CSR C

Communications Security, Reliability and Interoperability Council

March 2016 WORKING GROUP 7

Cybersecurity Workforce

Interim Report – Analysis of Applicability of the National Cybersecurity Workforce Framework (NCWF) to the Communications Sector and Identification of Gaps

Table of Contents

1 Executive Summary 3

2 Introduction 5

2.1 CSRIC Structure 7

2.2 Working Group 7 Team Members 7

3 Background 8

3.1 Cybersecurity Workforce Planning 8

3.2 The DHS Capability Maturity Model (CMM) 11

3.3 Using the DHS Maturity Model 11

4 Objective, Scope, and Methodology 12

4.1 Objective 12

4.2 Scope 12

4.3 Methodology 13

4.3.1 Evaluate National Cybersecurity Workforce Framework 13

4.3.1.1 Application of NCWF to the Communications Sector 14

4.3.1.2 Identify Gaps and Improvements 14

4.3.2 Identify, develop and recommend Best Practices 15

4.3.2.1 Communications Industry 15

4.3.2.2 Academic Segment 15

4.3.2.3 Public Safety 16

4.3.2.4 Financial Sector 16

4.3.2.5 Federal Sector 16

4.3.2.6 State Government Example 17

5 Findings and Recommendations 18

5.1 Findings 18

5.1.1 Application of the National Cybersecurity Workforce Framework (NCWF) to the Communications Sector 18

5.1.2 Identify Gaps and Improvements in the NCWF 18

5.2 Recommendations 19

6 Conclusions 19

7 Table of Appendices 20

# 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]](#footnote-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]](#footnote-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).

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.[[3]](#footnote-3) 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. [[4]](#footnote-4)

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 the context to enhance the volume and quality of the workforce, including[[5]](#footnote-5):

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 groups should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

This Interim Report addresses 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 plans to pursue over the next twelve months to identify, develop and recommend best practices for consideration by the CSRIC V membership for inclusion in the Final Report.

The [National Cybersecurity Workforce Framework](https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework) (NCWF)[[6]](#footnote-6) 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 Interim Report as Appendices 1 and 2. It will also be delivered to the FCC as a working database in Microsoft Excel format.

We recognize that cybersecurity workforce development is undergoing rapid change and evolution. This Interim 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 Planning gains maturity in our respective organizations. As part of the Final Report, WG7 will provide specific recommendations for consideration by CSRIC on a process for adaptation and improvement of the sector specific dataset.

# 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[[7]](#footnote-7). 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.

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[[8]](#footnote-8) 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 are developing a draft special publication of the NCWF to be released by NIST for public comments during spring of 2016 that will expand to add cyber work roles and the associated Knowledge, Skills, Abilities (KSAs) into a national cyber workforce framework.

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.[[9]](#footnote-9) Furthermore, the Council’s recommendations will 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.[[10]](#footnote-10)

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](https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework) (NCWF)[[11]](#footnote-11) 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. 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.

A more comprehensive overview of the NCWF is available at the National Initiative for Cybersecurity Careers and Studies (NICCS).

## 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 |
| 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 |

Table 1 - Working Group Structure

## 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) | Windup Ventures |
| Chris Boyer | AT&T Services |
| Prentis Brooks | Time Warner Cable |
| Upendra Chivukula | State of New Jersey |
| Frank Cicio | IQ4 representing Cybersecurity Workforce Alliance |
| Barbara Endicott-Popovsky | University of Washington |
| Jay English | APCO International |
| Andrew Fry | University of Washington |
| Mike Geller | Cisco Systems |
| Alexander Gerdenitsch | EchoStar |
| Kazuhiro Gomi | NTT America |
| Scott Haas | IID Security Central |
| Shinichi Hirata | NTT Corporation |
| Jeremiah Jones | DHS/OEC |
| Anna Jackson | FireEye |
| Kim Keever | Cox |
| Masato Kimura | NTT Corporation |
| Steven Leese | APCO International |
| Steve Mace | NCTA |
| Jennifer Manner | EchoStar |
| Shawn Matthews | PacOpticNetworks |
| Robert Mayer | US Telecom Association |
| Bill Newhouse | NICE Program Office at NIST |
| Daishi Sakakibara | NTT Corporation |
| Quentin Sa’Lay | Comcast NBC Universal |
| Matthew Straeb | Alert FM |
| Nobumitsu Takeuchi | NTT Corporation |
| Zachary Tudor | SRI International |
| Erik Wallace | TeleCommunication Systems |
| Gary Warner | UAB |
| Jen Weedon | FireEye |
| Kathy Whitbeck | Nsight |
| Shinichi Yokohama | NTT Corporation |

Table 2 - List of Working Group Members

# 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.[[12]](#footnote-12)

## Cybersecurity Workforce Planning[[13]](#footnote-13)

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](https://niccs.us-cert.gov/glossary#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](https://niccs.us-cert.gov/glossary#impact) an organization’s ability to meet goals and objectives.

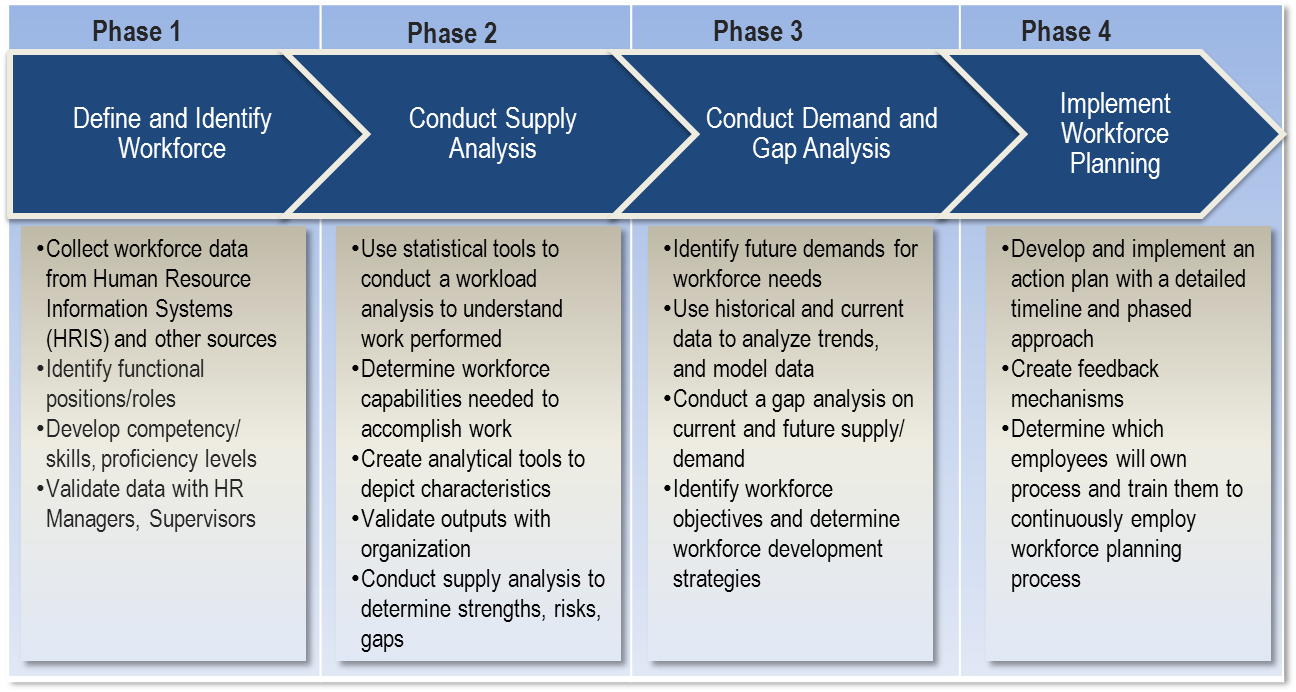


Figure 1 – Example Workforce Planning Process

Additionally, cybersecurity workforce planning will require a shared vision and performance management.  A shared vision will provide a common language and taxonomy to define cybersecurity workload and workforce allowing agile [response](https://niccs.us-cert.gov/glossary#response) to emerging technology and new threats.  Performance management is also [key](https://niccs.us-cert.gov/glossary#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](https://niccs.us-cert.gov/glossary#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](https://niccs.us-cert.gov/glossary#capability) Maturity Model to apply the elements of best practice workforce planning to [analyze](https://niccs.us-cert.gov/glossary#Analyze) their cybersecurity requirements and maturity needs.

## 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.

## 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 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
* Determine priority areas for increased maturity and develop action plans

# Objective, Scope, and Methodology[[14]](#footnote-14)

## 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.

## Scope

Specifically, this working group will leverage existing work in the context to enhance the volume and quality of the workforce, including[[15]](#footnote-15):

* 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; and
* 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 groups should consider means to promote a common lexicon and roadmap that will promote more effective interface with academic institutions and other training environments.

## Methodology

The approach that Working Group 7 has undertaken to address the cybersecurity workforce development tasking assigned by CSRIC V is 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.

### 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. WG7 Members focused on defining the role profiles from an extended baseline of the NCWF Specialty Area, Competencies, and KSAs instead of starting our work from scratch. WG7 leveraged the Cybersecurity Workforce Alliance (CWA) data set and process developed in support of the Financial Sector as our 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.

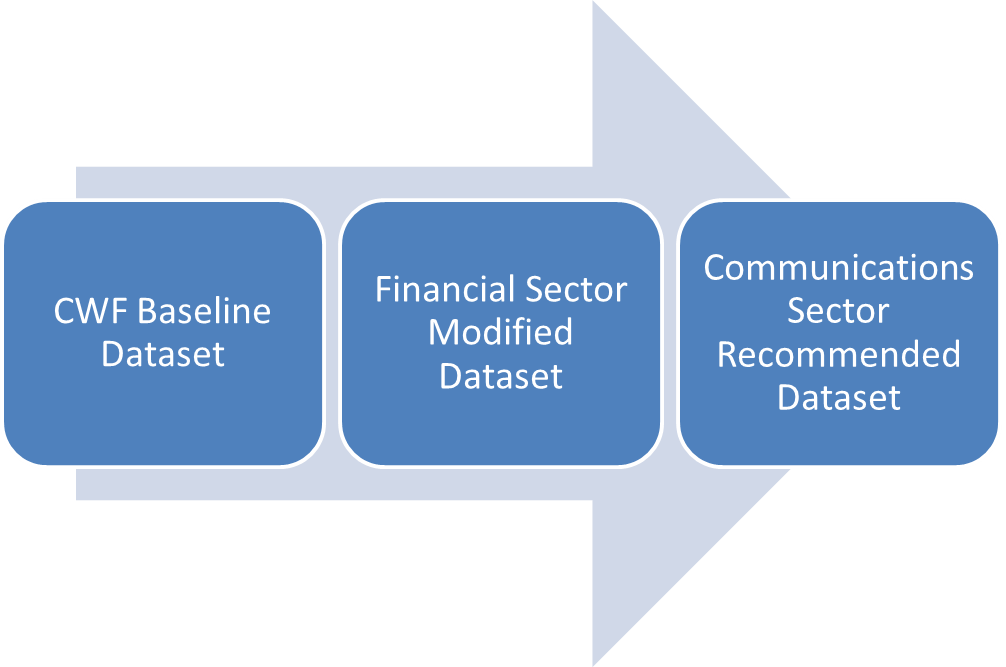


Figure 2 - NCWF Evaluation Process

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.

#### 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.

#### 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.

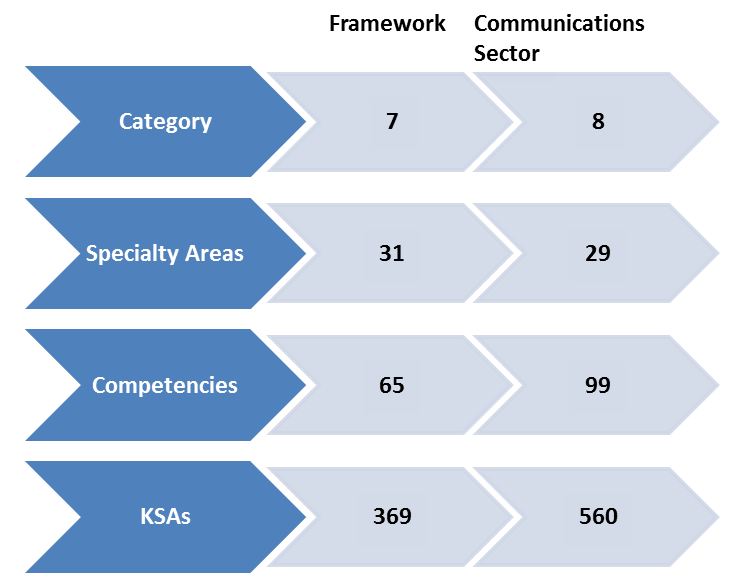


Figure 3 - Summary Data from NCWF Gap Identification

### 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 intend to follow will be 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 plan to gather 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.

#### Communications Industry

The Working Group members will be tasked to review 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.

This section will be completed in the final draft due March 2017.

#### 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.

As a tool for the CSRIC to better understand the nature of the challenge, the Working Group will develop and provide a matrix to describe the types of institutions – 2 year, 4 year, research, for profit technical schools – and the specific roles they have in the cybersecurity workforce development. We will catalog the 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. The result of this survey and analysis will be to provide guidance to the CSRIC on recommendations for the FCC to enhance workforce development.

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 will include 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.[[16]](#footnote-16)

This section will be completed in the final draft due March 2017.

#### 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, the FirstNet program is completely changing 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.”[[17]](#footnote-17)

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

This section will be completed in the final draft due March 2017.

#### Financial Sector

Working Group 7 was able to leverage work done by the Cybersecurity Workforce Alliance in support of the Financial Sector as part of our review of the National Cybersecurity Workforce Framework. In this section, we will review some of the lessons learned and practices from the Financial Sector as part of their initiative to tackle the cybersecurity workforce development gap.

This section will be completed in the final draft due March 2017.

#### Federal Sector

The 2013 Executive Order on Critical Infrastructure Security assigns roles for the adoption of the cybersecurity framework for critical infrastructure protection[[18]](#footnote-18) 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.[[19]](#footnote-19) The Working Group will review DHS NICCS available tools, practices, and policies for Cybersecurity Workforce Development that have been leveraged by Federal Sector agencies, and the recent focus on workforce in both the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government[[20]](#footnote-20) (October 2015), and the workforce aspects of the Cybersecurity National Action Plan (CNAP)[[21]](#footnote-21). The survey will also include a discussion of an example application to demonstrate application of the NCWF in practice.

This section will be completed in the final draft due March 2017.

#### State Government Example

The National Association of State Chief Information Officers (NASCIO) in partnership with Deloitte conducted a Cybersecurity Study in 2014. The study reports findings and analysis were 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:

“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.”[[22]](#footnote-22)

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 can also engage with the NICE Working Group (NICEWG)[[23]](#footnote-23) subgroups to leverage their extended reach across the nation to identify state and local progress in areas 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 in 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 will consolidate the information gathered from this sample of ongoing workforce development program activities in support of State government cybersecurity needs. The purpose here is not to create an exhaustive compendium, but rather to provide examples of active programs with the purpose of providing insights into current State best practices, policies and tools to inform the CSRIC V members.

This section will be completed in the final draft due March 2017.

# Findings and Recommendations

## Findings

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 will require 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, is 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.

### 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 input from NIST, DHS and the Office of the Secretary of Defense (OSD) that the Cybersecurity Workforce Framework and the soon to be released 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.

### 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 database developed by the financial sector.

Almost all of the KSAs reviewed by WG7 participants were common across their unique segment. Specifically, we found that Public Safety and Radio/Telecommunications specific KSAs were lacking in the initial data set provided 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.

## Recommendations

Cybersecurity Workforce Development is not static. The dataset reviewed was based on the 2014 NCWF release. During time period while the Working Group was evaluating the NCWF dataset from Communication Sector specific changes, DHS and NIST released an update to the National Cybersecurity Workforce Framework. The data elements of the NCWF database reviewed and developed as a deliverable for this initial phase of the Working Group 7 tasking serve as a first release. A process will need to be developed to support a periodic review and update through a continuous cycle or this data is likely to get stale and no longer be applicable to the dynamic needs of the Communication Segment. The Working Group will develop recommendations to the CSRIC V members in our Final Report for the sustainment of this dataset to include process, participants, and deliverable definition for consideration by the FCC.

This information base can be leveraged using automated tools that already exist. In preparing the Final Report, WG7 will investigate best practices across different sectors. We also plan to evaluate and report on tools that are readily available or can be adapted for the Communications Sector. Finally, we anticipate the need to investigate and report on the specific challenges facing Academia and possible approaches to mitigate these risks to meeting the rising demand for a skilled cybersecurity workforce.

# Conclusions

This interim 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 report will also be 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, the Working Group plans to further collaborate across academia, industry and Government to develop recommendations and identify best practices that can be leveraged to enhance cybersecurity workforce planning. We also anticipate identifying applications, templates, and other tools that are available to the Communications Sector to continue to promote existing and future cybersecurity workforce development activities. We also plan to document specific actions that are available to our industry to increase engagement with academia 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.

# Table of Appendices

|  |  |  |
| --- | --- | --- |
|  | Title | Page No. |
| Appendix 1 | **National Cybersecurity Workforce Framework Communications Sector Recommended KSAs** | **17** |
| Appendix 2 | **National Cybersecurity Workforce Framework Communications Sector Recommended Categories, Specialties and Competencies** | **40** |
| Appendix 3 | **Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals** | **45** |

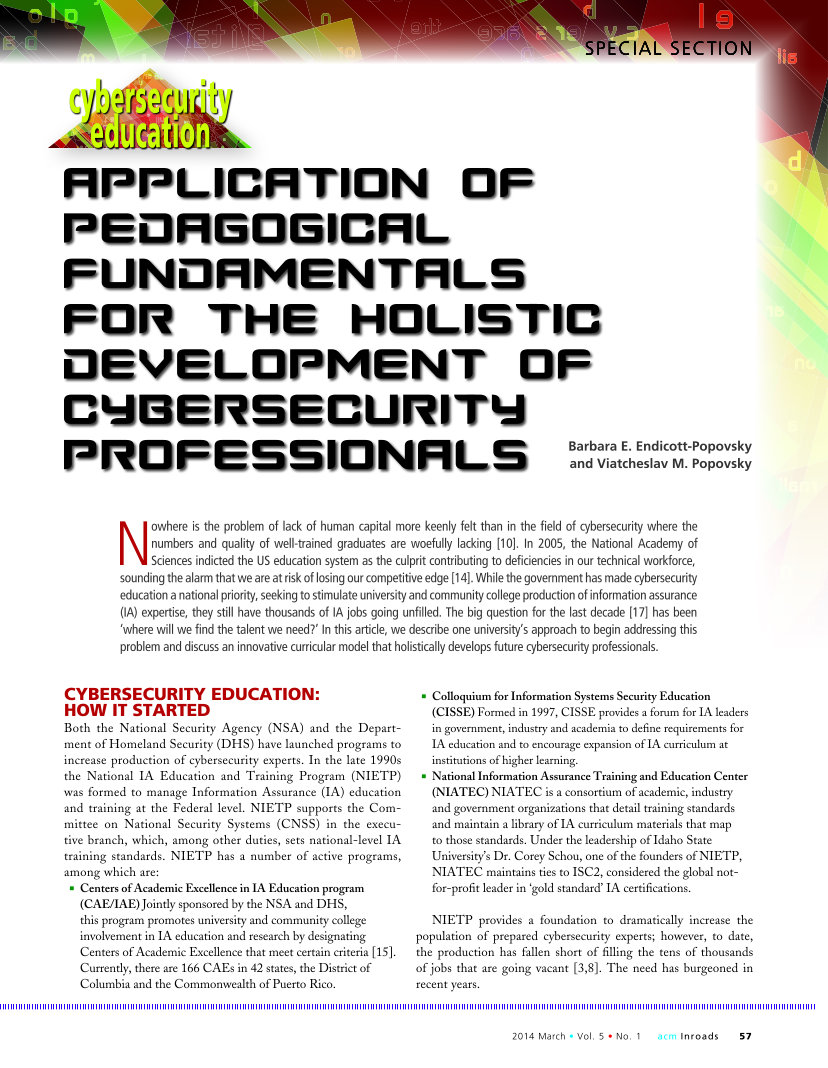
**Appendix 1 – National Cybersecurity Workforce Framework Communications Sector Recommended KSAs**

| **Knowledge, Skills, Abilities (KSAs)** | **Applicability** |
| --- | --- |
| Acknowledges and incorporates the values and interests of supervisors and/or leaders to produce results in-line with organizational vision. | Applicable |
| Initiates, maintains and facilitates the flow of needed information through organization following chain of command structure | Updated |
| Requests needed resources in order to meet organizational expectations. | Applicable |
| Analyzes threat information from multiple sources, disciplines, and Federal/State/Local agencies. Synthesizes and places intelligence information in context draws insights about the possible implications. | Updated |
| Accurately identifies and analyzes data and problems. | Applicable |
| Demonstrates the ability to identify and evaluate problems or issues | Applicable |
| Takes action to monitor and control time and costs | Applicable |
| Skill in analyzing network traffic capacity and performance characteristics. | Applicable |
| Adapts effectively to changing priorities/assignments. | Applicable |
| Effectively plans, prioritizes, and manages multiple projects. | Applicable |
| Treats change and new situations as opportunities for learning or growth | Applicable |
| Actively works across function on broad projects to achieve broad objectives. | Applicable |
| Builds strong partnerships by genuinely seeking out others’ opinions and ideas. | Applicable |
| Can gain the cooperation of others | Applicable |
| Can support delivery of services or solutions in own capability group | Applicable |
| Contributes actively in team activities, sharing experience and ideas | Applicable |
| Draws upon colleagues’ expertise to deliver results. | Applicable |
| Establishes and maintains effective working relationships with others | Applicable |
| Gains agreements with peers and business partners to support ideas and uses sound rationale to explain the value of actions | Applicable |
| Listens to customer concerns to identify their core needs. | Applicable |
| Listens to others and leverages their input to improve service and products. | Applicable |
| Works co-operatively with other managers to achieve team goals | Applicable |
| Works effectively with colleagues to accomplish goals and drive change. | Applicable |
| Executes collection using appropriate strategies within the priorities established through the collection management process. | Applicable |
| Knowledge of multi-channel user access technologies and use cases including mobile technology. | Applicable |
| Ability to decrypt digital data collections. | Applicable |
| Knowledge of anti-forensics tactics, techniques, and procedures (TTPs). | Applicable |
| Knowledge of common forensic tool configuration and support applications (e.g., VMware, Wireshark). | Applicable |
| Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools. | Applicable |
| Knowledge of data carving tools and techniques (e.g., Foremost). | Applicable |
| Knowledge of deployable forensics. | Applicable |
| Knowledge of investigative implications of hardware, operating systems, and network technologies. | Applicable |
| Knowledge of server diagnostic tools and fault identification techniques. | Applicable |
| Knowledge of types and collection of persistent data. | Applicable |
| Knowledge of types of digital forensics data and how to recognize them. | Applicable |
| Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files. | Applicable |
| Skill in analyzing volatile data. | Applicable |
| Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems). | Applicable |
| Skill in developing and executing technical training programs and curricula. | Applicable |
| Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics). | Applicable |
| Skill in identifying forensic footprints. | Applicable |
| Skill in preserving evidence integrity according to standard operating procedures or national standards. | Applicable |
| Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, Forensic Tool Kit [FTK]). | Applicable |
| Knowledge of basic concepts and practices of processing digital forensic data | Applicable |
| Knowledge of machine learning | Applicable |
| Knowledge of statistical methods | Applicable |
| Skill In data presentation and visual analytics | Applicable |
| Skill in experimental design | Applicable |
| Skill in pattern recognition and anomaly detection | Applicable |
| Skill in working with structured data | Applicable |
| Skill in working with unstructured data | Applicable |
| Knowledge of interpreted and compiled computer languages. | Applicable |
| Knowledge of low-level computer languages (e.g., assembly languages). | Applicable |
| Knowledge of programming language structures and logic. | Applicable |
| Knowledge of secure coding technologies. | Applicable |
| Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep). | Applicable |
| Skill in identifying common encoding techniques (e.g., Exclusive Disjunction [XOR], American Standard Code for Information Interchange [ASCII], Unicode, Base64, Uuencode, Uniform Resource Locator [URL] encode). | Applicable |
| Skill in reading Hexadecimal data. | Applicable |
| Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump). | Applicable |
| Skill in writing code that is compatible with legacy code (e.g., Common Business-Oriented Language [COBOL], FORTRAN IV) in a modern programming language (e.g., Java, C++). | Applicable |
| Knowledge of application development languages and scripting languages | Applicable |
| Skill in multiple application development and scripting languages (e.g. Java, C.net, Objective C, SQL, HTML, XML …) | Applicable |
| Skill in programming or development in at least one of the following languages: .NET (ASP.NET), Java, Perl, Python, Ruby, C/C++/ObjectiveC | Applicable |
| Skill in writing SQL queries to generate custom reports | Applicable |
| Skill with application security on multiple technology platforms (e.g. J2SE, Struts/Spring, SQL, SSO, HTML5, etc…) | Applicable |
| Skill with OSS (Open Source Software), must have extensive experience in Java technology, frameworks and security. | Applicable |
| Ability to apply supply chain risk management standards. | Applicable |
| Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/regulations. | Applicable |
| Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities). | Applicable |
| Knowledge of common attack vectors on the network layer. | Applicable |
| Knowledge of content development. | Applicable |
| Knowledge of cyber defense mitigation techniques and vulnerability assessment tools, including open source tools, and their capabilities. | Applicable |
| Knowledge of cyber defense policies, procedures, and regulations. | Applicable |
| Knowledge of defense-in-depth principles and network security architecture. | Applicable |
| Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution). | Applicable |
| Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored]). | Applicable |
| Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks). | Applicable |
| Knowledge of intrusion detection methodologies and techniques for detecting host-and network-based intrusions via intrusion detection technologies. | Applicable |
| Knowledge of Intrusion Detection System (IDS) tools and applications. | Applicable |
| Knowledge of malware analysis concepts and methodology. | Applicable |
| Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro). | Applicable |
| Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing). | Applicable |
| Knowledge of the types of Intrusion Detection System (IDS) hardware and software. | Applicable |
| Knowledge of virtual machine aware malware, debugger aware malware, and packing. | Applicable |
| Skill in analyzing anomalous code as malicious or benign. | Applicable |
| Skill in collecting data from a variety of cyber defense resources. | Applicable |
| Skill in deep analysis of captured malicious code (e.g., malware forensics). | Applicable |
| Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort). | Applicable |
| Skill in identifying obfuscation techniques. | Applicable |
| Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures (TTP). | Applicable |
| Skill in mimicking threat behaviors. | Applicable |
| Skill in protecting a network against malware. | Applicable |
| Skill in tuning sensors. | Applicable |
| Skill of identifying capturing, containing, and reporting malware. | Applicable |
| Knowledge of malware packing and obfuscation techniques | Applicable |
| Skill in conducting information searches. | Applicable |
| Skill in the basic operation of computers. | Applicable |
| Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., central processing units [CPUs], network interface cards [NICs], data storage). | Applicable |
| Knowledge of circuit analysis. | Applicable |
| Knowledge of microprocessors. | Applicable |
| Skill in physically disassembling personal computers (PCs). | Applicable |
| Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system. | Applicable |
| Knowledge of collection management processes, capabilities, and limitations. | Applicable |
| Knowledge of secure configuration management techniques. | Applicable |
| Skill in configuring and utilizing hardware-based computer protection components (e.g., hardware firewalls, servers, routers). | Applicable |
| Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs]). | Applicable |
| Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware). | Applicable |
| Knowledge of critical information technology (IT) procurement requirements. | Applicable |
| Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes). | Applicable |
| Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk. | Applicable |
| Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management). | Applicable |
| Skill in evaluating the trustworthiness of the supplier and/or product. | Applicable |
| Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed. | Applicable |
| Knowledge of electronic evidence law. | Applicable |
| Knowledge of International Traffic in Arms Regulation (ITARs) and relevance to cybersecurity. |  |
| Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence). | Applicable |
| Knowledge of legal rules of evidence and court procedure. | Applicable |
| Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. | Applicable |
| Knowledge of relevant laws, policies, procedures, or governance related to work impacting critical infrastructure. | Applicable |
| Knowledge of online banking and pertinent US regulations | Applicable |
| Knowledge of cryptography and cryptographic key management concepts. | Applicable |
| Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]). | Applicable |
| Knowledge of encryption methodologies. | Applicable |
| Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities. | Applicable |
| Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed operational plans and orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations. | Applicable |
| Ability to interpret and incorporate data from multiple tool sources. | Applicable |
| Knowledge of concepts and practices of processing digital forensic data. | Applicable |
| Knowledge of data administration and data standardization policies and standards. | Applicable |
| Knowledge of data classification standards and methodologies based on sensitivity and other risk factors. | Applicable |
| Knowledge of data mining and data warehousing principles. | Applicable |
| Knowledge of database theory. | Applicable |
| Knowledge of sources, characteristics, and uses of the organization’s data assets. | Applicable |
| Knowledge of the capabilities and functionality associated with various technologies for organizing and managing information (e.g., databases, bookmarking engines). | Applicable |
| Knowledge of the characteristics of physical and virtual data storage media. | Applicable |
| Skill in data mining techniques. | Applicable |
| Skill in developing data dictionaries. | Applicable |
| Skill in developing data repositories. | Applicable |
| Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Direct Algorithm [MD5]). | Applicable |
| Skills in data reduction. | Applicable |
| Knowledge of database structure and queries | Applicable |
| Skill in Extract Transform Load (ETL) processes | Applicable |
| Knowledge of advanced data remediation security features in databases. | Applicable |
| Skill in allocating storage capacity in the design of data management systems. | Applicable |
| Skill in designing databases. | Applicable |
| Skill in optimizing database performance. | Applicable |
| Knowledge of advanced data encryption (e.g., Column and Tablespace Encryption) security features in databases, including built-in cryptographic key management features. | Applicable |
| Knowledge of database management systems, query languages, table relationships, and views. | Applicable |
| Knowledge of database systems. | Applicable |
| Knowledge of Java-based database access application programming interface (API) (e.g., Java Database Connectivity [JDBC]). | Applicable |
| Knowledge of query languages such as Structured Query Language (SQL). | Applicable |
| Skill in conducting queries and developing algorithms to analyze data structures. | Applicable |
| Skill in generating queries and reports. | Applicable |
| Skill in maintaining databases. | Applicable |
| Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration. | Applicable |
| Knowledge of embedded systems and internet of things. | Applicable |
| Knowledge of digital rights management. | Applicable |
| Knowledge of symmetric key rotation techniques and concepts. | Applicable |
| Knowledge of Virtual Private Network (VPN) security. | Applicable |
| Skill in using Public-Key Infrastructure (PKI) Software Development Kit (SDK) to add encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic). | Applicable |
| Skill in using Virtual Private Network (VPN) devices and encryption. | Applicable |
| Knowledge of enterprise messaging systems and associated software. | Applicable |
| Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]). | Updated |
| Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model). | Applicable |
| Knowledge of the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DODAF], Federal Enterprise Architecture Framework [FEAF]). | Applicable |
| Knowledge of the nature and function of the relevant information structure. | Applicable |
| Knowledge of the organization’s enterprise information technology (IT) goals and objectives. | Applicable |
| Accepts responsibility for own decisions and actions. | Applicable |
| Acts with highest level of integrity, generating trust and protecting client interests | Applicable |
| Adheres to all Bank and FRS policies, bulletins and ethical guidelines. | Not Applicable |
| Demonstrates a consistency between actions and words. | Applicable |
| Follows set processes and methods | Applicable |
| Follows through on commitments | Applicable |
| Analyzes collected information to identify vulnerabilities and potential for exploitation. | Applicable |
| Knowledge of external organizations and academic institutions dealing with cybersecurity issues. | Applicable |
| Knowledge of social dynamics of computer attackers in a global context. | Applicable |
| Knowledge of Theories of Crime | Applicable |
| Knowledge of Underground Economy | Applicable |
| Knowledge of Financial Industry Investment Banking Products and Processing (i.e. Equities, FX, Fixed Assets, Derivatives) | Not Applicable |
| Knowledge of Financial Industry Payments Systems (i.e. Cash, Credit Cards) | Not Applicable |
| Knowledge of regulatory bodies and their responsibilities (FCC, FTC, SEC, etc.) | Updated |
| Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody). | Applicable |
| Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. | Applicable |
| Skill in setting up a forensic workstation. | Applicable |
| Knowledge of Human Factors/Digital Ergonomics | Applicable |
| Establishes relationships with and learns more about associates from other countries, cultures and backgrounds | Applicable |
| Keeps current on key economic, social and political trends throughout the world and their potential impact on business | Applicable |
| Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware. | Applicable |
| Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs]). | Applicable |
| Knowledge of network hardware devices and functions. | Applicable |
| Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware. | Applicable |
| Knowledge of human-computer interaction principles. | Applicable |
| Skill in the use of social engineering techniques. | Applicable |
| Knowledge of authentication, authorization, and access control methods. | Applicable |
| Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]). | Applicable |
| Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control). | Applicable |
| Knowledge of policy-based and risk-adaptive access controls. | Applicable |
| Skill in developing and applying security system access controls. | Applicable |
| Skill in developing and applying user credential management system. | Applicable |
| Skill in maintaining directory services. | Applicable |
| Knowledge of database procedures used for documenting and querying reported incidents. | Applicable |
| Knowledge of disaster recovery and continuity of operations plans. | Applicable |
| Knowledge of enterprise incident response program, roles, and responsibilities. | Applicable |
| Knowledge of incident categories, incident responses, and timelines for responses. | Applicable |
| Knowledge of incident response and handling methodologies. | Applicable |
| Knowledge of root cause analysis for incidents. | Applicable |
| Skill in performing root cause analysis for incidents. | Applicable |
| Skill in recovering failed servers. | Applicable |
| Skill in using incident handling methodologies. | Applicable |
| Knowledge of fault tolerance. | Applicable |
| Knowledge of information assurance (IA) principles and methods that apply to software development. | Applicable |
| Knowledge of information assurance (IA) principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data. | Applicable |
| Knowledge of information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data. | Applicable |
| Knowledge of key concepts in security management (e.g., Release Management, Patch Management). | Applicable |
| Knowledge of organization's enterprise information security architecture system. | Applicable |
| Knowledge of parallel and distributed computing concepts. | Applicable |
| Knowledge of the Security Assessment and Authorization (SA&A) process. | Applicable |
| Skill in applying confidentiality, integrity, and availability principles. | Applicable |
| Skill in designing security controls based on information assurance (IA) principles and tenets. | Applicable |
| Skill in determining how a security system should work, including its resilience and dependability capabilities, and how changes in conditions, operations, or the environment will affect these outcomes. | Applicable |
| Skill in developing, testing, and implementing network infrastructure contingency and recovery plans. | Applicable |
| Skill in performing damage assessments. | Applicable |
| Skill in recognizing and categorizing types of vulnerabilities and associated attacks. | Applicable |
| Skill in securing network communications. | Applicable |
| Knowledge of frameworks for authorization and entitlement management (e.x. EPV, SSO, etc) | Applicable |
| Knowledge of an organization's information classification program and procedures for level information loss. | Applicable |
| Knowledge of Risk Management Framework (RMF) requirements. | Applicable |
| Skill in creating policies that reflect system security objectives. | Applicable |
| \* Knowledge of cybersecurity principles. | Applicable |
| Knowledge of basic system administration, network, and operating system hardening techniques. | Applicable |
| Knowledge of current and emerging threats/threat vectors. | Applicable |
| Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities. | Applicable |
| Knowledge of front-end collection systems, including network traffic collection, filtering, and selection. | Applicable |
| Knowledge of host and network access control mechanisms (e.g., access control list). | Applicable |
| Knowledge of information security systems engineering principles. | Applicable |
| Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption). | Applicable |
| Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins. | Applicable |
| Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth). | Applicable |
| Knowledge of network traffic analysis methods. | Applicable |
| Knowledge of security event correlation tools. | Applicable |
| Knowledge of security system design tools, methods, and techniques. | Applicable |
| Knowledge of signature implementation impact. | Applicable |
| Knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization). | Applicable |
| Knowledge of the Enterprise Network Defense (END) provider reporting structure and processes within one’s own organization. | Applicable |
| Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities. | Applicable |
| Skill in developing and deploying signatures. | Applicable |
| Skill in discerning the protection needs (i.e., security controls) of information systems and networks. | Applicable |
| Skill in implementing, maintaining, and improving established security practices. | Applicable |
| Skill in reading and interpreting signatures (e.g., Snort). | Applicable |
| Demonstrated capability of designing and implementing global best practices and processes | Applicable |
| Knowledge of Security Design Patterns for Applications | Applicable |
| Knowledge of user access methods and privilege activity | Applicable |
| Skill with security technologies such as Firewalls, IDS/IPS, Web Proxies, DLP, etc. | Applicable |
| Knowledge of information technology (IT) architectural concepts and frameworks. | Applicable |
| Knowledge of remote access technology concepts. | Applicable |
| Knowledge of the enterprise information technology (IT) architecture. | Applicable |
| Knowledge of security architecture frameworks | Applicable |
| Skill in application, data, and infrastructure architecture disciplines. | Applicable |
| Skill in architecture and design across multiple systems | Applicable |
| Knowledge of measures or indicators of system performance and availability. | Applicable |
| Knowledge of performance tuning tools and techniques. | Applicable |
| Skill in conducting audits or reviews of technical systems. | Applicable |
| Skill in identifying and anticipating server performance, availability, capacity, or configuration problems. | Applicable |
| Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system. | Applicable |
| Skill in monitoring and optimizing server performance. | Applicable |
| \* Knowledge of computer networking concepts and protocols, and network security methodologies. | Applicable |
| Knowledge of common network tools (e.g., ping, traceroute, nslookup) and interpret the information results. | Applicable |
| Knowledge of common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications. | Applicable |
| Knowledge of communication methods, principles, and concepts (e.g., encoding, signaling, multiplexing) that support the network infrastructure. | Applicable |
| Knowledge of Extensible Markup Language (XML) schemas. | Applicable |
| Knowledge of how network services and protocols interact to provide network communications. | Applicable |
| Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI]). | Applicable |
| Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management. | Applicable |
| Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability. | Applicable |
| Knowledge of network design processes, including security objectives, operational objectives, and tradeoffs. | Applicable |
| Knowledge of network protocols (e.g., Transmission Critical Protocol/Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]), and directory services (e.g., Domain Name System [DNS]). | Applicable |
| Knowledge of networking protocols. | Applicable |
| Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways. | Applicable |
| Knowledge of use cases related to collaboration and content synchronization across platforms (e.g., tables, PC, Cloud, etc.). | Applicable |
| Skill in deploying Service Gateway at the network edge as the first point of contact or proxy into enterprise infrastructure handling layer 7 protocols (e.g., web, XML SOAP, REST, or legacy protocols [EDI]). | Applicable |
| Skill in establishing a routing schema. | Applicable |
| Skill in implementing enterprise key escrow systems to support data-at-rest encryption. | Applicable |
| Skill in installing, configuring, and troubleshooting local area network (LAN) and wide area network (WAN). | Applicable |
| Skill in network mapping and recreating network topologies. | Applicable |
| Skill in using sub-netting tools. | Applicable |
| Knowledge of Telephony | Updated |
| Identifies the possibility of new deals, extensions and ad-hoc service aspects | Applicable |
| Integrates information from a variety of sources, detects trends, associations and cause-effect relationships to drive actions | Applicable |
| Proposes innovations | Applicable |
| Knowledge of Capabilities and Maturity Model Integration (CMMI) at all five levels. | Applicable |
| Ability to match the appropriate knowledge repository technology for a given application or environment. | Applicable |
| Knowledge of knowledge-base capabilities for identifying the solutions to less common and more complex system problems. | Applicable |
| Skill in conducting knowledge mapping (e.g., map of knowledge repositories). | Applicable |
| Skill in conducting open source research for troubleshooting novel client-level problems (e.g., online development communities, system security blogging sites). | Applicable |
| Skill in the measuring and reporting of intellectual capital. | Applicable |
| Skill in using knowledge management technologies. | Applicable |
| \* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity. | Applicable |
| Ability to determine impact of technology trend data on laws, regulations, and/or policies. | Applicable |
| Knowledge of Import/Export Regulations related to cryptography and other security technologies. | Applicable |
| Skill in tracking and analyzing technical and legal trends that will impact cyber activities. | Applicable |
| Knowledge of industry-standard and organizationally accepted analysis principles and methods. | Applicable |
| Knowledge of process engineering concepts. | Applicable |
| Knowledge of structured analysis principles and methods. | Applicable |
| Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools. | Applicable |
| Knowledge of computer algorithms. | Applicable |
| Knowledge of information theory, including source coding, channel coding, algorithm complexity theory, and data compression. | Applicable |
| Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics. | Applicable |
| Skill in creating and utilizing mathematical or statistical models. | Applicable |
| Skill in design modeling and building use cases (e.g., unified modeling language). | Applicable |
| Skill in developing data models. | Applicable |
| Knowledge and experience in the Instructional System Design (ISD) methodology. | Applicable |
| Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools. | Applicable |
| Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, v3 [ITIL]). | Applicable |
| Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, Voice over Internet Protocol [VoIP], Instant Messenger [IM], web forums, direct video broadcasts). | Applicable |
| Knowledge of the range of existing networks (e.g., Private Branching Exchange [PBX], Local Area Networks [LANs], Wide Area Networks [WANs], Wireless Fidelity [WI-FI]). | Applicable |
| Knowledge of Wireless Fidelity (WI-FI). | Remove - redundant |
| Skill in applying host/network access controls (e.g., access control list). | Applicable |
| Skill in conducting server planning, management, and maintenance. | Applicable |
| Skill in correcting physical and technical problems that impact server performance. | Applicable |
| Skill in diagnosing connectivity problems. | Applicable |
| Skill in diagnosing failed servers. | Applicable |
| Skill in testing and configuring network workstations and peripherals. | Applicable |
| Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol). | Applicable |
| Knowledge of complex data structures. | Applicable |
| Knowledge of computer programming principles such as object-oriented design. | Applicable |
| Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip). | Applicable |
| Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]). | Applicable |
| Knowledge of how to troubleshoot basic systems and identify operating systems-related issues. | Applicable |
| Knowledge of operating systems. | Applicable |
| Knowledge of server and client operating systems. | Applicable |
| Knowledge of systems administration concepts. | Applicable |
| Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications). | Applicable |
| Knowledge of virtualization technologies and virtual machine development and maintenance. | Applicable |
| Knowledge of Windows and Unix ports and services. | Applicable |
| Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat). | Applicable |
| Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files). | Applicable |
| Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, Visual Basic Scripting [VBS]) on Windows and Unix systems (e.g., tasks such as parsing large data files, automating manual tasks, fetching/processing remote data). | Applicable |
| Skill in system administration for Unix/Linux operating systems. | Applicable |
| Skill in using virtual machines. | Applicable |
| Skill in utilizing virtual networks for testing. | Applicable |
| Knowledge of Android command line tools (e.g. adb). | Applicable |
| Knowledge of Authentication methods | Applicable |
| Knowledge of LINUX Boot Process | Applicable |
| Knowledge of Mac command line | Applicable |
| Knowledge of malware persistence methods | Applicable |
| Knowledge of operating systems (e.g., Windows, Unix/Linux, iOS, Android, etc) | Applicable |
| Knowledge of operating systems (ex. Windows, Unix/Linux, Mac OS, iOS, Android, etc.) boot process including a through understanding of the execution flow of boot time processes | Updated |
| Knowledge of Root-Kit design, techniques, and hiding strategies | Applicable |
| Knowledge of Solaris Boot Process | Applicable |
| Knowledge of the Android operating system | Applicable |
| Knowledge of the Apple iOS operating system | Applicable |
| Knowledge of Windows Boot Process | Applicable |
| Knowledge of windows process injection techniques | Applicable |
| Skill in identifying, modifying, and manipulating applicable system components (iOS or Android) (e.g., passwords, user accounts, files) | Applicable |
| Skill in identifying, modifying, and manipulating applicable system components (Windows, Unix/Linux, Mac OS/OS X, iOS and/or Android) | Updated |
| Knowledge of service catalogues and service management standards (e.g., Information Technology Infrastructure Library, v3 [ITIL]). | Applicable |
| Skill in talking to others to convey information effectively. | Applicable |
| Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportable criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions. | Applicable |
| Knowledge of the organization's core business/mission processes. | Applicable |
| Knowledge of the structure and intent of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement. | Applicable |
| Knowledge of Privacy Impact Assessments (PIA). | Applicable |
| Skill in deconflicting cyber operations and activities. | Applicable |
| Arrives at sound conclusions and recommendations based on business goals data, and practical constraints. | Applicable |
| Considers alternatives, implements decisions, and evaluates their effectiveness. | Applicable |
| Demonstrates urgency and timeliness when dealing with critical issues or people. | Applicable |
| Identifies efficiency improvements | Applicable |
| Identifies problems and appreciates the issues required to resolve them | Applicable |
| Organizes resources effectively to meet demands of projects. | Applicable |
| Resolves issues quickly and effectively, in a way that mitigates repeat inquiries. | Applicable |
| Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services and CMMI for Acquisitions). | Applicable |
| Actively identifies new areas for learning and regularly created and takes advantage of learning opportunities | Applicable |
| Acts courteously and professionally when dealing with customers. | Applicable |
| Consistently meets expected results within deadlines | Applicable |
| Follows-up to ensure satisfactory service and complete problem resolution. | Applicable |
| Gets all things done on a timely basis | Applicable |
| Is courteous and helpful when responding to requests, even if urgent or unplanned. | Applicable |
| Maintains composure during pressured/stressful situations. | Applicable |
| Maintains records as required for the project or service | Applicable |
| Places a priority on attending to the needs and inquiries from internal and external customers. | Applicable |
| Remains self-disciplined and prevent irrelevant issues or distractions from interfering with the timely completion of important tasks | Applicable |
| Takes action that goes beyond job requirements in order to achieve objectives | Applicable |
| Tracks and directs own workflow efficiently. | Applicable |
| Uses time and energy optimally to ensure delivery of all products and services. | Applicable |
| Knowledge of information security program management and project management principles and techniques. | Applicable |
| Knowledge of resource management principles and techniques. | Applicable |
| Knowledge of operations security. | Applicable |
| Skill in integrating black box security testing tools into quality assurance process of software releases. | Applicable |
| Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence. | Applicable |
| Skill in analyzing memory dumps to extract information. | Applicable |
| Skill in using scientific rules and methods to solve problems. | Applicable |
| Knowledge of Electronic Monetary Transaction Processes | Applicable |
| Ability to apply network programming towards client/server model. | Applicable |
| Ability to interpret and translate customer requirements into operational cyber actions. | Applicable |
| Knowledge of applicable business processes and operations of customer organizations. | Applicable |
| Knowledge of capabilities and requirements analysis. | Applicable |
| Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design. | Applicable |
| Skill in conducting capabilities and requirements analysis. | Applicable |
| Business process improvement mindset with a drive for controls, automation and efficiency | Applicable |
| \* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk). | Applicable |
| Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures. | Applicable |
| Knowledge of organization's risk tolerance and/or risk management approach. | Applicable |
| Knowledge of risk threat assessment. | Applicable |
| Knowledge of supply chain risk management standards, processes, and practices. | Applicable |
| Knowledge of threat assessment. | Applicable |
| Skill in building and running working groups to draft Policies and Standards, facilitate and capture feedback and negotiate mutually acceptable results. | Applicable |
| Skill in Policy & Standards writing (e.g. articulating regulatory/authoritative source and risk based requirements in non-subjective, unambiguous and succinct language. | Applicable |
| Risk management Governance (I.e. 3 layers of defense, CRO office, RCSA process) | Applicable |
| Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards. | Applicable |
| Knowledge of processes for reporting network security related incidents. | Applicable |
| Knowledge of debugging procedures and tools. | Applicable |
| Knowledge of middleware (e.g., enterprise service bus and message queuing). | Applicable |
| Knowledge of software debugging principles. | Applicable |
| Knowledge of software design tools, methods, and techniques. | Applicable |
| Skill in conducting software debugging. | Applicable |
| Skill in developing applications that can log errors, exceptions, and application faults. | Applicable |
| Skill in using code analysis tools to eradicate bugs. | Applicable |
| Skill in writing kernel level applications. | Applicable |
| Knowledge of mobile application packaging procedures (e.g. package signatures) | Applicable |
| Knowledge of debugging procedures and tools | Applicable |
| Skill in the development and deployment of mobile applications. | Applicable |
| Knowledge of secure software deployment methodologies, tools, and practices. | Applicable |
| Knowledge of software development models (e.g., Waterfall Model, Spiral Model, Agile Model). | Applicable |
| Knowledge of software engineering. | Applicable |
| Knowledge of software quality assurance process. | Applicable |
| Skill in configuring and optimizing software. | Applicable |
| Ability to tailor code analysis for application-specific concerns. | Applicable |
| Skill in creating programs that validate and process multiple inputs, including command line arguments, environmental variables, and input streams. | Applicable |
| Communicates appropriately with people at various levels and backgrounds, even if they have differing viewpoints. | Applicable |
| Conveys information that is well organized and analytically sound. | Applicable |
| Demonstrates an understanding of culturally appropriate communication styles. | Applicable |
| Recognizes the need for additional information and asks questions to obtain it | Applicable |
| Tailors communication style for diverse audiences. | Applicable |
| Utilizes civil discourse techniques to effectively navigate conflict. | Updated |
| Appropriately delegates and monitors progress of assignments to staff. | Applicable |
| Contributes to recruitment activities | Applicable |
| Effectively enhances the development and ongoing performance of subordinates | Applicable |
| Ensures staff understands expectations and time-lines for assignments. | Applicable |
| Establishes good interpersonal relationships by helping people feel valued, appreciated , and included in discussions | Applicable |
| Exhibits strong management skills that are at least commensurate with the role | Updated |
| Is able to set tasks and direction for the team | Applicable |
| Is able to work through project plans to completion without continuous oversight or supervision. | Applicable |
| Maintains oversight and responsibility for staff’s projects. | Applicable |
| Provides constructive and timely feedback and coaching to staff. | Applicable |
| Works within the SLA or project plan | Applicable |
| Knowledge of hacking methodologies in Windows or Unix/Linux environment. | Applicable |
| Knowledge of how system components are installed, integrated, and optimized. | Applicable |
| Knowledge of principles and methods for integrating server components. | Applicable |
| Knowledge of technology integration processes. | Applicable |
| Skill in designing the integration of hardware and software solutions. | Applicable |
| Knowledge of server administration and systems engineering theories, concepts, and methods. | Applicable |
| Knowledge of system life cycle management principles, including software security and usability. | Applicable |
| Knowledge of the life cycle process. | Applicable |
| Knowledge of the operations and processes for diagnosing common or recurring system problems. | Applicable |
| Knowledge of the systems engineering process. | Applicable |
| Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly. | Applicable |
| Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation. | Applicable |
| Skill in installing computer and server upgrades. | Applicable |
| Knowledge of agency evaluation and validation requirements. | Applicable |
| Knowledge of organization's evaluation and validation requirements. | Applicable |
| Knowledge of system diagnostic tools and fault identification techniques. | Applicable |
| Knowledge of systems testing and evaluation methods. | Applicable |
| Skill in applying organization-specific systems analysis principles and techniques. | Applicable |
| Skill in conducting test events. | Applicable |
| Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data). | Applicable |
| Skill in determining an appropriate level of test rigor for a given system. | Applicable |
| Skill in developing operations-based testing scenarios. | Applicable |
| Skill in evaluating test plans for applicability and completeness. | Applicable |
| Skill in secure test plan design (i.e., unit, integration, system, acceptance). | Applicable |
| Skill in systems integration testing. | Applicable |
| Skill in writing test plans. | Applicable |
| Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies. | Applicable |
| Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience. | Applicable |
| Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures. | Applicable |
| Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain. | Applicable |
| Skill in identifying gaps in technical capabilities. | Applicable |
| Ability to determine the validity of technology trend data. | Applicable |
| Knowledge of emerging computer-based technology that has potential for exploitation by adversaries. | Applicable |
| Knowledge of emerging security issues, risks, and vulnerabilities. | Applicable |
| Knowledge of key industry indicators that are useful for identifying technology trends. | Applicable |
| Knowledge of new and emerging Information Technology (IT) and cyber security technologies. | Applicable |
| Knowledge of new technological developments in server administration. | Applicable |
| Knowledge of products and nomenclature of major vendors (e.g., security suites: Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky, etc.) and how differences affect exploitation/vulnerabilities. | Applicable |
| Knowledge of the capabilities and functionality associated with various content creation technologies (e.g., wikis, social networking, blogs). | Applicable |
| Knowledge of the capabilities and functionality of various collaborative technologies (e.g., groupware, SharePoint). | Applicable |
| Skill in applying and incorporating information technologies into proposed solutions. | Applicable |
| Awareness and use of technology relevant to role and service provided | Applicable |
| Awareness of at least one vendor solution or security tool relevant to services or solutions in own capability group | Applicable |
| Awareness of other vendor solutions or tools | Applicable |
| Awareness of services and solutions in own capability group | Applicable |
| Can articulate at least one vendor solution or tool relevant to services or solutions in own capability group | Applicable |
| Competent in the use of own technology area for client and Company benefit | Applicable |
| Demonstrates an interest in associated technologies | Applicable |
| Has completed training on at least one vendor solution or tool relevant to services or solutions in own capability group | Applicable |
| Is aware of company and own area business plans | Applicable |
| Understands one method associated with services or solutions in own capability group | Not applicable |
| Knowledge of basic concepts, terminology, and operations of a wide range of communications media (e.g., computer and telephone networks, satellite, fiber, wireless). | Applicable |
| Knowledge of different types of network communication (e.g., Local Area Network [LAN], Wide Area Network [WAN], Metropolitan Area Network [MAN], Wireless Local Area Network [WLAN], Wireless Wide Area Network [WWAN]). | Applicable |
| Knowledge of Global Systems for Mobile communications (GSM) architecture. | Applicable |
| Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise. | Applicable |
| Knowledge of key telecommunication concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers). | Applicable |
| Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure [NII]). | Applicable |
| Knowledge of Voice over Internet Protocol (VoIP). | Applicable |
| Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities. Produces findings to help initialize or support law enforcement and counterintelligence investigations or activities. | Applicable |
| Able to communicate a point demonstrating logic, reasoning, and soundness of argument. | Applicable |
| Demonstrates culturally-inclusive communication. | Applicable |
| Demonstrates effective active listening skills (paraphrasing, clarifying, perception checking, summarizing). | Applicable |
| Utilizes non-verbal techniques appropriate to the context of communication. | Applicable |
| \* Knowledge of cyber threats and vulnerabilities. | Applicable |
| Ability to identify systemic security issues based on the analysis of vulnerability and configuration data. | Applicable |
| Knowledge of application vulnerabilities. | Applicable |
| Knowledge of hardware reverse engineering techniques. | Applicable |
| Knowledge of how different file types can be used for anomalous behavior. | Applicable |
| Knowledge of packet-level analysis. | Applicable |
| Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit). | Applicable |
| Knowledge of reverse engineering concepts. | Applicable |
| Knowledge of software reverse engineering techniques. | Applicable |
| Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code). | Applicable |
| Knowledge of system and application security threats and vulnerabilities. | Applicable |
| Skill in assessing the robustness of security systems and designs. | Applicable |
| Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems. | Applicable |
| Skill in designing countermeasures to identified security risks. | Applicable |
| Skill in evaluating the adequacy of security designs. | Applicable |
| Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). | Applicable |
| Skill in the use of penetration testing tools and techniques. | Applicable |
| Skill in using network analysis tools to identify vulnerabilities. | Applicable |
| Skill in using protocol analyzers. | Applicable |
| Skill in utilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (e.g., penetration and testing). | Applicable |
| Skill in utilizing network analysis tools to identify software communications vulnerabilities. | Applicable |
| Knowledge of hacking methodologies in Windows or Unix/Linux environment | Applicable |
| Knowledge of OWASP Security Remediation Framework Projects (ESAPI, AntiSamy, CSRFGuard) | Applicable |
| Knowledge of OWASP Top 10 and other web and mobile application security taxonomy | Applicable |
| Skill in CVSS, CVE and related schema and scoring. | Applicable |
| Skill in establishing and optimizing service models, defining and measuring to SLA/KPIs. | Updated |
| Skill in implementation programs for supply chain security, vBSIMM and Binary code scanning. | Applicable |
| Skill in interpreting log output from networking devices, operating systems and infrastructure services | Applicable |
| Skill in remediation of application vulnerabilities (e.g. OWASP Top 10 application security risks) | Applicable |
| Skill in reviewing raw log files, data correlation, and analysis (i.e. firewall, network flow, IDS, system logs) | Applicable |
| Skill in security testing program management and development | Applicable |
| Skill in the use of penetration testing tools and techniques in regards to Mobile application assessments | Applicable |
| Skill in Threat Modeling methodologies and approaches such as STRIDE, Attack Trees… | Applicable |
| Skill in using static code analysis tools principles and practices (i.e. HP Fortify, IBM Appscan Resource, Pylint, RATS, Veracode, The Black Duck Suite). | Applicable |
| Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi]. paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly. | Applicable |
| Knowledge of web filtering technologies. | Applicable |
| Knowledge of web services, including service oriented architecture, Simple Object Access Protocol (SOAP), and web service description language. | Applicable |
| Knowledge of webmail collection, searching/analyzing techniques, tools, and cookies. | Applicable |
| Adapts writing style and content to fit mode of messaging (sales, email, supervision, or short/long form reporting). | Applicable |
| Demonstrates a mastery of language structure and syntax through formal and informal writing. | Applicable |
| Utilizes a strong vocabulary for precise description. | Applicable |
|  |  |
| **New Communications specific KSAs submitted from Working Group** |  |
|  |  |
| Knowledge of cyber incident information sharing protocols such as STIX, TAXII and CybOX | Applicable |
| General understanding of technology trends and emerging standards in the Cyber Security domain | Applicable |
| Understands unique Workforce Development for Cyber security professionals | Applicable |
| Knowledge of various network architectures including near field communications, DAS, LTE, etc. | Applicable |
| Knowledge of impact to network architectures and management techniques as a result of NFV, SDN, and CDN | Applicable |
| Skill in installing, configuring and trouble shooting Telco network core components (ENodeB, Gateways, Session Border Controllers, HSS, etc.) | Applicable |
| Knowledge of NFV, CDN, virtual machines, SDN, and other emerging technologies and their impact to architecture and design | Applicable |
| Knowledge of legal constraints associated with collection of PII and CPNI data and the release of that data | Applicable |
| Skill with OSS (Open Source Software), must have extensive experience in understanding OSS agreements and implications of usage | Applicable |
| Skill with OSS (Open Source Software), must have extensive experience in working with OSS license management tools such as Black Duck software | Applicable |
| Knowledge of telecommunications specific networking protocols, platforms (e.g., SS7, UMTS, LTE, EPC, eNodeB, etc.) and services (e.g., HLR, HSS, PCRF, etc.) and how they interact to provide network communications. | Applicable |
| Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Signaling System 7, MPLS, LTE, UMTS, etc.) subject to the network type and protocol. | Applicable |
| Knowledge of the structure and intent of business operation plans, concept operation plans, orders, and policies. | Applicable |

**Appendix 2 – National Cybersecurity Workforce Framework Communications Sector Recommended Categories, Specialties and Competencies**

| **Category** | **Specialty** | **Competency** |
| --- | --- | --- |
| Cybersecurity - Securely Provision | Secure Acquisition | Capacity Management |
| Cybersecurity - Operate and Maintain | Secure Software Engineering | Communications Security Management |
| Cybersecurity - Protect and Defend | Systems Security Architecture | Computer Forensics |
| Cybersecurity - Investigate | Technology Research and Development | Computer Languages |
| Cybersecurity - Oversee and Govern | Systems Requirements Planning | Computer Network Defense |
| Cybersecurity - Collect and Operate | Test and Evaluation | Computer Skills |
| Cybersecurity - Analyze | Systems Development | Computers and Electronics |
| Essential Skills | Data Administration | Configuration Management |
|  | Customer Service and Technical Support | Contracting/Procurement |
|  | Network Services | Criminal Law |
|  | System Administration | Cryptography |
|  | Systems Security Analysis | Data Management |
|  | Enterprise Network Defense Analysis | Database Administration |
|  | Incident Response | Database Management Systems |
|  | Enterprise Network Defense Infrastructure Support | Distributed Systems |
|  | Vulnerability Assessment and Management | Embedded Computers |
|  | Digital Forensics | Encryption |
|  | Cyber Investigation | Enterprise Architecture |
|  | Legal Advice and Advocacy | External Awareness |
|  | Strategic Planning and Policy Development | Forensics |
|  | Training, Education, and Awareness | Hardware |
|  | Information Systems Security Operations | Hardware Engineering |
|  | Security Program Management | Human Factors |
|  | Risk Management | Identity Management |
|  | Knowledge Management | Incident Management |
|  | Public Safety | Information Assurance |
|  | EMS | Information Management |
|  | Radio Systems | Information Systems Security Certification |
|  | RF Engineering | Information Systems/Network Security |
|  |  | Information Technology Architecture |
|  |  | Information Technology Performance Assessment |
|  |  | Infrastructure Design |
|  |  | Internal Controls |
|  |  | Knowledge Management |
|  |  | Legal, Government, and Jurisprudence |
|  |  | Logical Systems Design |
|  |  | Mathematical Reasoning |
|  |  | Modeling and Simulation |
|  |  | Multimedia Technologies |
|  |  | Network Management |
|  |  | Object Technology |
|  |  | Operating Systems |
|  |  | Operations Support |
|  |  | Oral Communication |
|  |  | Organizational Awareness |
|  |  | Personnel Safety and Security |
|  |  | Political Savvy |
|  |  | Process Control |
|  |  | Project Management |
|  |  | Public Safety and Security |
|  |  | Quality Assurance |
|  |  | Reasoning |
|  |  | Requirements Analysis |
|  |  | Risk Management |
|  |  | Security |
|  |  | Software Development |
|  |  | Software Engineering |
|  |  | Software Testing and Evaluation |
|  |  | Surveillance |
|  |  | Systems Integration |
|  |  | Systems Life Cycle |
|  |  | Systems Testing and Evaluation |
|  |  | Teaching Others |
|  |  | Technology Awareness |
|  |  | Telecommunications |
|  |  | Vulnerabilities Assessment |
|  |  | Web Technology |
|  |  | Collection Operations |
|  |  | Cyber Operations |
|  |  | Cyber Operations Planning |
|  |  | All Source Intelligence |
|  |  | Exploitation Analysis |
|  |  | Targets |
|  |  | Threat Analysis |
|  |  | Advocacy |
|  |  | Analytics |
|  |  | Change Management |
|  |  | Coalition-Building |
|  |  | Ethical Decision-Making |
|  |  | Financial Industry Awareness |
|  |  | Global Awareness |
|  |  | Innovation and Creativity |
|  |  | Problem-Solving |
|  |  | Professionalism |
|  |  | Software Development / Engineering |
|  |  | Strategic Communication |
|  |  | Supervision |
|  |  | Verbal Communication |
|  |  | Written Communication |
|  |  | Geospatial Information Systems |
|  |  | - Technician/Cartographer |
|  |  | - Administrator |
|  |  | Public Information Relations |
|  |  | Training Coordinator |
|  |  | Radio Systems Operation/Technician |
|  |  | Public Safety Dispatcher/Call Taker |
|  |  | Senior Technical Coordinator (Public Safety) |
|  |  | Technical Support Specialist |
|  |  | Privacy (Statutes/Advocacy) |
|  |  |  |
|  |  | *Others:* |
|  |  | RF Engineering |

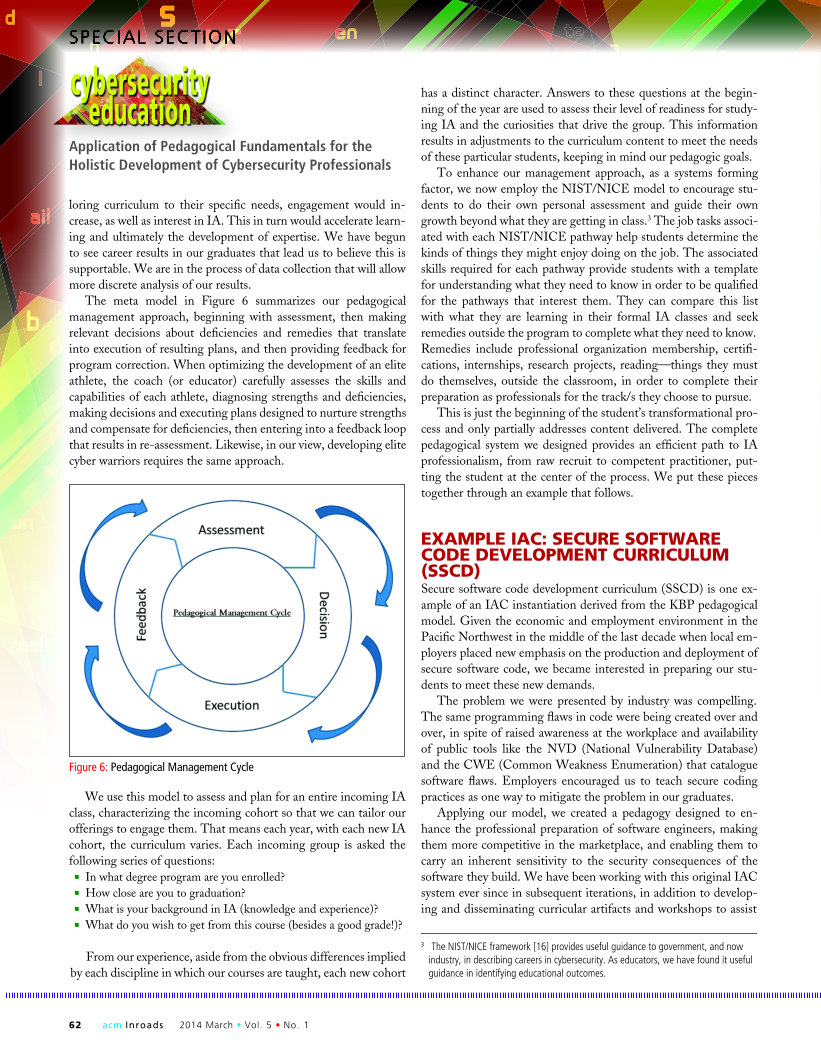
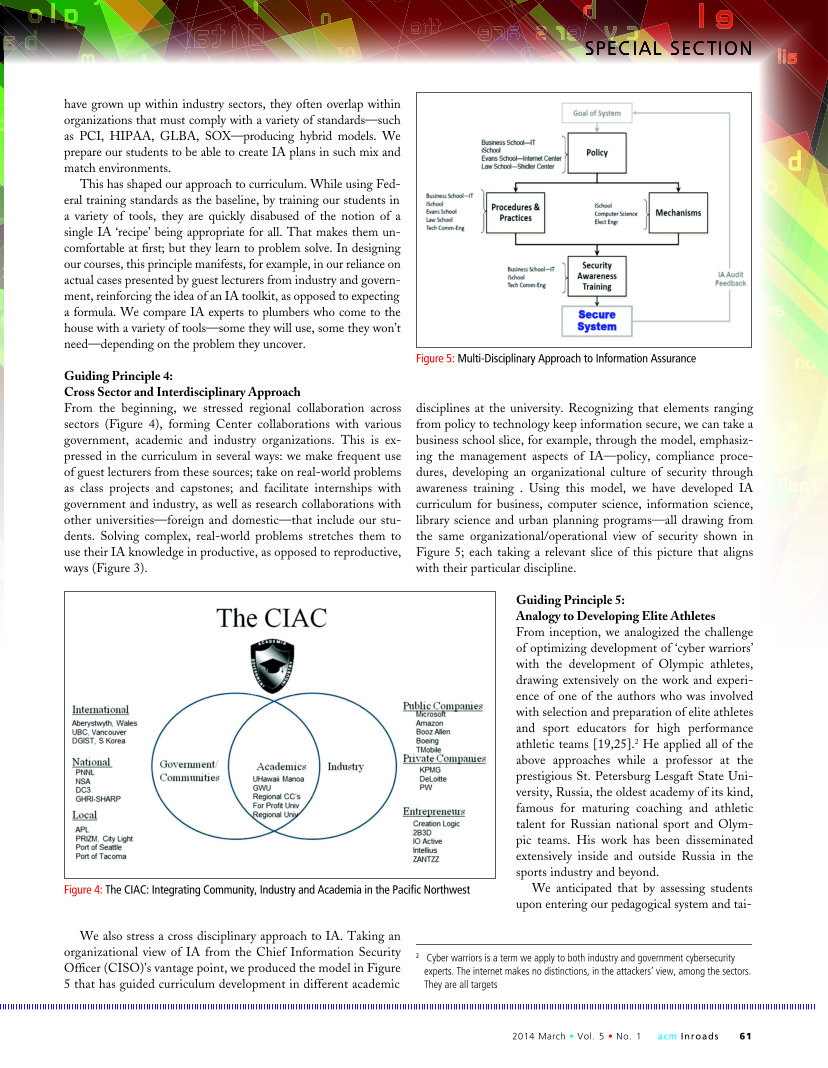
**Appendix 3 – Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals[[24]](#footnote-24)**

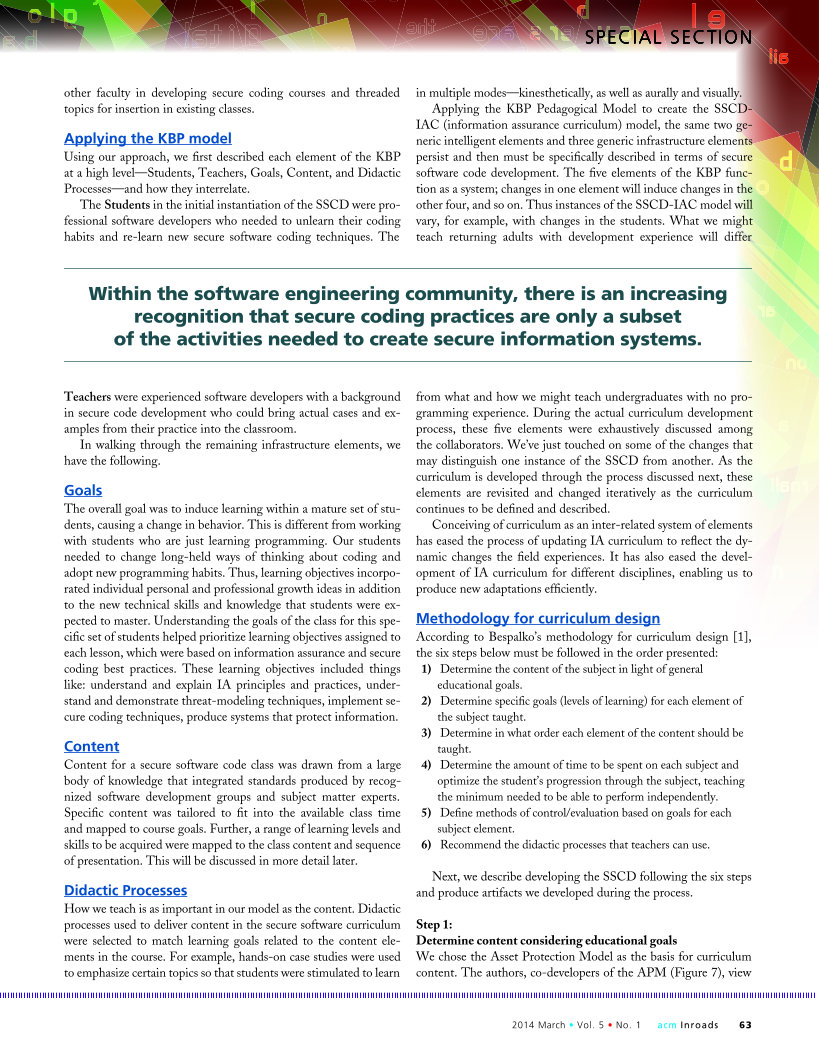


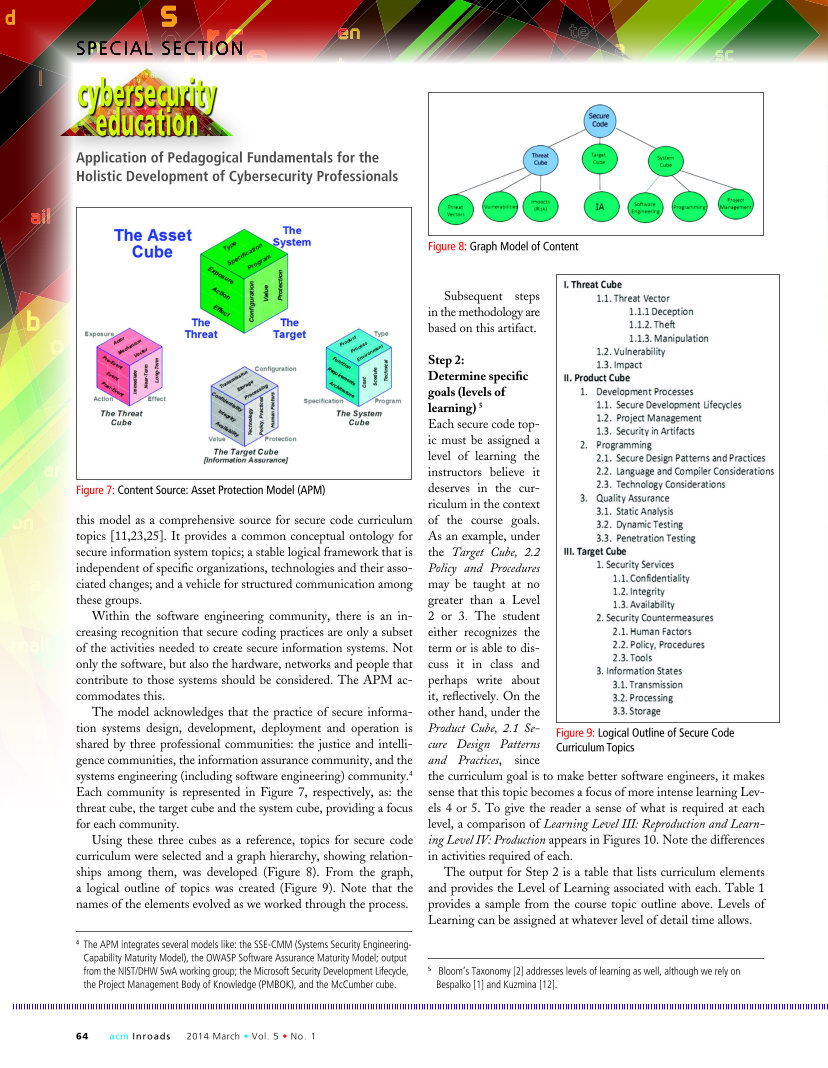


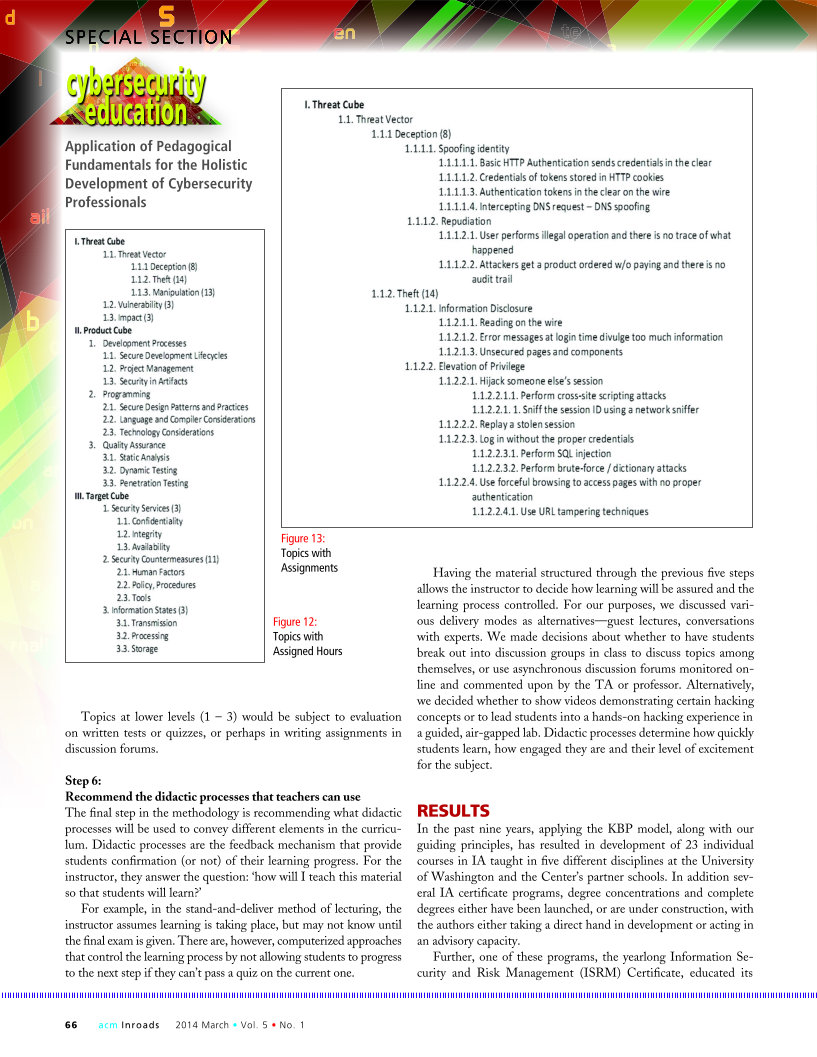




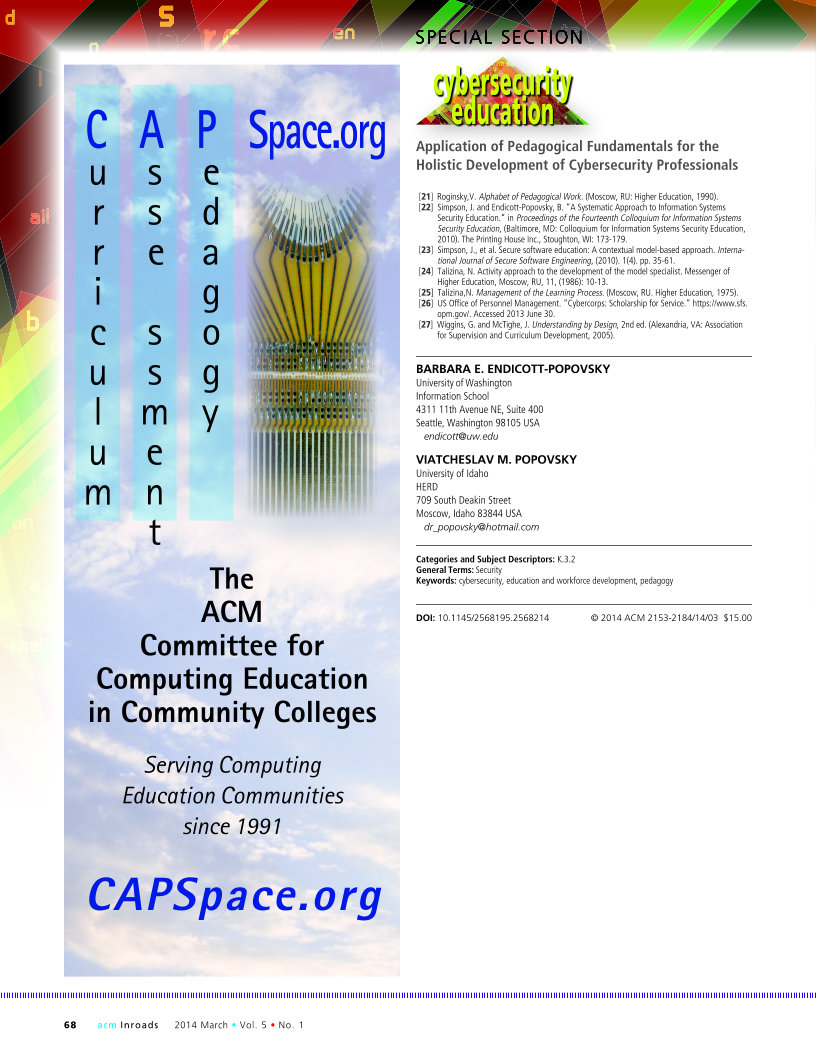












1. Cybersecurity Workforce Development Toolkit, How to Build a Strong Cybersecurity Workforce, https://niccs.us-cert.gov/ [↑](#footnote-ref-1)
2. Executive Order 13636 dated February 12, 2013 [↑](#footnote-ref-2)
3. Charter of the FCC’s Communications Security, Reliability and Interoperability Council [↑](#footnote-ref-3)
4. CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016 [↑](#footnote-ref-4)
5. 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 [↑](#footnote-ref-5)
6. https://niccs.us-cert.gov/training/tc/framework [↑](#footnote-ref-6)
7. Executive Order 13636 dated February 12, 2013 [↑](#footnote-ref-7)
8. http://csrc.nist.gov/nice/Sept2011-workshop/index.html [↑](#footnote-ref-8)
9. Charter of the FCC’s Communications Security, Reliability and Interoperability Council [↑](#footnote-ref-9)
10. CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016 [↑](#footnote-ref-10)
11. https://niccs.us-cert.gov/training/tc/framework [↑](#footnote-ref-11)
12. http://csrc.nist.gov/nice/ [↑](#footnote-ref-12)
13. https://niccs.us-cert.gov/careers/workforce-planning [↑](#footnote-ref-13)
14. CSRIC V Working Group Descriptions and Leadership, last updated, 1/27/2016 [↑](#footnote-ref-14)
15. 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 [↑](#footnote-ref-15)
16. Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals, Appendix 3 [↑](#footnote-ref-16)
17. Task Force on Optimal PSAP Architecture, Working Group 1, Optimal Cybersecurity Approach for PSAPs [↑](#footnote-ref-17)
18. http://www.nist.gov/cyberframework/index.cfm [↑](#footnote-ref-18)
19. Executive Order 13636 of February 12, 2013 [↑](#footnote-ref-19)
20. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf [↑](#footnote-ref-20)
21. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [↑](#footnote-ref-21)
22. 2014 Deloitte-NASCIO Cybersecurity Study – State governments at risk: Time to Move Forward, NASCIO Publications, October 2014 [↑](#footnote-ref-22)
23. <http://csrc.nist.gov/nice/nicewg.html> [↑](#footnote-ref-23)
24. Article published March 2014 in ACM Inroads [↑](#footnote-ref-24)