leverage mentoring programs. Critical for success, ensure development programs are more than adequately funded and supported by the cybersecurity leadership team. Enabling development opportunities, including setting aside sufficient time for the staff to avail themselves is also critically important.
7. Encourage cybersecurity staff to become active industry participants. Cybersecurity, telecom, and cable consortiums provide opportunities for staff members to explore interesting topics, shape public policy, collaborate with peers, work with leading edge vendors, present a conferences and publish articles in trade journals.
8. Push for cybersecurity process automation to keep the staff focused on what's important. A strong cybersecurity culture and personal development won't mean much if the infosec team is constantly focused on mundane manual tasks. Embrace process automation and managed services to free up the security team to focus on high-priority, high-intelligence activities.
9. Recognize key accomplishments for the cybersecurity staff, reinforcing and recognizing the value that each staff member brings to the organization. Encourage shameless self-promotion both internally and externally. Promote participation in industry recognized award programs, such as ISE and SC Awards for team accomplishments.

5.4 Academic Segment

In order to better inform the CSRIC V, the Working Group believes it is valuable to include a discussion of the broader challenge facing academia with respect to cybersecurity education. This section includes a brief discussion of how the University of Washington has begun to approach the cybersecurity gap through development of an innovative curricular model to holistically address the development of future cybersecurity professionals. Their holistic approach endeavors to produce cybersecurity (in their context, Information Assurance) graduates with the requisite problem solving skills and the short amount of time that a University educational program offers.

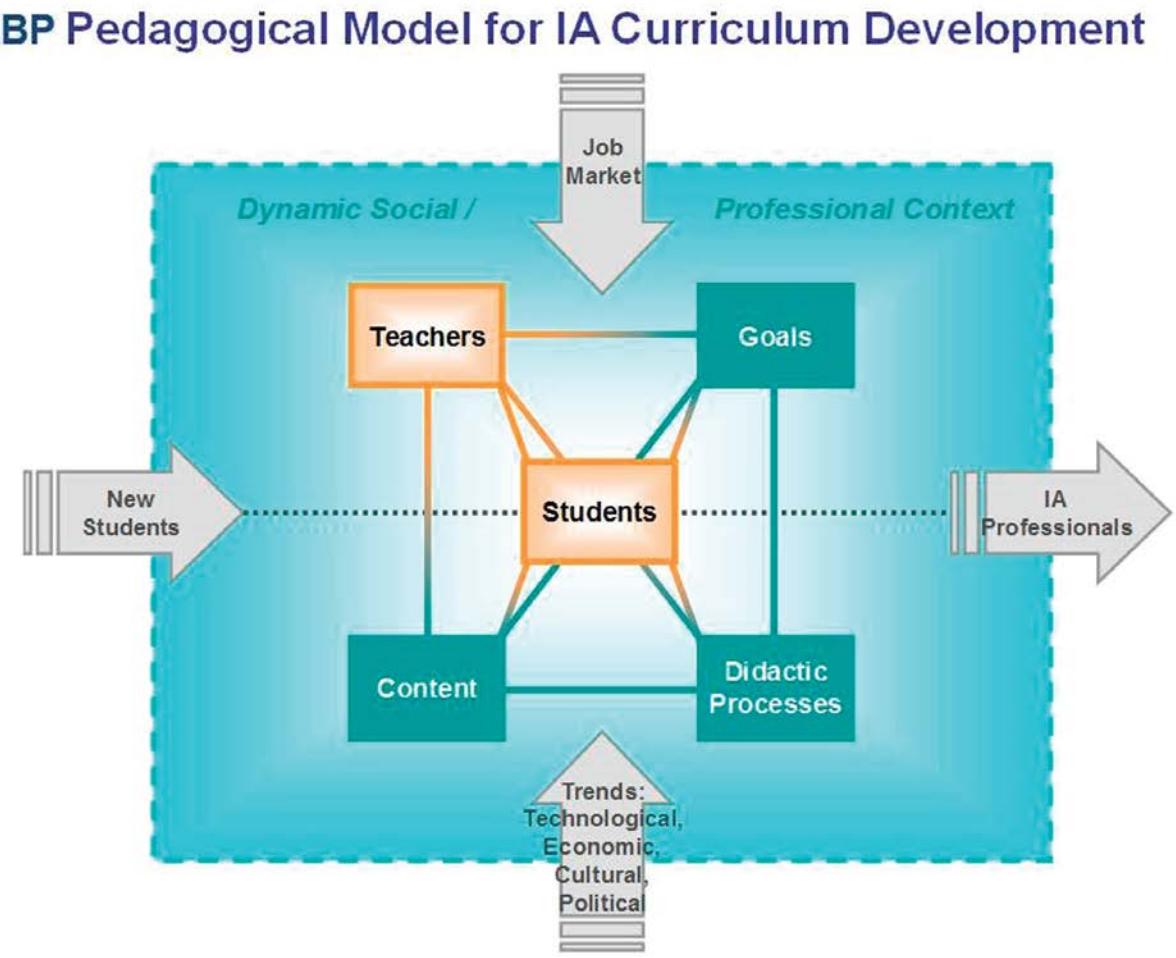


Figure 5: The KBP Pedagogical Model: CIAC as a pedagogical system[28]

> "The KBP [depicted in Figure 5] is composed of five model elements—*students*, *teachers*, *goals*, *content* and *didactic processes*—the first two of which are intelligent elements, the *teacher* and the *student*; the remaining three are infrastructure elements—the *goals*, *content*, and *didactic processes* of the curriculum. All elements of the model are dynamic, subject to varying rates of change and adaptation. All of the elements of the model function as an interconnected whole. They operate within a larger dynamic professional and social context that includes economic and political environments, as well as a constantly evolving set of threats, vulnerabilities and operational systems that are affected by influences such as global competition; technological innovation; legal policies; and the creativity of business leaders, entrepreneurs and IA specialists. This context informs the different elements of the model."

The complete text of the published article is included in Appendix 3, "Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals", Barbara E. Endicott-Popovsky and Viatcheslav M. Popoovsky, ACM Inroads, March 2014.

[28] This operational pedagogical system is derived from intensive research into two schools of thought regarding the theory of pedagogical systems whose originators are Dr. N.V. Kuzmina and Dr. V.P. Bespalko, respectively. The authors named the Kuzmina-Bespalko-Popovsky (KBP) model in acknowledgement of the body of work of these two distinguished academics.

5.4.1 GenCyber Summer Camp Program[29]

The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K-12 level. The goals of the program are to help all students understand correct and safe on-line behavior, increase diversity and interest in cybersecurity and careers in the cybersecurity workforce of the Nation, and improve teaching methods for delivering cybersecurity content in K-12 computer science curricula.

Our vision is for the GenCyber program to be part of the solution to the Nation's shortfall of skilled cybersecurity professionals. Ensuring that enough young people are inspired to direct their talents in this area is critical to the future of our country's national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives.

To ensure a level playing field, GenCyber camps are open to all student and teacher participants at no cost. Funding is provided jointly by the National Security Agency and the National Science Foundation. The GenCyber Program description presented to the Working group by the Chief of the National Information Assurance Education and Training Program (NIETP) is included in Appendix 6.[30] It also includes descriptive information on the National Centers for Academic Excellence Program that follows.

5.4.2 National Centers of Academic Excellence Program[31]

The Department of Homeland Security (DHS) and The National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program, designating specific 2- and 4-year colleges and universities as CAEs in Cyber Defense (CD). Schools are designated based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field. Nearly 200 top colleges and universities across 44 states, the District of Columbia, and the Commonwealth of Puerto Rico are designated CAEs for cyber-related degree programs. CAE graduates help protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors.

Depending on Federal Government funding, next steps planned include studies to identify CAE needs for hands-on education and measurement of student proficiency. The approach will be to have one group looking at metrics and how to gather/report student proficiency relative to education while the other group will look at how to create a virtual environment where schools/students can engage in hands-on learning. The objective is to make that environment universally accessible by the CAE schools initially and then to further expand availability if possible. This study will provide a follow-on opportunity for the CSRIC to participate in the development and enhancement of the CAE program in a manner consistent with the skills and roles needed by the Communications Industry.

[29] https://www.gen-cyber.com/
[30] Building the Cyber Workforce Pipeline: Preparing for Tomorrow and the Day After Tomorrow, GenCyber and the Centers of Academic Excellence in Cybersecurity
[31] https://niccs.us-cert.gov/education/national-centers-academic-excellence-cae

5.4.3 ACM Joint Task Force on Cybersecurity Education[32]

The ACM Joint Task Force on Cybersecurity Education (JTF) was launched in September 2015 with the purpose of developing comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts.

The JTF is a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF grew out of the foundational efforts of the Cyber Education Project (CEP). After a year of community engagement and development work, the ACM JTF launched a survey in September 2016 to solicit broad input on the proposed curricular thought model. This survey was published in October 2016 and is included in Appendix 13, ACM JTF Survey on Cybersecurity Education. General feedback on the thought model provided additional insight for the development process. Summary comments include:

- Clarify the intended audience of the curricular volume
- Clarify the definitions and distinguish between the elements
- Provide additional information on the content of each of the categories
- Simplify the model
- Provide a logical placement for emerging topics

The curricular volume, CSEC 2017, is estimated to be published in December 2017.

5.4.4 University of Washington Center for Information Assurance and Cybersecurity (CIAC) Apprenticeship Program

Cyber operations is a rapidly evolving and expanding field. Failures in cyber operations present industry with operational disruption, financial liabilities, diminishment of brand, and other risks. The University of Washington (UW) Center for Information Assurance and Cybersecurity (CIAC) has discussed industry's needs for professional training and professional development in cybersecurity and is preparing to launch an affiliation with an industry member from the communications sector to improve training programs to meet the industry's immediate needs.

Under this affiliation, the Information Security team from industry will work closely with CIAC to define and pilot training programs and develop the underlying resources that will provide near-term benefits to cybersecurity professionals and students entering this field. The hallmarks of the new programs are:

- Multidisciplinary training. Cyber operations require a technical foundation, but communication skills, risk management, and team participation are equally important. Cyber operations rely on business operations, policies, and systems; and beyond incident response it entails strategic planning, operational planning, effective

[32] http://www.csec2017.org/

communications, and robust auditing. Through this affiliation, students will learn about the real business environment around cyber operations.

- Conforming to federal standards. There are federal standards helping to define the professional field of cybersecurity. Like the field itself, these standards are evolving, and a quality training program must address both industry needs and align with the current federal standards and guidelines.
- Apprenticeship. Students will participate in an apprenticeship program that integrates progressive industry experience with academic course work.
- Cyber lab. High quality simulations of operational environments help fill the gap between academic training and real incident response. Level 1 of this lab provides individual assessment on foundational knowledge, which will be used to assess skills for job candidates. Level 2 (simulated environments) and Level 3 (competitions) will provide valuable resources for ongoing professional development.

By establishing an affiliation which will extend into subsequent years by mutual agreement of both parties, CIAC anticipates evolving the relationship over five or more years. The details below address specific activity for the inaugural year.

5.4.4.1 Apprenticeship program

Students opt into an integrated program of instruction and industry internship that together lasts for at least one year. Through the apprenticeship program, a student receives academic training, certification, and industry experience to accelerate their impact as cybersecurity professionals. The academic program will be offered through the Information Security & Risk Management (ISRM) certificate program. This is a well-established and successful certificate program. The course content will be updated to reflect the new NIST/NIICE knowledge-unit requirements. The National Security Administration (NSA) through its National Information Assurance Education and Training Program will partner in developing this apprenticeship model. The following table provides an overview of the apprenticeship program for 2017:

Affiliate Apprenticeship program 2017		
Quarter	**UWB CIAC contributions**	**Affiliate contributions**
Fall 2016	Recruit students (4 Business, 4 STEM), assess proficiencies, create individual plans for meeting requirements. Establish cohort. Establish assessment and review process for the apprenticeship program.	Participate in selection of students and establishment of cohort. Participate in plan for program assessment and review.
Wtr 2017	ISRM-1: *Business context for cybersecurity.* Fulfilling prerequisites	Hold on-site orientations for students. Host cohort meetings.
Spr 2017	ISRM-2: *Risk management.* Capstone course (for internship) Host cohort meetings	On-site 0.5 FTE internships
Sum 2017	ISRM-3: *Solving problems.* ISRM certification. Capstone course (for internship) Program review and assessment.	On-site 0.5 FTE internships Host cohort meetings Participate in program review and assessment.

For the industry internships, the students may be able to enroll for capstone credits in their respective departments. The capstone course may include poster presentations as part of a final project.

Students will be selected based on a balance of technical foundations, interpersonal skills, team participation, and collaborative problem-solving. Each student will have a quarter in which to fulfill prerequisites, and CIAC will help direct students to free online courses and resources for this. The students will participate in the apprenticeship program as a cohort, to strengthen their team skills and professional networks. The cohort will also serve as a peer group to enhance the students' learning and to provide support around personal, academic, or professional challenges.

As part of the evaluation, CIAC will consider recruiting in Spring/Summer 2017 for the 2017-2018 school year and having the courses run Fall 2017 – Winter 2018 – Spring 2018. If CIAC decides to move the calendar up in subsequent years, the industry on-site internships would run January to June (this first year the internships will run from March to September).

5.4.4.2 Industry Affiliate contributions

For the initial launch of the CIAC Internship Program, UW has identified the following methods and level of contributions from Industry Affiliate:

- 4 FTE (8 x 0.5 FTE) internships with progressive responsibilities, to run from mid-March 2017 through mid-September 2017.
- Leadership participation in selection of students, oversight and review of the program from Affiliate's perspective.
- Team participation in supervising interns and in helping facilitate cohort meetings.
- Tuition for ISRM certificate program for 8 students.

5.4.4.3 CIAC governance

CIAC is developing educational programs for cybersecurity professionals, at the intersection of academic culture, federal standards, and industry needs. To do this well, we need consistent input and feedback from all three sectors, and this input and feedback is more valuable when the representatives from the three sectors are in one collective conversation. In this way, challenges can be addressed and solutions worked out that are responsive to the needs of everyone involved.

The Vice Chancellor of Academic Affairs at UW Bothell and the Executive Director of CIAC will convene an advisory council to advise and comment on CIAC's ongoing progress and plans. The industry affiliate will be invited to participate on this advisory council.

5.4.5 Broadening Advanced Technological Education Connections (BATEC)[33]

BATEC is a National Center of Excellence for Computing and Information Technologies. It is headquartered at the University of Massachusetts in Boston and sponsored by the National Science Foundation ATE Program. Academic partners are leading edge community colleges in

[33] www.batec.org

the cities of Boston (Massachusetts), Chicago (Illinois), Springfield (Ohio), Las Vegas (Nevada), San Francisco (California) and Fort Lauderdale (Florida). The mission of BATEC is to increase both the capacity and the robustness of career-focused pathways in the fields of Computer Science, Information Technology, Computer Networking and Data Analysis. Their primary focus is public post-secondary education (community college and university) in the fields of Computer Science, Information Technology, Computer Networking and Data Analysis. They also work to address workforce development issues at the high school, community college, and university levels through the design and development of programs that build awareness and increase interest in computing and information technology fields of study.

5.4.5.1 Outreach programs[34]

BATEC offers many programs for outreach to achieve their goals. These include sponsoring the placement of students in technical internships designed to be the first step in their career pathway, offering introductory courses at community-based organizations for non-traditional learners, and convening regional stakeholders to discuss common goals, identify resources, document programs and share information on the subject of career pathways. The following examples represent the portfolio of their recent offerings:

- The Technology Internship Program (TIP) is a comprehensive model for placing community college technology students into semester (or summer) long internships with small businesses. In our experience, small business internship demand has been concentrated in web design/social media, help desk technician, and database support. All of the applications, flyers, letters, and surveys, we created for implementing this program are available by request.
- We work in partnership with city-sponsored initiatives to place high school students into paid summer internships. These students are recruited and selected based on their interest in pursuing a career in Information Technology. The Boston-based version of this program works with over 50 companies and places over 130 students annually.
- The Summer Bridge program, an offering of credit courses and non-credit workshops, was enhanced and scaled at Mass Bay Community College. High school students (juniors and seniors) and incoming freshmen are afforded the opportunity to take one of two credit bearing courses, or participate in a set of awareness building workshops that are technology based.
- The Bridge to Community College program caters to nontraditional learners, embedding community college classes in community-based organizations alongside tutoring and social services. Introductory classes in a technical field combined with a general education component act as a ladder to the community college.
- Workforce and economic development are some of the greatest challenges facing urban cities. An emerging strategy for Career and Technical Education is to offer high school students opportunities for transferable credit in introductory courses in Computer Science and Information Technology. BATEC frequently acts as a subject-matter

[34] www.batec.org/outreach/

consultant for such endeavors, providing strategic direction, supplying expertise, and curriculum.

- This program provides an opportunity for university level students to participate in high technology start-up culture. It provides mentoring, workshops and a curriculum of courses designed to prepare students for a career in the start-up economy. Piloted at the University of Massachusetts, more than 120 students have been placed in over 40 of the best start-up companies in the Boston area.
- Many cities have disparate programs targeting workforce development issues. ICT Pathways is a model for bringing together stakeholders from high schools, community-based organizations, community colleges, 4-year institutions, non-profit organizations and local industry to work on a common goal. BATEC developed a network of systematic resources to support retention, degree completion and career readiness for students and job seekers in computing fields.
- Students engage in a viral video challenge to best convey their passion for technology and the benefits of a career involving computers through short videos. "LoveTech" stars community college students and faculty.

5.4.5.2 Cybersecurity Workforce Development Report

While not singularly focused on cybersecurity, BATEC released a report in January of 2016 in partnership with Burning Glass that "analyzes the dimensions of the career pathway (number of jobs, average compensation, and geographic distribution of jobs) and the requirements of the employment opportunity (job responsibilities, technical and soft skill proficiencies" with the aim of accelerating "…the development of dynamic, innovative academic programs and a pipeline of workforce talent that support the industry needs for trained professionals."

The top ten findings from the cybersecurity workforce report[35] are presented below:

1. The field of cybersecurity is pervasive. Cyber-related skills are finding their way into every job in Information Technology, Digital Networking, and Computer Programming.
2. The cybersecurity job landscape is large and growing, and offers strong employment opportunities across the economy. There were 238,158 online job postings, in 2014, for cybersecurity job postings in the United States. This represents a 91% increase in the four year period 2010 to 2014.
3. Cybersecurity job postings remain open longer (8% longer than IT jobs overall) suggesting that these jobs are harder to fill than IT jobs in general.
4. Cybersecurity jobs pay well. The average advertised salary for these jobs is almost $84,000 – well above the average for all IT roles.
5. Cybersecurity jobs break into seven key broad categories (listed in order of employer demand): Engineers, Managers, Analysts, Specialists, Architects, Auditors, and Consultants.
6. The strongest growth in job postings is for the entry level roles of Specialist, Analyst and Auditor. These positions work in operations and defend information resources on a day-by-day basis.

[35] CyberSecurity: Defending our Information Assets, January 2016

7. Workforce opportunities in cybersecurity exist for job seekers of all educational levels. Candidates, with appropriate skills but not a bachelor's degree, can enter the workforce in the Specialist category where 37% of the positions do not require a four-year degree. A career in cybersecurity does, however, require a commitment to continued education as the majority of positions require a Bachelor's Degree and many high paying positions require a Master's Degree.
8. The career pathway in cybersecurity has reasonable definition. The job categories of Specialist and Analyst provide entry level opportunities for candidates with modest skills. The job category of Engineer provides economic incentive for continued educational achievement and skill development. The job categories of Manager, Architect and/or Consultant are the highest paying opportunities and require advanced training, experience, and/or certification.
9. There is a career transition opportunity for returning veterans. Many corporate cybersecurity roles require similar competencies to those required in the military, and require security clearances which veterans either have in their possession or have experience qualifying for.
10. The workforce challenge can be best addressed when employers, educators, and policymakers work together in close collaboration. A shared vision and mutual understanding of the requisite skills, academic credentials and industry certifications required of a qualified candidate can empower educators to properly prepare an entry level workforce.

The full report is included in Attachment 7 and presents a data driven analysis of the employment opportunities across the cybersecurity workforce. It documents workforce needs and includes a mapping of academic skills into a specific set of job roles and career pathways.

5.4.6 George Washington University CyberBlue Program Proposal

We currently face massive cybersecurity workforce shortages worldwide, lacking people who think critically, recognize patterns, efficiently analyze data, discard preconceptions, and focus deeply. Many autistic adults possess these exact cognitive abilities, but employers are aware of only their social disabilities, creating a workforce mismatch that exacerbates security threats and perpetuates disenfranchisement of persons with social disabilities. Over 70 million people worldwide are living with autism and the dramatic upswell of autistic adults will exceed 3 million in the U.S. alone by 2020. At the George Washington University (GW), researchers are proposing an innovative approach: "CyberBlue"[36]—a bold, scalable solution that uses one social challenge to solve another. The GW-led initiative is a collaboration between the I3P[37] and GW's Autism and Neurological Disorders Institute. GW's team of experts aims to prepare a new generation of autistic adults to be "cyber warriors" and launch new workforce initiatives to strengthen systems, transform lives, and change global thinking about populations with disabilities.

[36] Video introduction: https://youtu.be/oJhzM4ttW-E

[37] I3P members involved include: MITRE, SRI, JHU APL, University of California Davis, Dartmouth

5.4.7 List of candidate best practices from Academic Findings

1. The Federal Government (DHS and NSA partnership) next iteration study will provide a follow-on opportunity for the CSRIC to participate in the development and enhancement of the Centers for Academic Excellence (CAE) program in a manner consistent with the skills and roles needed by the Communications Industry. Proposed Best Practice is to engage in the next iteration of the CAE public-private partnership workforce development program that integrates educators and government to address the gap and include the specific needs of the communications industry.
2. There is not only a lack of a skilled cyber security Workforce, but even worse there is a lack of subject matter experts that are available to provide training. Proposed Best Practice is to engage industry representatives to provide subject matter experts to the Academic community to provide skilled resources for teaching courses or augmenting instruction with lectures specific to industry needs and experience.
3. Successful programs have been developed to encourage early development of the skills necessary in science, technology, engineering and mathematics (STEM) such as GenCyber, the BATEC Summer Bridge program, cybersecurity competitions and internship programs that engage K-12 students. These programs would benefit and expand with active Communications Industry involvement and support.

5.5 Public Safety

For over 40 years, the 911 infrastructure was changed little from its initial deployment in the 1960s. During that time, communications capabilities, information processing and advances in data sharing have revolutionized the way we interact, capture information and apply it to our everyday lives. In order to revolutionize the capabilities of the modern PSAP, the emergency services community including both public and private sector, developed an Internet Protocol standards based architecture dubbed Next Generation 911 (NG-911). This new technology is bringing about significant operational and technological changes. As next-generation applications, services and infrastructure are deployed, PSAPs will have to make sense of voice, video, text, and digital data that are converging on them simultaneously. From a 911 call-taker's point of view, PSAP managers need to think about how such information is going to be received and processed, and what type of interfaces will be used for this task. There is an increasing need to understand that in the future, the transition from a private community to a connected PSAP will result in a dramatic increase in system vulnerabilities to cyberattack. Public Safety organizations such as NENA and APCO are actively involved in reaching out to the emergency services community to foster better understanding of these new and emerging threats and to encourage the adoption of a program of education to become better prepared.[38]

The distributed (or local) nature of PSAPs and their corresponding workforce results in a unique geographical challenge for development of skilled workforce to support cybersecurity operations in support of the Public Safety mission. The diversity of implementation options for NG-911 under consideration (Multi-State, State, Regional, Local) call attention to the fact that implementation and sustainment of cybersecurity for the local jurisdiction will be more costly and difficult to execute. Reported numbers vary, but according to NENA as of August 2016, the

[38] Cybersecurity & the PSAP, Protecting Against Malicious Cyber Activity by Jay English, March 2014, https://www.apcointl.org/doc/training-certification-1/481-cde-36485-cybersecurity-and-the-psap/file.html

United States has 5,893 primary and secondary PSAPs in 3,135 counties. This presents a very specific Public Safety challenge when it comes to locally staffing PSAPs to address cybersecurity needs. The distribution of academic institutions qualified to provide training in cybersecurity for the widely distributed Public Safety telecommunicator workforce is not adequate to address the local need. So, in addition to understanding the specific requirements for Public Safety cyber security Workforce development, there is a need to deliver this training broadly in a consistent manner and subject to the rigors of academic excellence needed to ensure consistent performance across the entire workforce.

The first step in workforce planning, Define and Identify, emphasizes the collection of workforce data that defines the workforce and the identification of positions/roles within the workforce with specific role based competencies and proficiency levels. This activity in turn establishes the knowledge, skills, and abilities (KSAs) that are the attributes required to perform a job and are generally demonstrated through qualifying experience, education, or training.

As a prescriptive example to Define and Identify Workforce, the working group members reviewed job titles, roles and skills to assess NICE Framework labor categories, scope of work, and information technology skills most closely associated with each. While PSAPs generally do not have a single consistent model for job titles, a generalized set of job titles were mapped to labor categories with identification of required skills and recommended training based on the NICE Workforce Framework. The results compiled by Working Group 1 - Cybersecurity under the FCC Task Force on Optimal PSAP Architecture program[39] are presented in the Table below as a baseline example of application of the Workforce Framework to Public Safety.

[39] https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_FINALReport_012916.pdf

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
Director/Administrator	Oversight and Development	Administer the telecommunications and Emergency Medical Dispatch functions of the Bureau of Emergency communications thru planning both short and long term goals. Analyze and develop staffing plans based on historical data in order to revise or develop operational policies and procedures.	Operates computers and AV equipment as needed.	Cyber Hygiene Cyber Security for Managers
Deputy Director, Operations Manager, Technical Manager, Radio Systems Manager	Oversight and Development	Direct support to the Director/Administrator in the management of the telecommunications and Emergency Medical Dispatch functions of the Bureau of Emergency communications thru planning both short and long term goals. Analyze and develop staffing plans based on historical data in order to revise or develop operational policies and procedures. Dependent on organization of the department/agency, deputy directors may have specific responsibilities involving one or more of operations, technology, training, radio networks and systems, quality assurance.	Operates computers and AV equipment as needed. Additional system specific IT skills driven by organizational responsibility that would define specific scope of additional recommended training.	Cyber Hygiene Cyber Security for Managers - Network + - Security + - IR Framework - CISSP
Administrative Assistant	Administrative support	Under the supervision of the Director, performs a variety of administrative support tasks and reviews and processes warrants. Drafts and types various correspondence, maintains accounting records, gathers data and prepares reports. Attends meetings and takes minutes.	Operates computers and AV equipment as needed.	Cyber Hygiene
Case Review & Evaluation Specialist/Quality Assurance Manager	Oversight and Development	Provides assistance to the Emergency Medical Service (EMS) Medial Control Board in determining if correct protocol was used in handling of medical calls, respond to complainants, and to serve as a liaison between the Medical Control Board, the Bureau of Emergency Communication and all public safety emergency agencies.	Operates computers and AV equipment as needed.	Cyber Hygiene Cyber Security for Managers
Data Processing Supervisor, MSAG Coordinator /Location Services Administrator, Field Representative	Oversight and Development	Summarize the collection and verification of location data and make recommendations for inclusion in the E911 and NG-911 transition of telephone and GIS databases. Checks and monitors accuracy of GIS data collected in the field. Performs data comparisons to sync telephone and GIS databases. Accomplish and maintain a mapping database to be used for emergency response directions.	Operates computers and AV equipment as needed. Uses database management systems. Monitors calls for addressing accuracy and initiates reports of incorrect information to assure database update	Cyber Hygiene Cyber Security for Managers - Security +

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
Public Safety Answering Point Supervisor	Oversight and Development	Supervises subordinate field representative employees (dispatchers, call takers, and/or telecommunicators; see below) in the daily operations of their sections to achieve agency objectives. Responsible for understanding the technologies and workflows for the data operations support section.	Operates computerized the phone system for E911, NG911. Operation of TTY/TDD Operation of Text 911 systems Monitors 911 data to get real-time information about emerging threats.	Cyber Hygiene Cyber Security for Managers
Police, Fire, EMS Dispatcher / 911 Call Taker / Public Safety Telecommunicator	Operate and Maintain	Operate emergency telecommunications computerized console system, to receive, assess, make judgment, and forward to appropriate emergency service providers emergency requests for police, fire or medical assistance. Provide life sustaining instructions for medical patients until the arrival of responding medical personnel. Follows strict Division, state, and national standards and policies.	Operates computerized the phone system for E911, NG911. Operation of TTY/TDD Operation of Text 911 systems Monitors 911 data to get real-time information about emerging threats.	Cyber Hygiene Cyber Security for Managers
Public Information Representative	Operate and Maintain	Create and Maintain a media campaign to educate the public about E-9-1-1	Operates computers and AV equipment as needed.	Cyber Hygiene
Training Coordinator	Oversight and Development	Plan, develop, and monitor training programs in a variety of Emergency communications related classes in order to maintain an enhanced service to the public. Review supervisors and Telecommunications Specialists work performance, perform annual evaluations on supervisory and training staff and make recommendations for salary increases.	Training programs for PSAP staff to maintain proficiency and ensure conformance to standards maintains employee training records for certification and performance Administers in-house testing and leads interview panel for selected applicants	Cyber Hygiene Cyber Security for Managers

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
GIS Administrator	Operate and Maintain	Manages GIS objectives by authorizing and directing implementation of policies and procedures to meet long term strategies. Analyzes, develops, and approves applications for grant funds to support new GIS tech. Develops and manages GIS projects as assigned.	Authorizes the development of statewide advanced GIS policies, goals and objectives Monitors operational activities for efficient and effective allocation of resouces. Manages personnel in the Special Operations section Coordinates interagency GIS data transfer and maintenance Manages the design, development, and maintenance of custom software for DESC special operations	Cyber Hygiene - Security +
GIS Technicians/ Cartographers	Operate and Maintain	Performs public safety and ER mapping activities utilizing geospatial tools and equipment to support division.	Develops and maintains GIS components Provides data management for GIS components Recommends policies and procedures Supervises and trains employees in the use of various GIS systems Utilizes a variety of databases	Cyber Hygiene - Security +
IT Manager/Director	Oversight and Development	Administers all aspects of agency-wide technology solutions in support of the agencies core and ancillary functions under the direction of Division Director. Senior IT manager for the Technical Support Unit. Manages all aspects of agency data operations including 911 Telephone Database, 911 GIS Database, and implemention of NG911 and the ENS.	Authorizes Policies and Procedures for design and administaration of Databases. Plans and Evaluates E911 HW & SW solutions. Evaluates trends in communications. Makes recommendations on HW&SW Directs assigned managers and supervisors to coordinate team resources. Evaluates IT & IP communications to ensure productivity of assigned resources	Cyber Hygiene Cyber Security for Managers - Network + - Security + - IR Framework - CISSP

PSAP job titles:	Category	Scope of Work	Required Skills (IT Related)	Example Training
Network Administrator	Operate and Maintain	Network and computer systems administrators are responsible for the day-to-day operation of voice and data networks. They organize, install, and support an organization's computer systems, including local area networks (LANs), wide area networks (WANs), network segments, intranets, and other data communication systems.	Network and computer system operating systems, router configurations, IP and other communications protocol stacks, access control systems, network encryption (VPN, SSL, etc.), network monitoring	Cyber Hygiene - Network + - Security + - IR Framework - CISSP
PC Technician, Systems Technician, Network Technician, Radio Technician	Operate and Maintain	They install, configure and maintain the hardware and software that comprise voice and data communications networks. May be responsible for network components, client workstations, servers, domain controllers, shared printers, cables, and routers, radio system controllers, RF network components, cable and fiber systems and other related communications systems. They maintain network equipment, applications, data and user interfaces and workstations as well as troubleshoot local and wide area networks.	Computer system hardware and software configuration, maintenance, and troubleshooting, Land Mobile Radio equipment configuration, maintenance and troubleshooting	Cyber Hygiene - Network + - Security + - IR Framework
Database Administrator	Operate and Maintain	Responsible for the performance and security of databases. The role includes the development and design of database strategies, system monitoring and improving database performance and capacity. They may also plan, co-ordinate and implement security measures to safeguard the database	Computer system hardware and software configuration, maintenance, and troubleshooting. Specific skills focus on database architecture, application development, system backup and recovery, and database performance indexing.	Cyber Hygiene - Security +
Senior Technical Coordinator	Operate and Maintain	Designs, plans, and implements agency wide technology solutions in support of the agency functions under the direction of the IT manager. Interfaces with vendors IT resources to develop plan and implement installations and upgrades. Serves as a technical resource for junior staff and conducts in-house training.	Computer system hardware and software, network hardware and software, IP and other protocol stacks, system and network monitoring and performance management	Cyber Hygiene - Network + - Security + - IR Framework - CISSP
Technical Support Specialist	Operate and Maintain	Maintain current and future information technology systems, evaluate and develop system procedures, resolve system problems and assist in the development of training for users in a computer environment.	backup and restore - COOP plan Implements agency use and security policies and reviews for compliance monitors, projects, and analyzes network performance Coordinates with IT staff to troubleshoot, enable, or limit WAN/LAN connectivity	Cyber Hygiene - Network + - Security + - IR Framework

Table 2 - NICE Framework mapping for Public Safety

5.5.1 Candidate Best Practice for Public Safety

Based on our analysis of the data provided and the unique challenges facing Public Safety both in terms of the geographic reach required and the nature of the training needed, the WG7 members propose consideration of a distance learning initiative for delivery of the cybersecurity curriculum that can initially support basic cybersecurity hygiene and eventually expand into a broader course list addressing awareness and basic/entry level skills in cybersecurity for small and rural PSAPs. By offering this program in partnership with local schools, universities and/or community colleges, this could become a "lightening rod" for expanding basic literacy in cybersecurity and potentially lead to expansion of skills required for higher paying jobs/careers where the opportunity currently does not exist. This could help develop new workforce sourcing opportunities in the rust belt or rural areas to cross the digital divide.

5.6 Financial Sector

This summary of findings from the Financial Sector is based on the Cybersecurity Workforce Alliance (CWA), which co-chairs the NICE Framework Working Group for Private Sector (WGPS),40 and informed by the iQ4 Workforce Supply-Chain platform aimed at improving the workforce development process through automation in cybersecurity. The CWA was formed in January 2015 with the support of SIFMA (Securities Industry and Financial Markets Association), which represents hundreds of securities firms, banks and asset managers. Founding members in addition to SIFMA included iQ4 and 12 Wall St and Healthcare CISOs, Federal Reserve Bank NY and The John Jay School for Criminal Justice at City University NY. By word of mouth and reputation, there are now over 320 individual members, 120 employers, over 120 current CWA Alumni graduates (with 108 in the Fall 2016 Semester). The CWA has developed and matured a scalable education-to-industry engagement and accelerated supply chain model, which has proven to be very successful by accelerating the training of the student and professional cybersecurity/risk workforce by 6-9 months, making them productive and less risk to the employer with an approximate 40:1 ROI.41

The CWA has been working with the CSRIC V WG7 and to date completed the NICE Framework adoption stage of our alliance, adding 161 new KSAs to support the Communication Sector specific needs identified in the Interim Deliverable from Working Group 7 produced in March 2016. The next phase will leverage this work to define a Role Profile version, more in line with industry adoption of the NCWF. The CWA and JPMChase co-chair the NICE WGPS, and together with member companies from WG7, are working to identify critical roles and competencies that members can leverage in supporting infrastructure and compliance requirements. Role profiles will begin with skills, then tasks and objectives supported by a maturity assessment model, analytics, and development planning tools. The US Navy, JPMC and others have contributed to the mapping of the taxonomy to Job Roles and to Professional certificates. This helps map the right people to roles and ensure that money is not wasted on professional development/certificates when the candidate's competency is assessed as not having the pre-requisite skills for a given level for a course. As the taxonomy and model can be used for next generation outreach and internally for Workforce Supply Chain, it follows that Communication Industry participants can achieve the following benefits from the work of the CWA by supporting continued improvement:

---

[40] http://csrc.nist.gov/nice/nicewg/index.html

[41] ROI calculation is included in Appendix 11, "How to Generate a 4,100% ROI without Breaking a Sweat"

1. Profiling employees, contractors, interns and students in an engaging way for individuals to capture and update their education, experience, certificates, personal highlights and skills in a profile "Passport";
2. Automatically matching the skills-for the-job to the people with the right skills based on their "Passport";
3. Workforce visibility into critical roles, staffing, skills proficiencies, assessments and development, at the business unit and enterprise levels to expose organizational security or compliance risks;
4. Optimizing on-boarding of current and new talent by instantly finding the specific expertise required by each team member/role;
5. Ensuring a "good-fit" hire is made (as a bad hire costs 6x of that of a good hire); and
6. Cutting the time and cost it takes to hire, on-board and train new next generation hires.

Notably, as iQ4 is a co-chair of the NICE Workforce workgroup and is a representing member of the CSRIC WG 7, they are currently serving to sustain and communicate the taxonomy delivery to all users, after NICE has approved any updates.

5.6.1 CWA recommended best practices for implementing the framework into an organization

Each organization should have a workforce roles champion with the contextual knowledge of the sector and the ability to adapt the taxonomy to the roles required by the sector or employer. Leveraging an automated tool to manage the roles and taxonomy databases can greatly simplify the process. Tools, such as the iQ4 platform, provide automated matching engines to find direct and "near-to" candidate fits; to stand up project teams quicker or to identify and upskill people for a more economic internal transfer than hiring externally which positively impacts retention.

CSRIC V WG7 CWA- Financial Services Input									
	Jan-15	Prep and Pilot		Fall 2015		Spring 2016		Fall 2016	
Sector/Bodies Joined	SIMFA		FSSCC	FCC interest		UTC	Federal Reserve Bank Recognition/Support		
Firms Involved	12		28	90	96	101	118	136	160
Members	14		24	32	95	118	155	300	350
Mentors Used			7						12
Student Teams			2		4		9		11
Badged Alumni			18		23		56	Fall graduating	92
Adding Universities with CWA Programs	John Jay C. Crimal Justice, City Uni NY			Uni Business at u-Albany SUNY		CUNY and SUNY		| U Albany Homeland |Hunter | Baruch | Queens | California | Rhode	
Pivot points		iQ4 asked to lead NICE private sector "Workforce" taxonomy		JPMC co-chairs NICE workforce taxonomy	CWA-EMEA	NICE taxonomy mapping to Job Roles and Professional Certifcates		UK-Pilot	New CWA Chapters

Figure 6 - Cybersecurity Workforce Alliance Program Growth

The CWA developed engagement model adoption by industry and education is growing rapidly in the USA with early stage overseas activities in the UK and APAC. Academic transcripts are validated by the National Student Clearinghouse (NSC) and the CWA digitally badges successful Alumni. Collective sponsorship from Operations, GRC, CIO and CISO is valuable. iQ4 provides webinars and guides for the adoption of the platform, adapting the CWA outreach

to universities and the internal use cases. CWA's Alumni are landing great jobs in employers (FBI, NY DA 's Office, PwC, Capgemini, Bank NY Mellon Federal Reserve, Harvard Research, Virtusa Corp., International Securities Exchange) that have never sourced from their schools before. CWA goes beyond the traditional sourced schools to enable employers to cast a wider net and level the playing field to scale the supply of great next generation hires.

Active engagements that members have driven to enhance availability of a skilled cybersecurity workforce are described in the following sections and include:

- **City Uni NY:** Summer 2015, Fall 2015, Spring 2016, Fall 2016
- **u-Albany SUNY:** Fall 2015, Spring 2016, Fall 2016
- **FS Support:** The 12 regional Federal Reserve Banks locations have been offered as locations for CWA semester final presentation to audiences of employers.
- **Cyber 101:** Entry Level Awareness training module released Fall 2016

These programs are described in additional detail in the paragraphs below.

5.6.1.1 City Uni NY: Summer 2015, Fall 2015, Spring 2016, Fall 2016

iQ4 formed the Cybersecurity Workforce Alliance to accelerate student workforce readiness. Together with the Securities Industry and Financial Markets Association (SIFMA) and the Vice Chancellor of the City University of New York (CUNY), we launched an initiative to resolve student readiness, by extending the workforce into the classroom. During the first 2 quarters, the CWA identified the four cornerstones to make this work including; technology, standards based lexicon, industry engagement model and a business case to continue sustainability. The program based on the NICE taxonomy was used to create Role Based profiles and represent the most epic challenges facing country and world today. iQ4 and JPM Chase co-chair the NICE Framework for Private Sector with a focus on adopting the framework, and build industry driven technology, content and models to create a scalable and sustainable model that supports the CISRIC WG7 initiative.

A 6-week pilot with two teams of students (total 17) was run in July and August mentored by CWA industry members. Students were from Law, Forensics, Business, Criminology and IT - none had any previous experience in Cyber or any work experience. At the final presentation at Bank NY Mellon, students were assessed by mentors as "being equal to someone in employment for 12-months"; in terms of poise, confidence, understanding of the NIST framework and which roles pull together to respond to insider and other threats.

As a best practice, the final presentations are at an employer site in front of mentors, employers, academics and interested parties from State Education and Dept. Labor. The employer site helps inspire the students within an employer's workplace environment and develop them through the experience in presenting/communication in the real-world workplace in front of a diverse audience, including a sometimes tough grilling from a few of the mentors. After the sessions, students go to tables organized by the job role that they have played during the course, where they are interviewed and counselled by prospective employers.

John Jay is now expanding the CWA curriculum and model to offer the CWA applied learning across campus (445,000 students) including 15,000 in IT. They applied for and received a grant top "scaffold" the program upstream to associated Community Colleges and Schools to influence STEM based learning using Cyber at the core.

The pilot has now been extended to a 10-14-week production credited curriculum to align with academic teaching. Each semester sees an expansion of the program.

5.6.1.2 u-Albany SUNY: Fall 2015, Spring 2016, Fall 2016

University at Albany, SUNY, adopted the plug-and-play CW model and has been instrumental in helping streamline the engagement process to reduce the time mentors need to apply to the program. Dr. James Stellar, the President, is an enthusiastic supporter of applied learning. He is extending the CWA program from the Business school to across faculty/campus, including the new College of Emergency Preparedness, Homeland Security and Cybersecurity (CEHC), which was formed from funding by NY State Governor Cuomo.

CWA Fall 2016 includes over 80 students in 9 teams on "The Threat Within" being mentored in 3 classes for 1-hour per week. To increase efficient scaling, 80 students work in 9 teams are being mentored in 3 classes by 9 senior industry experts. We recommend 3 mentors per class, as they can share the workload, offer specific/different subject matter expertise and cover for one another when their work takes priority.

U-Albany is taking a State University system lead by collaborating and expanding the program across other Universities.

5.6.1.3 Financial Services Support

The 12 regional Federal Reserve Banks locations have been offered as locations for CWA semester final presentation to audiences of employers.

Senior IT Risk Examiners from the Federal Reserve Bank NY were part of the CWA founding membership because they identified the potential of a near systemic collapse of the banking system if certain organizations were compromised. FRBNY hosted the combined CUNY and SUNY team finals in Fall 2015 and Spring 2016. Based on the successful outcomes, the support has grown to include all 12 FRB locations has focal points for hosting and supporting the CWA. This association will help provide credentials for the CWA to recruit FS firms of all sizes.

5.6.1.4 Cyber 101: Entry Level Awareness training module released Fall 2016

"Awareness" was a word raised by all founding members. It carries a number of meanings but, in summary, all members want:

- All new employees to enter the workplace with some level of cybersecurity "awareness" - from risks to good personal/employee practices to mitigate the risk. Thus avoid the

impacts from lack of knowledge later.

- Students to be aware of their brands and the career offering they have in Cyber and GRC.
- Awareness that all industry sectors offer great, well paid, careers that are likely to last a lifetime

This is an extremely helpful 3-week self-paced lead into the program as it sets out the challenge landscape and the NIST framework to respond to it, as well as the roles that the students will elect to role-play in their teams through the balance of the course they are taking.

5.6.1.5 101 variants

1. A high-level, scalable general awareness program is under development with results being measured/recoded for trackable evidence of measured completion.
2. Based on the CUNY and SUNY experience focused on perfecting the CWA model, it was clear that a deeper 101 program was important as a precursor to entering the CWA Epic Challenges. This was designed by CWA mentor/members as part of "Project Scale" where CWA member voluntarily helped design the expansion plan, map roles from the NICE taxonomy and plan for IoT, Mobility, Autonomous Vehicles and "The Soft War" Anti-terrorism modules.

5.6.2 Cross sector workforce development industry association

With other sectors adopting the CWA approach, the members of the Communications Industry do not have to invest heavily to get the same benefits. Importantly, Communications Sector industries can therefore progressively benefit from a standardized cross sector association of CWA Alliances, all pulling in the same standards-based direction.

iQ4 has made its platform tooling and engagement model and the automated NICE taxonomy available to the Communications Sector members. By adopting the plug and play model and the taxonomy, with CSRIC extensions in Specialties and KSAs, the industry members can take immediate advantage of a proven model and create a communications industry specific program that supports the cross sector transportability of skills. As in the Financial Services sector specific model (FS-CWA), a cohort of lead members from industry is required as volunteers to review and update evolving taxonomy.

5.6.3 Keeping the Communications Industry up to date with CWA Activities

1. Frank Cicio of iQ4/CWA is co-opted on the CSRIC V WG7 and can assist in establishing direct and open communications with CWA.
2. Industry members can join the CWA as an observer on the platform.
3. The CWA holds a monthly update conference call on the third Wednesday of each month. All interested parties are invited. Contact frank@iQ4.com
4. NICE runs monthly sessions for the Workforce workgroup with monthly webinars and update reports http://csrc.nist.gov/nice/nicewg/index.html

5.6.4 Use of an Automation Tool to keep up to date with NICE Taxonomy

The CWA was formed to support workforce development through industry led initiatives including: NICE Framework adoption; epic challenge projects that extend the workplace into the classroom; and industry virtual mentorship models. iQ4's Workforce Supply Chain platform, was built to address the missing automation needed to identify workforce risk, optimize resources, develop and track talent, skill progression and performance. By leveraging the iQ4 platform, the CWA has automated the NICE taxonomy in ways that support the NIST-CA Framework. iQ4 makes the NICE-based 4-tier taxonomy (Job Roles, Specialty Areas, Competencies and KSAs - Knowledge, Skill and Abilities), available as controlled Open Source to CWA members. The FCC is currently a CWA member.

5.6.5 List of candidate best practices from Financial Sector Findings

1. CWA records the outcomes and tracks the CWA Alumni progress into jobs. Their Profile/Passports remain on the iQ4 Workforce Supply Chain Platform to be found/matched by employers seeking candidates by role/taxonomy and they are invited to the exclusive invitation only CWA Alumni Group on LinkedIn.
2. To increase efficient scaling, 80 students work in 9 teams are being mentored in 3 classes by 9 senior industry experts. We recommend 3 mentors per class, as they can share the workload, offer specific/different subject matter expertise and cover for one another when their work takes priority.
3. The final presentations are at an employer site in front of mentors, employers, academics and interested parties from State Education and Dept. Labor. The employer site helps inspire the students within an employer's workplace environment and develop them through the experience in presenting/communication in the real-world workplace in front of a diverse audience, including a "sometimes tough" grilling from a few of the mentors. After the sessions, students go to tables organized by the job role that they have played during the course, where they are interviewed and counselled by prospective employers.

5.7 Federal Sector

5.7.1 DoD Leads Migration from Certificate Based Training to KSA Focused Metrics and the NCWF

DoD 8570 was published in 2005 to address concerns associated with having unqualified personnel performing critical cyber security functions. The directive required personnel that had access to information systems and performed specific security functions to receive and certify on specific training to show competency in the job field. This raised the standard of the DoD and industry as well as military and civilian components followed the standard.

In 2015 DoD 8140 was published to reissue and renumber 8570 and to update and expand policies and responsibilities for managing DoD cyberspace workforce. As part of this updated guidance, emphasis has been placed on the establishment and effective measure of cybersecurity

training programs. Cyber security work role requirements must be integrated into training, courses, and curriculum.

Work role (knowledge, skills, and abilities), baseline qualifications, and training requirements derived in 8140 will emphasize job skills and experience over rote certifications. 8140 also provides alignment to the NIST Cybersecuirty Framework as shown below in mapping of job roles to the framework function areas.

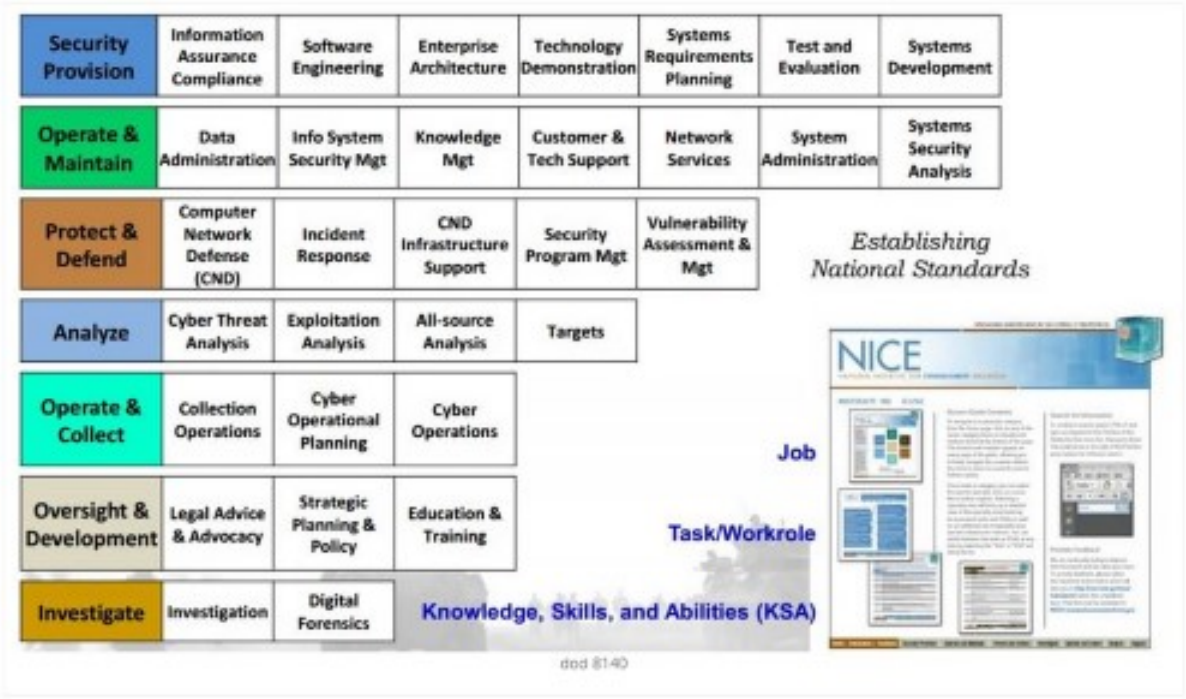


Figure 7 – 8570 Mapping to NIST Cybersecurity Framework

In addressing this shift, vendors and those that are supplying training to the DoD need to adjust the method and mechanism of the training provided to meet 8140 guidance. To address this shift a few best practices were presented:

- Hands on training in realistic simulated environments
- Performance based assessment in simulated live fire environments
- Methods to measure true knowledge skills and abilities of the individual
- Proficiency verification – tools for measuring student (KSAs)

As part of the Working Group information gathering, Erik Wallace of Comtech Telecommunications Corporation provided the presentation included in Appendix 8 to inform the members on the DoD timeline and process for cybersecurity training to include the transition from a certification driven process to the current KSA metrics driven standard.

5.7.2 Research Paper – "Closing the Federal Talent Gap"

There is a nationwide shortage of highly qualified cybersecurity experts, and the federal government in particular has fallen behind in the race for this talent—individuals who are

essential to protecting our nation's critical public and private information technology infrastructure. Federal agencies were having a difficult time recruiting, hiring, retaining and properly training skilled workers in the cybersecurity field. The government did not even know the size and competencies of the workforce let alone what would be needed in the future, and it had no plan to address this problem.

During the past five years, the federal government has taken some positive steps, but the same basic problems have grown more acute as the threat has multiplied. In short, the government still lacks the cyber workforce it needs and still does not have a comprehensive, enterprise-wide strategy to recruit and retain that workforce.

Federal agencies are left to fend for themselves in the hypercompetitive market for top cyber talent. Some agencies—like the NSA and FBI—fare better than others, partly because of their mission and partly because they have more personnel flexibilities than their sister agencies. That agency-centric, "have versus have-not" approach has resulted in a federal cyber workforce that in 2015 is uneven at best, especially when compared with top-tier private sector organizations.

Our interconnected world requires a seamless team of cyber defenders to protect our networks. Those defenders must be able to operate quickly and collaboratively in ways that cut across both private and public organizations. The cyber talent crisis has persisted long enough. Our Nation is at risk as the number and sophistication of cyber-attacks continue to grow, but the government has failed to act with urgency.

Many of the personnel issues confronting the cybersecurity workforce are endemic in the federal system that makes recruiting and retaining the best and brightest talent in any career field a formidable challenge.

It has been argued that the best way to deal with this government-wide challenge is to reform the entire civil service system through market sensitive, performance-based pay that accounts for occupational differences; a new, modern job classification system; expectations and rewards for excellence; more flexibility to hire talented candidates and hold them accountable; and a new enterprise-focused leadership structure that engages its employees, all without comprising the core principles that have always anchored our civil service.

While such a government-wide overhaul may take time, cybersecurity is one area that simply cannot wait. The current federal personnel system is more than 60 years old, created decades before the Internet was a reality. With our national and economic security at stake, the cyber workforce is an ideal place to launch a comprehensive strategy that will address current and future cybersecurity workforce needs.

5.7.3 Federal Cybersecurity Workforce Strategy

Federal departments and agencies face increasingly sophisticated and persistent cyber threats that pose strategic, economic, and security challenges to our Nation. These cyber threats demonstrate the need to employ the Federal civilian cybersecurity workforce with the necessary knowledge, skills, and abilities to use those tools to enhance the security of the Federal digital infrastructure and improve the ability to detect and respond to cyber incidents when they occur. However, there simply is not a sufficient supply of cybersecurity talent to meet the increasing

demand of the Federal Government. It is projected that this shortfall will expand rapidly over the coming years unless companies and the Federal Government act to expand the cybersecurity workforce to meet the increasing demand for talent.

The Federal Cybersecurity Workforce Strategy[42] details government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats. The Strategy anticipates that the Government will see the return on its investment through enhancements to Federal cybersecurity and the improved knowledge, skills, and abilities incoming cybersecurity talent bring to the Federal workforce.

5.7.4 DHS Workforce Development Tookit[43]

To develop a more resilient and capable cyber nation, we must have a highly-skilled cybersecurity workforce across industry and government. The Department of Homeland Security (DHS) is committed to helping organizations build a comprehensive cybersecurity professional capability. DHS has created tools and resources, including the National Cybersecurity Workforce Framework, to help organizations understand and act on their cybersecurity workforce needs.

DHS's workforce development tools and resources help organizations answer questions such as:

- What is the current state of my employee's cyber capabilities?
- What gaps do we need to fill?
- What kinds of cybersecurity workers do we need to hire?
- How can I keep and grow my cybersecurity staff?

Effective cybersecurity workforce development helps organizations more efficiently and effectively recruit qualified cybersecurity professionals, and to provide this critical workforce with clear job descriptions and development opportunities. DHS has a resource to help organizations get – and keep – the right cybersecurity staff: The Cybersecurity Workforce Development Toolkit. The Toolkit will help you understand your organization's cybersecurity workforce and staffing needs, and includes things like templates to create your own cybersecurity career paths, and resources to recruit and retain top cybersecurity talent.

A copy of the DHS Cybersecurity Workforce Development Toolkit is included in Appendix 4.

5.7.5 OPM CyberCorps Scholarship for Service Program[44]

CyberCorps (R): Scholarship For Service (SFS) is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. This program provides scholarships that may fully fund the typical costs incurred by full-time students while attending a participating institution, including

[42] Memorandum for Heads of Executive Departments and Agencies, July 12, 2016; this is included in Appendix 12 to this Working Group 7 Final Report
[43] https://www.dhs.gov/cybersecurity-workforce-development-resources
[44] https://www.sfs.opm.gov/

tuition and education and related fees. Additionally, participants receive stipends of $22,500 for undergraduate students and $34,000 for graduate students. The scholarships are funded through grants awarded by the National Science Foundation.

5.7.6 List of candidate best practices from Federal Government Findings

Cyber security workforce includes both technical and non-technical professionals but it is the responsibility of all agency leadership, employees, contractors, private industry, and American people. The following are the Key findings addressing the insufficient supply of cybersecurity talent.

Identify Cybersecurity Workforce Needs

Cybersecurity workforce needs can be addressed through the Cybersecurity Workforce Framework and through the education of key Federal agency stakeholders, such as Human Resources (HR) and Chief Information Officer (CIO) staff, about and the benefits of the Workforce Framework and associated tools. The framework provides for the expansion of cybersecurity position descriptions and the alignment with cybersecurity vacancies. Work with the private sector to explore trends and anticipate future workforce needs can be performed as a part of Strategic Workforce Planning.

Expand the Cybersecurity Workforce through Education and Training

Expanding the cybersecurity workforce through Education and Training will need long-term investments in nationwide cybersecurity education that are crucial to establishing a sustainable cybersecurity workforce. By identifying , compiling, and disseminating foundational cybersecurity guidelines for academic institutions across the nation, collaboration with academic institutions can identify new or promote existing foundational curriculum that address skill gaps. The review of the current state of cybersecurity curriculum with academic institutions can collaboratively align cybersecurity education with specific work roles and career paths. The development of cybersecurity curriculum guidelines would provide minimum learning requirements in specific areas in partnership with academic organizations.

Providing resources to academic institutions should accelerate and expand cybersecurity education across the Nation by working with educational organizations to establish incentives for cybersecurity experts to serve as faculty. Additionally, measuring the success of supported educational programs that provide competencies, and knowledge, skills, and abilities associated with each category and Specialty Area in the Workforce Framework provides to incentivize academic institutions to expand and enhance their cybersecurity education programs.

Recruit and Hire Highly-Skilled Cybersecurity Talent

The Federal government struggles to attract and retain cybersecurity talent, Federal agencies must engage in strategic recruitment and awareness campaigns, and pursue individuals with cyber talent who, historically, may not have sought out government careers. This can be accomplished through enhancing recruitment efforts with dedicated human capital personnel and finding ways to streamline hiring and security clearance processes for cybersecurity personnel consistent with governing law and applicable standards. This also includes pay and leave flexibility, direct hire authority for information security professionals and a strategy aimed at recruiting diverse talent from among veterans, existing civil service employees, apprenticeship program graduates, and traditional sources. As well as providing opportunities for private sector

employees to participate in rotational assignments at Federal agencies, enabling professionals who may be reluctant to commit to a career in Federal service for short periods of time to share their skills with Federal employees while gaining Federal service experience.

Retain and Develop Highly-Skilled Cybersecurity Talent

In order to retain cybersecurity talent, agencies must foster an environment that provides rewarding and hands-on training experiences; supplies useful and appropriate technology; empowers employees; creates a positive and supportive workplace culture; and acknowledges that some of the cybersecurity employees the Federal Government hopes to attract may only wish to stay for a short period of service. Such non-traditional opportunities for training and skills refreshment must be considered in order to retain cybersecurity talent.

Enterprise-wide workforce planning includes efforts to incorporate certifications and training opportunities so that cybersecurity professionals remain knowledgeable about emerging trends in their area(s) of responsibility, with these and other professional development opportunities serving as retention strategies. Helping agencies develop career paths that leverage existing programs and responsibilities to deliver on best practices of performance management, talent development, and compensation flexibility increases the focus on retention for top performers.

These planning efforts include the development of:

- Orientation programs for new cybersecurity professionals.
- Cybersecurity career paths, rotational assignments, and mentoring and coaching programs, to provide employees with opportunities to become subject matter experts in their field or move into managerial roles and take on increased responsibilities.
- Tailored cybersecurity training for employees, senior managers, and executives who work in related career fields outside of cybersecurity
- Competitions, certifications, and credentialing to improve the skills of existing employees that may qualify them for potential pay increases or promotions based on demonstrated improvements in technical abilities.
- A common training program for specific categories of cybersecurity professionals.

The Government Lacks a Master Cyber Workforce Strategy to Attract and Retain Top Cyber Talent:

- **Develop a comprehensive cybersecurity workforce strategy**
  - Undertake a comprehensive, enterprise-wide examination of the cybersecurity workforce to better understand current capabilities and to develop a strategy to meet future needs. This strategy should contain clear steps to attract and retain cybersecurity talent, and include metrics for evaluating its success and shortfalls.
- **Create a new occupational job series for cybersecurity employees**
  - Establish a separate occupational series for the cyber workforce, or even a framework for an occupational group. The Cybersecurity Workforce Framework should serve as the basis for defining the new occupation.

Skilled Cyber Workers Are in High Demand and the Federal Government Struggles to Compete:

- **Expand cybersecurity internships and scholarships**
  - Internship programs in the cybersecurity arena could be used as a way to assess potential talent, agency officials then could convert top talent to full-time positions following completion of the internship. Congress should allow agencies to use Scholarship for Service authority to offer high-performing students scholarships directly in order to build a pipeline of talent that they want.
- **Create a cybersecurity reserve corps for college students**
  - To encourage more students to consider government service, we propose a civilian Cyber Reserve Training Corps, similar to the military's ROTC and modeled after the intelligence community's program.
- **Make academic cybersecurity certification more rigorous**
  - To increase the number of skilled cyber workers is to invest in the CAE program.

Government Loses Top Candidates to a Slow and Ineffective Hiring Process:

- **Expand direct-hire authority**
  - Expand direct-hire authority to cover all the jobs described in the Cybersecurity Workforce Framework, where cyber work is a considerable percentage of the individual's time. If one job series for the positions is covered by the Cybersecurity Workforce Framework, it could then grant direct-hire authority to the full series.
- **Put all cyber positions in the excepted service**
  - This will make it easier to hire the talent needs for all agencies. The administrative authority exists to place jobs in the excepted service when it determines that it is administratively difficult to evaluate candidates by traditional means.
- **Validate cybersecurity competitions and scenario-based testing to identify and assess talent**
  - Use competitions and challenges to identify talented individuals relating to such cyber skills as ethical hacking, penetration testing, vulnerability assessment, continuity of system operations, security in design, cyber forensics and offensive and defensive operations. Working with competition sponsors and other game developers, as a basis to immediately begin designing, developing and validating a prototype game-based assessment battery that is linked directly to the Cybersecurity Workforce Framework, and that can effectively and efficiently evaluate candidates' proficiency for cybersecurity jobs.
- **Allow agencies to share best qualified candidate lists**
  - Creating cross-agency lists will reduce the number of times a qualified applicant has to apply for and undergo assessment for similar jobs, and it will save agencies time and money in their search for cybersecurity employees. This would be

particularly feasible if OPM validates a common skills-based assessment. Create a national best-qualified applicant pool for major occupations or specialties.

- **Reform the security clearance process**
  - Ensure that the investigations are rigorous while being done in a timely manner to ensure the government can hire the cybersecurity talent it needs. Begin the lengthy security clearance process as early as possible.
- **Develop recruitment expectations of managers**
  - Agencies can hold program managers accountable for this expectation through their performance plans. Agencies' human resource offices should be made available to support these managers.

Agency Cyber Training and Development Is Uneven:

- **Create a cybersecurity training academy focused on both technical and leadership skills**
  - An academy will help ensure that the government's cybersecurity professionals meet the most rigorous technical standards. It also would allow cyber talent to build relationships with each other that could enhance protection of our networks. An academy would also provide significant economies of scale.
- **Create a cyber reserve for experienced talent**
  - A Cybersecurity Reserve Corps could include graduates of the training academy who agree to assist agencies with specific projects over time. Since we know that many of government's top talent leave federal service for the private sector, we need to create opportunities to re-engage them as needed.
  - A Cybersecurity Reserve Corps could be an organization that captures the intellectual rigor and standards of conduct of the medical and legal professions; and the ethos of the Public Health Service and the military reserves, as well as their agility, continuous learning and ability to provide assistance in times of need. Borrowing from the emergency management field, establishing opportunities for individuals to train together and work together will improve their ability to work together and leverage each other's areas of expertise when needed.

Government Compensation Isn't Competitive, Especially for Experienced Talent:

- **Conduct a pay study**
  - Commission a biannual total compensation comparison between federal and private-sector cybersecurity jobs to more precisely measure differences in pay and benefits that may impact recruiting, hiring and retention. The comparison should be built off of the cyber professions that have been identified in the Cybersecurity Workforce Framework.
- **Track cyber attrition**
  - Develop and administer a common web-based exit survey to track and understand the reasons behind cybersecurity attrition. An exit survey would further our

understanding of why top talent is leaving across the government so so it can be learned how better to retain it. Track the Federal Employee Viewpoint Survey data by occupation, which could point to warning signs before talent leaves government.

- **Develop a market-sensitive pay system for the cyber workforce**
    - Based upon the compensation comparison, immediately begin the design and development of a special occupational pay system for jobs covered by the Cybersecurity Workforce Framework. Implement pay reforms with respect to its mission-critical cybersecurity occupations. Establish "special occupational pay systems" that supersede the limitations of the General Schedule.

5.8 State Government Findings

Each and every state has a need to recruit, retain, and train a workforce capable of reducing the cybersecurity risks for all state maintained cyber infrastructure that underpins all aspects of state government and the state services provided to its residents. A strong cybersecurity workforce is needed to protect the information and communication technologies used by state employees to perform their daily jobs as well as to protect the state run critical infrastructure.

Information and communication technologies are being added and networked together in more and more places meaning that all organizations like states who have responsibility to reduce risk, in this case cybersecurity risk, are constantly challenged to maintain a workforce capable of reducing cybersecurity risk in an increasingly complex environment. Our entire Nation is coming to grip with the cybersecurity challenges presented by the adoption of cyber-physical systems, the need to protect sensitive data, and the privacy and security challenges added by the data being derived from Internet-Of-Things devices that are becoming more pervasive. States are competing to recruit and retain their cybersecurity workforce. The challenges faced by states are generally the same as those faced by Federal and private sector organizations with cybersecurity workforces. Most states have four year (4Y) and two year (2Y) schools who are preparing students and producing graduates capable of entering into state government service in cybersecurity positions. The NSA/DHS Centers of Academic Excellence program has been in existence since 1998. There NSA/DHS Centers of Academic Excellence offers the following designations:

- CAE-IAE 4Y- National Centers of Academic Excellence in Information Assurance Education
- CAE-CDE 4Y Cyber Defense Education
- CAE/IAE 2Y Information Assurance 2-Year Education
- CAE-CDE 2Y Cyber Defense 2-Year Education
- CAE-IA-R Information Assurance Research

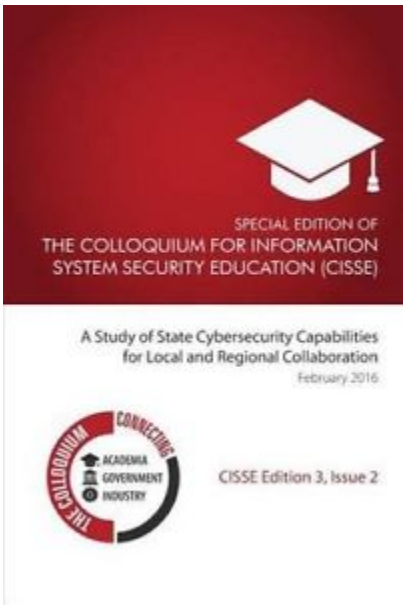
Designated schools offer programs that reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. Designation is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation.

- Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.
- CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.
- Alphabetical listing by state of designated schools https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm

There are NSF grants focused on helping more 2Y schools receive the designation, and there is a CAE community https://www.caecommunity.org/ where one can connect with other schools who have already received the designation for guidance on how to prepare a non-CAE school to obtain the designation.

As awareness of the cybersecurity workforce challenges have grown, more Governors, state legislature, CIOs, CISOs, Attorney Generals are stepping up to address state cybersecurity workforce issues.

This summary does not try to duplicate one reference point that organizations can use to explore state capabilities, the Special Edition of the Colloquium for Information System Security Education (CISSE) A Study of State Cybersecurity Capabilities for Local and Regional Collaboration by Barbara Endicott Popovsky Phd 9781523285778 (Paperback, 2016)



The National Governors Association chaired by Virginia governor Terry McAuliffe has a "Meet the Threat – States Confront the Cyber Challenge" initiative[45] with the primary goal for states to

[45] http://ci.nga.org/cms/home/ci1617/index.html

develop strategies for strengthening cybersecurity practices as they relate to state IT networks, health care, education, safety, energy, transportation, critical infrastructure, economic development and workforce. At present, the resources offer DHS resources that support the NICE Workforce Framework.

The National Association of State Chief Information Officers (NASCIO) has identified improving cybersecurity as a pressing public sector challenge. Human Resources/Talent Management is item 8 in their top 10 final ranking of state CIO priorities for 2016[46]. The prioritized list is provided in Attachment 9. Additionally, NASCIO has a cybersecurity committee and has a number of resources on its webpage[47], including a map on which you can click on any state and be taken to state page focused on cybersecurity. No direct workforce initiatives are identified on the NASCIO site.

All 50 states are represented in the MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER (MS-ISAC)[48]. The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative effort based on a strong partnership with the Office of Cybersecurity and Communications within the U.S. Department of Homeland Security (DHS). The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. The MS-ISAC has built and nurtured a trusted environment of collaboration and cooperation that is improving the cyber posture of SLTT governments. State Principal members are generally CISOs from each state. While not specifically involved with cyber workforce development, the MS-ISAC negotiates discounts on behalf of all SLTT governments, saving as much as 85% off the commercial price, providing cost-effective access to the training that governments need most.

Attachment 10 provides a state by state summary listing of highlights in workforce development initiatives.

6 Recommendations

The CSRIC V Working group 7 was tasked to examine and develop recommendations for the CSRIC's consideration regarding any actions that the FCC should take to improve the security of the nation's critical communications infrastructure through actions to enhance the transparency, skill validation, and best practices relating to recruitment, training, retention, and job mobility of personnel within the cybersecurity field. We evaluated many different segment approaches to specific aspects of the challenges we face as an industry. The information gathered and analysis conducted lead us to focus on recommendations that would positively impact the global challenge that we face across both the private and public cybersecurity workforce. Workforce Development is not about filling job openings, although that is a source of metrics often used to represent the scale of the challenge. Instead, we chose to base our

[46] http://www.nascio.org/Portals/0/Publications/Documents/2015/State_CIO_Top%20_Ten_Policy_and_Technology_Priorities_for_2016.pdf
[47] http://www.nascio.org/Advocacy/Cybersecurity
[48] https://msisac.cisecurity.org/members/state-government/

approach on the simple adage – a rising tide raises all boats. This led us to focus on the following broad based recommendations that would expand the available pipeline of skilled candidates for our industry as a whole.

6.1 The FCC Should Support a Process for the Communications Industry to Cooperatively Support Updates to the NICE Cybersecurity Workforce Framework (NCWF)

The NCWF builds upon decades of industry research into how to effectively manage the risks to valuable organizational electronic and physical information. Through the years, the industry that has been referred to as computer security, information security, and now cybersecurity has been supported by dedicated workers supporting an evolving set of Work Roles, Tasks, and KSAs. Cybersecurity tactics are ever-changing, always identifying new ways to gain information advantage through technology. As organizations evolve the ways they perform cybersecurity functions, so must the components of the NCWF continue to evolve. During the time period while the Working Group was evaluating the fit of the NCWF as a reference resource for Communication Sector specific requirements, DHS and NIST released an update in the form of Draft NIST SP 800-181, the NICE Cybersecurity Workforce Framework. The data elements of the NCWF version 2.0 from 2014 were reviewed and developed as a deliverable for this initial phase of the Working Group 7 tasking. WG7, in a cooperative engagement with CWA, submitted inputs through the NICE Working Group to the updated NCWF to include review of roles and identification of common KSAs across industries that serve as the core for development of curricular guidance. Ongoing Industry participation in the process of supporting periodic review and update through a continuous cycle is a recommendation resulting from these efforts. By continuing to identify and evolve the NCWF training requirements, this data is less likely to get stale or become inapplicable to the dynamic needs of the Communication Segment. The Working Group recommends to the CSRIC V that it should guide the FCC to encourage Industry participation in the CWA to facilitate the sustainment of this dataset.

The plug-and-play nature of the CWA model enables a local, national and international role out of the industry, which has already proven to deliver the requisite workforce readiness skills on a massive scale. The CWA has opened operations in the United Kingdom and due to demand is planning on opening in Europe, Singapore, Kuala Lumpur, India and Hong Kong (and wherever there is a viable cohort of education and industry stakeholders). The Communications Industry sector members can join the CWA 'boat' to take immediate advantage of internationalization on a rising tide. Thus, minimizing cost/effort while maximizing contribution, standardization and benefits.

While the CWA was founded in the Financial Markets, the taxonomy is open source (on spreadsheets) and is transportable across the private sectors. FCC can be both a collaborator and a beneficiary. As a collaborator, the CSRIC V Working Group 7 has contributed 162 additional rows to the NICE cybersecurity taxonomy and as a beneficiary now has access to1,230 taxonomy rows including essential workplace roles and professions. Common KSAs found in all job roles can now be aligned with Knowledge Units taught by education, thus improving education curriculum to industry requirement alignment. It is anticipated that the Utilities Technology Council will also be adopting the CWA led taxonomy and NIST framework to adopt the standard and not go-it-alone. All development outcomes get fed back to NICE for validation and recycling and new NCWF releases. On behalf of the CWA, iQ4 has automated

the NICE taxonomy, avoiding the burden of management by spreadsheets and initiated a project to apply the Knowledge, Skills and Abilities (KSAs) to all job families across the IT/Digital disciplines. A CWA workgroup will then expand and validate the content which can then be automated as well.

The CWA has developed a model where, via virtual-*menternships*™, the workplace is delivered into the classroom for team-based, role-based, time-bound real world experiential learning challenges where students are mentored by industry Cyber/Risk experts.

- The on-line curriculum is designed to develop workforce skills and readiness in entry-level enables cyber/risk candidates to cut 3-months or more out of the time taken to on-board them and spin up to productivity.
- The model enables employer to cast a wider net (locally, nationally and internationally) and level the playing field to find hidden talent and meet diversity and veteran employment opportunity goals.
- Universities engaged as CWA members are commencing to "scaffold" in Colleges and High Schools (down to K9 in one case) to the CWA course they run for undergraduates.

6.2 Communications Industry can Benefit by Growing Awareness of and Supporting Programs Encouraging K-12 Youth to Study Cybersecurity

Successful programs have been developed to encourage early development of the skills necessary in science, technology, engineering and mathematics (STEM) such as GenCyber, the BATEC Summer Bridge program and other internship programs that engage K-12 students. These programs would benefit and expand with active Communications Industry involvement and support. General areas of support to include Seminars, presentations at schools, after school workshops and even summer programs like cyber camps can all be used to spread awareness of cybersecurity and encourage the next generation to both practice good cyber hygiene and potentially consider a career in cybersecurity.

Industry members should also consider the value of participating in or supporting cybersecurity competitions as a means to raise awareness about cybersecurity and to develop skills in students who may become part of our workforce. The Competitions subgroup of the National Institute for Cybersecurity Education (NICE) Working Group recognized a need for a deeper look into the role that cybersecurity games play in developing tomorrow's workforce. A commissioned study resulted in the report, "Cybersecurity Games: Building Tomorrow's Workforce" which is included as Appendix 14 to this report and quoted below:

> "Competitions provide a valuable learning opportunity for participants, regardless of skill level. 'Cyber as a sport' is a growing trend in high schools; the number of high school teams that participated in the Air Force Association's CyberPatriot doubled in a two-year period from over 2,200 in 2014 to over 4,000 in 2016.9 Educators increasingly recognize cyber competitions demonstrate and develop planning, leadership, collaboration and communication skills and offer a compelling alternative for students of all ages who are less likely to compete or excel at physical sports.
>
> Finally, the safety, security and enjoyment aspects of competitions should not be

overlooked. When practicing both offensive and defensive maneuvers in a typical competition environment, players are encouraged to practice and hone cybersecurity skills in a controlled, real-world environment where no harm can come to the competitors. Moreover, cyber competitions are enjoyed as a forum for networking, team building, and information sharing."[49]

The Working Group membership further recognize the value of competitions that extend beyond the K-12 student population to Colleges and even industry professionals as a method to increase awareness of the opportunities in cybersecurity across a broader population.

6.3 The FCC Should Encourage Communications Industry Development of Cooperative Work-Study Program Partnerships

Internship programs in the cybersecurity arena could be used as a way to assess potential talent, agency officials then could convert top talent to full-time positions following completion of the internship. Successful programs:

- Develop engaging internship roles with clearly defined expectations and deliverables that provide value to the company and the individual
- Ensure the intern has the opportunity to explore several cybersecurity functions within IIS, in addition to their internship role
- Enable the intern to appreciate the depth and breadth of the cybersecurity program
- Assist with recruiting for future interns and permanent roles

In addition to Internships, the use of Apprenticeships is a provide solution for recruiting, training, and retaining world-class talent. Programs like ApprenticeshipUSA offer the Communications Industry access tools that can be leveraged to establish, monitor, and grow a successful ApprenticeShip program.[50] Accordingly, WG7 recommends that Communications Industry members consider participating in existing partnerships or establishing their own work-study programs as a best practice to develop and hone cybersecurity skills in new or existing staff specifically focused on the unique needs to the members of the Communications Industry segment.

6.4 The FCC should engage with the Communications Industry to Develop or Expand Scholarship for Service Programs in Industry

Industry should consider scholarship for service programs in which students are given scholarships while in school that obligate the student to work for a certain period of service for a private employer. The United States government CyberCorps®: Scholarship for Service (SFS)[51] is a unique program designed to increase and strengthen the cadre of information assurance professionals working in federal, state, local, and tribal entities protecting the government's critical information infrastructure. This program provides scholarships that may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. Additionally, participants receive stipends of $22,500 for undergraduate students and $34,000 for graduate students. The scholarships are funded through National Science Foundation grants awarded to a higher education faculty member who recruits

[49] http://lp.katzcy.com/cybersecuritygames
[50] https://www.dol.gov/featured/apprenticeship
[51] https://www.sfs.opm.gov/

the students into the program. Recently, two year schools have been added to the program such that students apply at two year schools apply for the SFS scholarship that will include completion of a degree at a four year school.

6.5 The FCC Should Encourage Communications Industry Cybersecurity Professionals to Help Train the Next Generation

The Academic Segment has identified a severe shortage of qualified instructors. As a result of this shortage, it is becoming increasingly difficult for the Academic Segment to address the growing demands for training in cyber security practices. CSRIC WG7 believes that the Communications Industry is well positioned to assist the Academic Segment by encouraging our current professional staff with skills in cyber security to pursue adjunct faculty positions, participate as guest speakers or even host seminars/webinars that will help to bring an industry specific view of opportunities in the Communications Industry for cybersecurity specialist. By helping to address the specific gap with qualified staff from the Communications Industry, the Working Group believes that this will both increase the number of candidates that can receive training and also influence the content to be more specific to the needs of the Communications Industry.

6.6 The FCC Should Encourage the Communications Industry to Participate in the Development of Curriculum Guidelines by the Joint Task Force on Cybersecurity Education

The ACM Joint Task Force on Cybersecurity Education (JTF) was launched in September 2015 with the purpose of developing comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts. The JTF is a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF grew out of the foundational efforts of the Cyber Education Project (CEP).

The Communications Industry should be prepared to provide comments as the JTF surveys industry and publishes material for comments. Additionally, in late 2016, NSA's College of Cyber solicited proposals from educational institutions who wish to educate and prepare cybersecurity graduates to fill Federal government cybersecurity positions. The communications industry should track which educational institutions receive funding and collaborate with those institutions when opportunities arise.

6.7 FCC Should Partner with Communications Industry, Public Safety, and Federal GenCyber to Develop a Cybersecurity Distance Learning Program for Public Safety and Rural Communities

Based on our analysis of the data provided and the unique challenges facing Public Safety both in terms of the geographic reach required and the nature of the training needed, the WG7 members propose consideration of a distance learning initiative for delivery of the cybersecurity curriculum that can initially support basic cybersecurity hygiene and eventually expand into a broader course list addressing awareness and basic/entry level skills in cybersecurity for small

and rural PSAPs. By offering this program in partnership with local schools, universities and/or community colleges, this could become a "lightening rod" for expanding basic literacy in cybersecurity and potentially lead to expansion of skills required for higher paying jobs/careers where the opportunity currently does not exist. This could help develop new workforce sourcing opportunities in the rust belt or rural areas to cross the digital divide.

6.8 The Communications Industry Should Support Innovative Cybersecurity Workforce Development Initiatives such as the CyberBlue Program Support to Engage Populations with Disabilities

We currently face massive cybersecurity workforce shortages worldwide, lacking people who think critically, recognize patterns, efficiently analyze data, discard preconceptions, and focus deeply. Many autistic adults possess these exact cognitive abilities, but employers are aware of only their social disabilities, creating a workforce mismatch that exacerbates security threats and perpetuates disenfranchisement of persons with social disabilities. Over 70 million people worldwide are living with autism and the dramatic upswell of autistic adults will exceed 3 million in the U.S. alone by 2020. At the George Washington University (GW), researchers are proposing an innovative approach: "CyberBlue"[52]—a bold, scalable solution that uses one social challenge to solve another. The GW-led initiative is a collaboration between the I3P[53] and GW's Autism and Neurological Disorders Institute. GW's team of experts aims to prepare a new generation of autistic adults to be "cyber warriors" and launch new workforce initiatives to strengthen systems, transform lives, and change global thinking about populations with disabilities.

6.9 Communications Industry Cybersecurity Experts Should Join the National Initiative for Cybersecurity Education (NICE) Working Group or One of its Subgroups

The NICE Working Group (NICEWG) has been established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. Subgroups have been established to focus in areas that are reflected in the earlier recommendations of this report. Below is a table that describes the NICE Working Group and the five subgroups. Each subgroup and the overall working group meet once a month via conference call/webinars. The subgroup members agree to voluntarily work on initiatives or the sharing of best practices that further progress towards the NICE Strategic Goals and Objectives.[54]

[52] Video introduction: https://youtu.be/oJhzM4ttW-E

[53] I3P members involved include: MITRE, SRI, JHU APL, University of California Davis, Dartmouth

[54] http://csrc.nist.gov/nice/about/strategicplan.html

Group	Description (Purpose)	Subscribe (send email to with this in subject line)
NICE Working Group	The NICE Working Group (NICEWG) has been established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.	Email nicewg-request@nist.gov with the subject line: "Subscribe" and include your full name and email address in the body of the message.
K12	Focuses on topics pertaining to developing strategies and recommendations for filling the national cybersecurity pipeline through a K-12 Cybersecurity Education Strategy.	Email nicewg.k12@nist.gov with the subject line: "K-12 Subscribe", and with your full name and email address in the body of the message.
Collegiate	Focuses on topics pertaining to the burgeoning Information Security discipline, including guiding curricular standards, aligning academic pathways to the National Cybersecurity Workforce Framework job roles, and stimulating the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers	Email nicewg.collegiate@nist.gov with the subject line: "Collegiate Subscribe", and with your full name and email address in the body of the message.
Competitions	Focuses on topics pertaining to increasing and strengthening the cadre of cybersecurity professionals and connecting cybersecurity employees and employers. This subgroup will explore the supply and demand of cybersecurity professionals.	Email nicewg.competitions@nist.gov with the subject line: "Competitions Subscribe", and with your full name and email address in the body of the message.
Training and Certification	Focuses on topics pertaining to the development and management of performance-based evaluation and training programs, capable of adapting to meet the nation's evolving cybersecurity needs. This sub-committee will also explore mapping professional certifications to the framework.	Email nicewg.tandc@nist.gov with the subject line: "Training & Certifications Subscribe", and with your full name and email address in the body of the message.

Group	Description (Purpose)	Subscribe (send email to with this in subject line)
Workforce Management	Focuses on facilitating, developing, and promoting cybersecurity workforce management guidance and measurement approaches that create a culture where the workforce is managed and engaged to effectively address the cybersecurity risks of their organization.	Email nicewg.wm@nist.gov with the subject line: "Workforce Management Subscribe", and with your full name and email address in the body of the message.

7 Conclusions

This final report demonstrates the applicability of the National Cybersecurity Workforce Framework to the Communication Sector specific cybersecurity skills requirements. The dataset provided as an Appendix to this Final Report was also provided to the FCC as an electronic file (Excel Spreadsheet) that can be released at the discretion of the FCC without restriction.

In developing our final report, Working Group 7 collaborated across academia, industry and government to develop recommendations and identify best practices that can be leveraged to enhance cybersecurity workforce planning. We also identified applications, templates, and other tools that are available to the Communications Sector to continue to promote existing and future cybersecurity workforce development activities. This final report includes specific recommended actions that are available to our industry to expand and fill the cybersecurity workforce pipeline.

As an industry, we are still in the early days of addressing the development of a skilled cybersecurity workforce that can meet our needs. Future activities may include:

- Extending and integrating activities across the Communications Sector to raise cybersecurity awareness;
- Identifying and supporting foundational research opportunities in areas including cybersecurity awareness, training, and education, and security usability;
- Continuing to improve our understanding of sector specific cybersecurity workforce needs; and
- Issuing guidelines, tools, and other resources to develop, customize and deliver cybersecurity awareness, training, and education materials.

8 Table of Appendices

Appendix No.	Title
Appendix 1	National Cybersecurity Workforce Framework Communications Sector Recommended KSAs
Appendix 2	National Cybersecurity Workforce Framework Communications Sector Recommended Categories, Specialties and Competencies
Appendix 3	Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals
Appendix 4	Cybersecurity Workforce Development Toolkit
Appendix 5	Cyber Workforce Development Best Practices
Appendix 6	Building the Cyber Workforce Pipeline
Appendix 7	BATEC Cybersecurity Workforce Report
Appendix 8	Cyber Training Best Practices – Federal Government Segment
Appendix 9	State CIO Top Ten Policy and Technology Priorities for 2016
Appendix 10	State Workforce Initiatives by State
Appendix 11	IQ4 Business Case Talent Investment ROI Model
Appendix 12	Fed Cybersecurity Workforce Strategy – OMB Memorandum
Appendix 13	ACM JTF Survey on Cybersecurity Education
Appendix 14	Cybersecurity Games – Building Tomorrow's Workforce