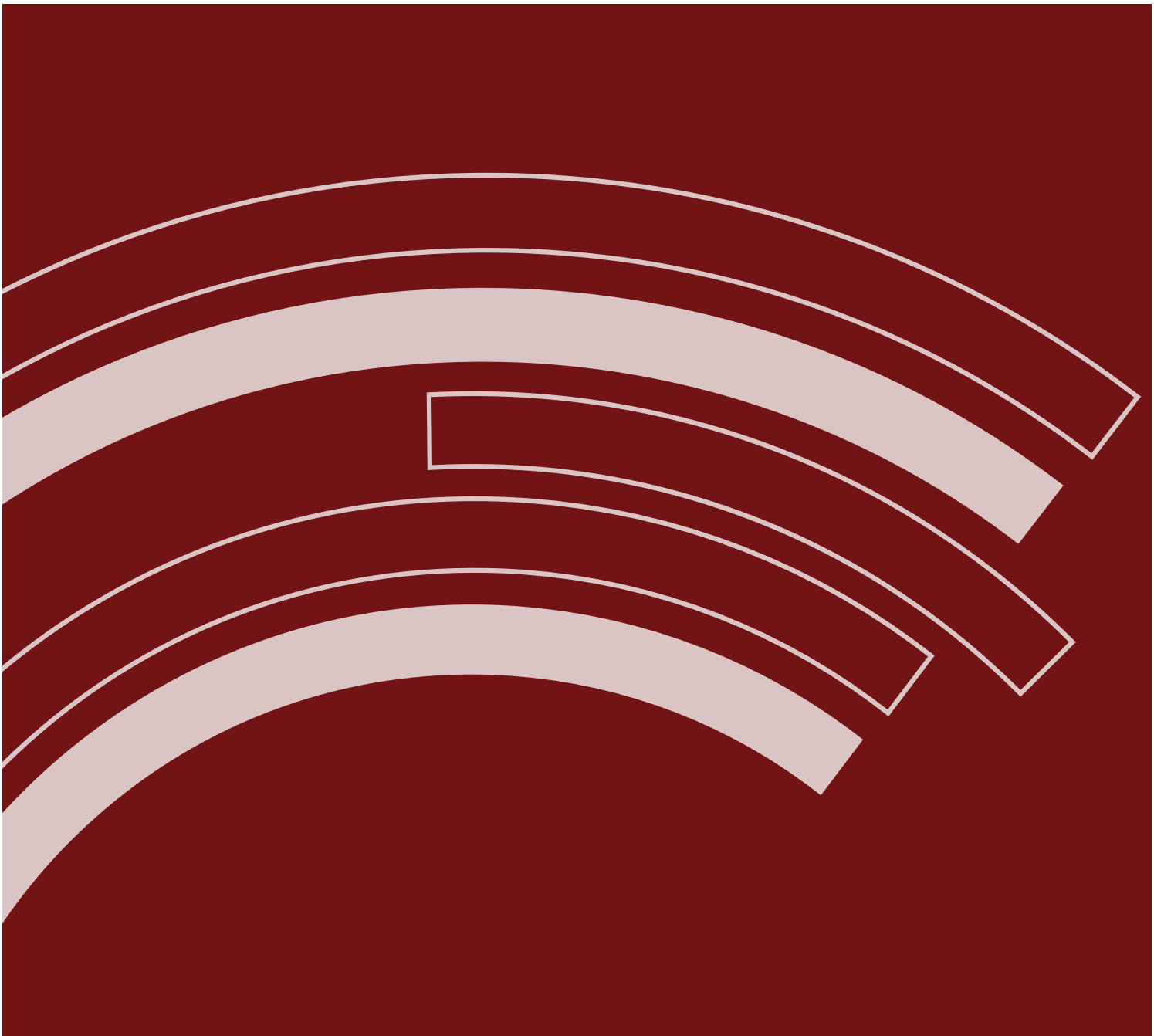
NATIONAL CYBERWATCH CENTER

CYBERSECURITY CORE CURRICULUM MAPPING REPORT

MAPPING OF THE NATIONAL CYBERWATCH CENTER'S CURRICULUM TO NATIONAL WORKFORCE COMPETENCY REQUIREMENTS

AUTHOR: **DR. DAVID H. TOBEY, DIRECTOR OF RESEARCH AND ASSESSMENTS, DECEMBER 2017**



Contents

INTRODUCTION

When the National CyberWatch Center started in 2005, quality Information Assurance curriculum was in short supply, so the development of new curriculum was a necessity. In 2006, the National CyberWatch Center, working in conjunction with Anne Arundel Community College, developed model Information Assurance and Computer Forensics curricula, which supported the growth of cybersecurity education nationally, including complete courses for degrees and multiple certificates.

Building on its model curriculum base, the National CyberWatch Center expanded the reach of cybersecurity education curriculum in several other ways, including the sharing of stackable credential models. These specialization certificates allow students to earn multiple certificates while pursuing their Associate's degree and to earn industry credentials by sitting for industry certification exams.

The following is at the heart of NCC's content-strategy:

- Up-to-date
- Focused on principles (e.g., Least Privilege, Simplicity of Design, Information Hiding, Resource Encapsulation, Process Isolation, Domain Separation, Modularity, Abstraction, and Layering)
- Performance-based
- Modular
- Aligned with job roles
- Mapped to federal and national standards (e.g., NICE Framework and NSA KUs)
- Sharable Content Object Reference Model (SCORM) compliant
- All Digital
- Aligned with industry certifications

In addition, NCC has also created course materials for some 25 technical courses that include some combination of the following: e-Books, lecture slides, hands-on lab exercises, assessment questions, instructor guides, and syllabi. These technical courses are used by hundreds of faculty throughout the U.S. in both undergraduate and graduate courses. See here (https://www.nationalcyberwatch.org/programs-resources/curriculum) for more information.

The Curriculum Standards Panel

In 2016, the National CyberWatch Center Curriculum Standards Panel (NCC- CSP) was established. Our mission is to help to identify the learning objectives, concepts, procedures, situational judgments, and intellective abilities required to develop capabilities maturity in cybersecurity foundational principles, techniques, tactics, and protocols.

The standards produced by the NCC-CSP are the first to align instructional design, skill practice facilities, cybersecurity professional job performance standards, national workforce frameworks, and industry needs. Currently over 100 faculty, industry professionals, and government representatives have volunteered to serve on subject matter expert panels for curriculum design. Additional panel members are recruited based on their expertise and instructional experience from 228 National CyberWatch Center member organizations (128 two-year and 100 four-year) and through alliances with industry and professional associations.

Developing a Competency-Based Curriculum for Cybersecurity

"Competency-based education stands out as the innovation most likely to disrupt higher education"

- Weise and Christensen (2014) Hire Education

Closing the growing cybersecurity skills gap may require disruptive innovation. The classic separation of learning and doing has persisted since the founding of the ancient *Greek Academy*. In the United States, university education is focused primarily on teaching *how to think*. Community college and professional education is focused on teaching *how to do* a particular job. However, professional capability maturity (for example, in law and medicine) depends upon integrating thinking and doing. Accordingly, the professions use the term practices to describe their organizations, acknowledging the central role of *doing* in learning how to apply knowledge to develop professional expertise. Education outside the U.S. began some time ago to integrate practice into education by aligning industry competency requirements into instructional designs (Craig, 2013; Higgs, 2013). Considering that just over one year ago *Forbes Magazine* (Morgan, 2016) projected six million cybersecurity job openings by 2020, with a shortfall in supply of 1.5 million capable workers, the timing is right for improving the alignment between cybersecurity curriculum and industry job performance requirements.

This report will describe an analysis of alignment between a standard cybersecurity curriculum and the competency requirements of professional practice. The report outlines an evidence-based curriculum mapping method that supports a holistic development model for enhancing the cybersecurity workforce (Assante & Tobey, 2011). The report will conclude with a review of the implications of taking a competency-based approach for cybersecurity education.

The graphic in Figure 1 summarizes the insights received from a panel of over 100 subject matter experts who participated in the curriculum mapping project. The depicted cybersecurity workforce development pathway shows that competency-based courses aligned with industry job performance requirements can contribute to closing the skills gap by implementing a spiral model of lifelong learning. Traditional students enter at the top of the diagram into courses providing a strong foundation in the concepts, principles and procedures of cybersecurity. Upon achieving mastery of Foundation Series concepts and techniques, these learners progress into the Pathway Series courses for which assessments indicate the learner possesses the prerequisite aptitude and interest. Mastery of the Pathway Series may lead directly to employment in entry level positions with cybersecurity responsibilities or into advanced courses at accredited 2-year or 4-year educational institutions, supported by articulation agreements facilitated by adoption of the standard curriculum. Those entering the workforce return periodically with their peers or transitioning workers for continual assessment, maintenance, and updating of their cybersecurity capabilities. Finally, career seekers with 4-year degrees in other domains can address workforce shortages through reverse articulation agreements into two-year accelerated job readiness programs which apply the Foundation and Pathway Series instructional techniques and content libraries. Research shows that this integrated, practice-centric, lifelong learning process is what is necessary to accelerate cybersecurity capability maturity in the workforce (Grossman, Spencer, & Salas, 2013).

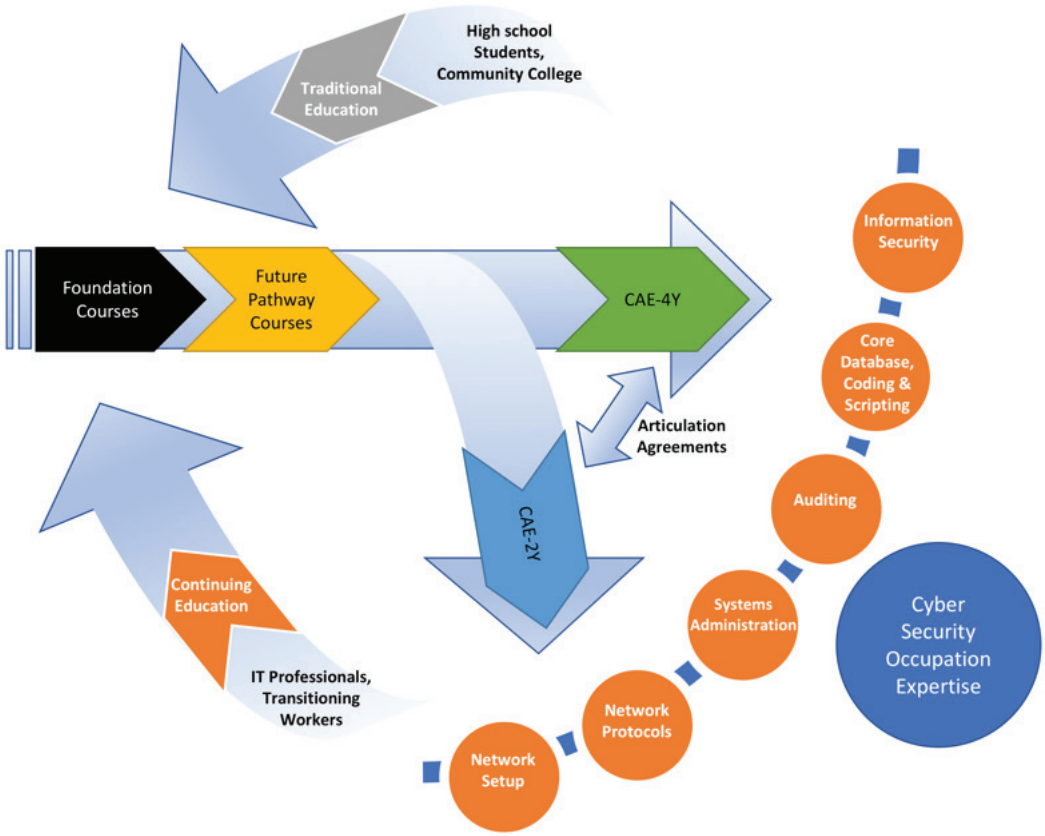


Figure 1. Path from Foundation/Pathway courses to cyber careers

Evidence-based Practices for Model Curriculum Development

The National CyberWatch Center Cybersecurity Core Curriculum Standards apply evidence-based principles established through the empirical study of effective practices in competency-based learning (Jones & Voorhees, 2002) to continually evaluate, enhance, and develop model curriculum for cybersecurity education. Eleven practices were identified as necessary to design curriculum that is valid and reliable for maturing job- and career-ready capabilities of program graduates. Each of these eleven practices will be applied in producing the NCC curriculum standards. These evidence-based practices will be replicated within each course design process. The result is a multiphase, technology-supported, agile development process that permits simultaneous development of courseware. The modular design of the Core Curriculum Development Process enables rapid prototyping, deployment and flexible scalability.

Model Curriculum Development Process

1. Recruitment and selection of renowned educators/instructional designers in the course content domain to provide subject matter expertise necessary to ensure validation of instructional designs.

2. A panel of 20-40 subject matter experts (instructors, industry practitioners, and instructional designers) participates in identifying, defining, and reaching a consensus about important competencies to which the curriculum is aligned.

3. Competencies are clearly defined, understood, and accepted by relevant stakeholders through a systematic process of public review and comment.

4. Multiple learning paths and related assessments of competencies provide useful and meaningful information to guide attainment of mastery in course content.

5. The assessment team considers precision, reliability, validity, credibility, and cost requirements in making decisions about the use of commercially developed assessments and/or panel-developed assessments.

6. The panel of experienced faculty and practitioners participate in the development of instructional designs and related assessment items (as required).

7. The course instructional and assessment designs are aligned with a continually updated National CyberWatch Center Core Curriculum Standards Curriculum Map. The curriculum map provides institutional guidance for course, certificate, degree, and career development pathways associated with the National Cybersecurity Workforce Framework Specialty Areas and National Security Agency Centers of Academic Excellence in Cyber Defense Knowledge Units.

8. Assessment items are directly mapped to learning goals in competency profile scorecards that will support individual or personalized development plans (IDP/PDP) for each learner.

9. Pilot implementation of each developed course module (i.e., instruction, assessment, practice lab and challenge lab) enables critical decisions about strategies to improve student learning and program effectiveness.

10. The pilot implementation results are disseminated through public review and comment workshops to ensure all relevant stakeholders fully understand the findings.

11. The pilot implementation results are used to experiment with new ways to document students' mastery of competencies that supplement the traditional transcript.

Scope of the Core Curriculum Standards Mapping Project

The purpose of the first initiative under the National CyberWatch Center Curriculum Standards Project (NCC-CSP) was to map five technical courses from the National CyberWatch Center Curriculum Library (https://www.nationalcyberwatch.org/programs-resources/curriculum/technical-courses/) which might be candidates to form the basis for a core, or foundational, cybersecurity curriculum to four competency and workforce frameworks:

1. Cybersecurity Job Performance and Capability Maturity Model (JP-CMM) adapted from competency frameworks developed by the National Board of Information Security Examiners

2. National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework

3. National Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units

4. Department of Homeland Security Mission Critical Role Project

METHOD

The core curriculum mapping project involved seven weekly sessions. Each session was supported by an online collaboration architecture including a web portal in the Google+1 social media system and a group decision support system, VivoInsight, which provides elicitation, voting, statistical analysis, and reporting. A Call for Participation was distributed through the *National CyberWatch Communicator*, a monthly e-Newsletter, a LinkedIn post on the Information Security Community (358,201 members) and personal invitations from National CyberWatch Center officers. Each registrant was provided a randomly generated ID that was used in subsequent surveys to anonymize the responses.

Participants

Interest in participating in the Curriculum Standards Panel was substantial: 124 individuals expressed Interest in participating on the panel; 111 people completed a registration questionnaire. Registrants were located in 35 states, the District of Columbia, and the countries of Australia, India, Indonesia, Kenya, Morocco, and the United Kingdom. The registrants reported the following qualifications:

Demographics:

Demographic
Gender: 79 male; 32 female
Age: Mean = 49.9, Range = 24-79

Ethnicity:

Ethnic Affiliation	Percent
Caucasian - White	66%
Caucasian - Hispanic	12%
Asian	11%
African-American	8%
Other	3%

[1] Google+ © 2017 Google. VivoInsight © 2015 VivoWorks, Inc.

Education:

Highest Degree Earned	Percent
Doctoral Degree	34.75%
Master's Degree	51.69%
Bachelor's Degree	10.17%
Other Degree or Certificate	3.39%

Certifications Held by More Than 10% of Participants:

Certification	Percent
CompTIA Security+	34.75%
CompTIA A+	31.36%
CompTIA Network+	28.81%
ISC^2 CISSP	22.88%
Cisco CCNA Security	11.86%

Teaching Experience:

Institutional Setting	Participants	Average Years of Experience (sd)
Post-secondary (4-year)	68	10.0 (8.1)
Post-secondary (2-year)	65	11.5 (7.1)
Secondary	20	6.4 (5.2)
Corporate training (in-house)	46	9.0 (9.0)
Corporate training (3rd party)	39	7.1 (5.4)

Participants with Experience Teaching the Courses to be Mapped

Course[2]	Participants
Ethical Hacking and Systems Defense (NCC214)	57
Information Security Fundamentals (NCC210)	91
Scripting Fundamentals (NCC212)	33
Linux Fundamentals (NCC204)	55
Network Fundamentals (NCC200)	85

Participants with Experience in Instructional Design Elements:

Instructional Design Element	Pct. of Participants	Avg Years of Experience (sd)
Assessment design	63.4%	9.4 (6.1)
Assessment item development	51.9%	10.3 (7.5)
Assessment validation	40.5%	8.8 (6.1)
Curriculum design	84.0%	9.7 (7.4)
Instructional content authoring	62.6%	10.1 (7.0)
Lab/simulation exercise design	58.0%	9.8 (6.3)
Teacher evaluation or accreditation	36.6%	9.2 (5.6)

Industry Experience (with at least 10% of participants):

Industry	Pct. of Participants	Avg Years of Experience (sd)
Education	79.4%	14.9 (8.8)
Professional Services: Cybersecurity	34.4%	9.7 (5.6)
IT Development and Manufacturing	33.6%	9.6 (6.9)
Professional Services: Technical (not cyber)	30.5%	13.8 (8.3)
Government: Federal	28.2%	10.7 (9.3)
Defense Contracting	22.9%	6.6 (5.9)
Emergency Management and Response	22.1%	8.9 (7.1)

Government: State/Local/Tribal	21.4%	9.8 (7.9)
Financial services	18.3%	7.4 (7.3)
Professional Services: Mgt Consulting	16.8%	10.9 (8.0)
Communications	14.5%	6.0 (4.5)
Healthcare	13.7%	6.7 (5.6)
Energy and Utilities	12.2%	7.7 (5.3)
Retail	12.2%	7.2 (7.0)
Aviation	10.7%	9.6 (8.3)

National Cybersecurity Workforce Framework Functional Role Experience (with at least 25% of participants)

Functional Role	Pct. of Participants	Avg Years of Experience (sd)
Education and Training	81.7%	15.4 (8.8)
Training, Education and Awareness	69.5%	13.4 (8.6)
System Administration	47.3%	11.4 (6.9)
Customer Service and Technical Support	42.0%	13.8 (8.2)
Risk Management	41.2%	9.5 (6.3)
Network Services	39.7%	14.1 (7.1)
Vulnerability Assessment and Management	38.2%	8.1 (5.6)
Information Assurance Compliance	37.4%	7.7 (4.4)
Digital Forensics	35.9%	7.1 (5.6)
Incident Response	35.9%	7.3 (5.8)
Systems Security Analysis	34.4%	11.3 (7.2)
Test and Evaluation	34.4%	11.8 (7.5)
Information Systems Security Operations	32.1%	7.9 (5.6)
Computer Network Defense Analysis	31.3%	9.6 (6.2)
Investigation	31.3%	9.8 (9.4)
Technology Research and Development	29.8%	11.6 (8.2)

Systems Development	29.0%	13.2 (7.4)
Computer Network Defense Infrastructure Support	27.5%	10.7 (6.6)
Systems Requirements Planning	26.0%	13.5 (7.3)

Panelist participation differed by session based on their availability and self-assessment of qualifications to provide the input required. The number of participants in each activity was as follows:

Activity	Number of Participants
1. Mapping Learning Objectives to JP-CMM Responsibilities	74
2. Mapping the Content of the NCC 200 to JP-CMM Tasks	40
3. Mapping the Content of the NCC 204 to JP-CMM Tasks	20
4. Mapping the Content of the NCC 210 to JP-CMM Tasks	38
5. Mapping the Content of the NCC 212 to JP-CMM Tasks	13
6. Mapping the Content of the NCC 214 to JP-CMM Tasks	24
7. Mapping NSA CAE-CD Knowledge Units to NCC 200	35
8. Mapping NSA CAE-CD Knowledge Units to NCC 204	27
9. Mapping NSA CAE-CD Knowledge Units to NCC 210	27
10. Mapping NSA CAE-CD Knowledge Units to NCC 212	27
11. Mapping NSA CAE-CD Knowledge Units to NCC 214	27
12. Mapping NICE KSAs to NCC Courses	34
13. Mapping DHS Mission Role Abilities to Learning Objectives	19
14. Mapping DHS Mission Role Abilities to Labs	17

Procedure

An advancement in job analysis, *Predictive Performance Modeling* (Tobey, Reiter-Palmon, & Callens, 2012), was previously applied to identify the distracting, esoteric, fundamental and differentiating tasks that distinguish the stages of expertise development (O'Neil et al., 2013; O'Neil, Assante, & Tobey, 2012; Tobey, 2011a, 2011b, 2015): novice (Level 0), beginner (Level 1), proficient (Level II), competent (Level III), and expert (Level IV). The result was a Job Performance Model that facilitates cybersecurity capability maturity assessment and development. Essential

job performance scenarios (vignettes), cross-functional role responsibilities, and the tasks that predict and differentiate expert performance comprise the Cybersecurity Job Performance and Capability Maturity Model (JP-CMM). The JP-CMM was developed by the National Board of Information Security Examiners in partnership with representatives from the National Security Agency, White House Communications Agency, U.S. Department of Energy, the U.S. Department of Homeland Security, and industry initiatives, such as the Electricity Sector Cybersecurity Capability Maturity Model (ES-C2M2). The mission critical cybersecurity responsibilities were validated through extensive public review and psychometric analyses of the human vulnerability and risk inherent in a workforce based on their level of cybersecurity capability maturity. During their first activity, panelists were asked to consider how the 91 cybersecurity responsibilities in the JP-CMM are related to five National CyberWatch Center curriculum courses.

The primary purpose of the second panel session was to extend the mapping of the five National CyberWatch Center courses to the JP-CMM. In this group of five activities, panelists mapped course topics to the tasks required to fulfill each responsibility mapped in the first activity. Panelists chose topics to map based on their areas of expertise and teaching experience. During each mapping activity, the panelists were asked *"For each statement listed, please select the SINGLE BEST Course Topic which you are HIGHLY CONFIDENT would provide SUFFICIENT prerequisite knowledge to effectively perform the listed action."* A task was selected as mapped to a course topic if the a majority of the panel showed between a slight and fair agreement (*Fleiss Kappa > .1*) in rating course topics as providing sufficient knowledge to effectively perform the task.

The third set of panel activities involved mapping the Core Knowledge Units from the National Security Agency's Center for Academic Excellence - Cyber Defense program. As with the mapping of course topics to the JP-CMM, an activity was created for subgroups of the panel to map specific courses based on the panel members area of expertise and experience. During this mapping activity, the panelists were asked: *"For the Course Topic listed, please select ANY and ALL of the NSA Knowledge Units listed below for which this topic provides relevant knowledge."* Since the mappings in this activity were not mutually exclusive, Core Knowledge Units were determined to be mapped to a specific course topic based on two criteria. First, the course topic ratings must have received a minimum of a slight level of interrater agreement (*Fleiss Kappa is positive*). Second, a majority of raters must have indicated the Knowledge Unit should be addressed by the course topic.

The fourth set of panel activities involved mapping the Core Curriculum Courses to the National Initiative for Cybersecurity Education (NICE) Knowledge, Skills and Abilities (KSAs) listed in the National Cybersecurity Workforce Framework, interactive version 1.0 as published on the NICE website (http://csrc.nist.gov/nice/framework/). During this activity, panelists were asked, *"For each NICE KSA, indicate the course in which the listed knowledge, skill or ability should be able to be demonstrated by the conclusion of the course."*

The final set of activities mapped the DHS Mission Role Abilities to the National CyberWatch Center course learning objectives and tutorial labs. This session accordingly had two activities. During the first activity, the panelists were asked: *"For the learning objective listed, please select all of the abilities which would be helpful in achieving this objective."* During the second activity, the panelists were asked, *"For the lab listed below, please select all of the abilities which would be helpful in achieving this objective."*

Analysis

Each panel session was evaluated by assessing interrater agreement among panelists using the intraclass correlation coefficient (ICC; Shrout & Fleiss, 1979, 1981). Mappings of curriculum objects were by majority rating only when such rating exhibited a minimum of fair agreement. There were two types of analyses to which this minimum agreement was applied. First, the purpose of the first twelve mapping activities was to identify as many items as possible that could be included to identify the broadest scope for the core curriculum. For these activities, the recommended cutoff of 0.21 suggested by Shrout and Fleiss (1981) was used to determine a fair level of agreement. Second, the final two activities were focused on pinpointing the appropriate step in the learning path each course should occupy. Accordingly, a more restrictive recommended cutoff of 0.31 (LeBreton and Senter, 2008) was used to signify fair agreement. Additionally, the overall agreement for each session was calculated and was analyzed to determine whether the agreement was significant (i.e., not due to chance).

RESULTS

I. Mapping Learning Objectives to JP-CMM Responsibilities

Mapping Across the Core Curriculum

All 91 JP-CMM responsibilities were found to map to at least one of the five courses. However, most of these mappings were to the Information Security Fundamentals (NCC 210) and Ethical Hacking and Systems Defense (NCC 214) courses. The other three courses, collectively, only mapped to six responsibilities. The results suggest that the NCC 210 course is the central core of the standard curriculum.

NCC 210 learning objectives mapped to 86.8% of the JP-CMM responsibilities. The next closest mapping was for NCC 214 which mapped to 53.8% of the JP-CMM responsibilities. However, most (75.5%) of the NCC 214 mappings were in common with NCC 210. Twelve responsibilities (13.2%) were uniquely mapped to NCC 214 (see Table below).

JP-CMM Responsibilities Uniquely Mapped to NCC 214
Ensure demonstrated proficiency with authorized/approved pentesting toolbox
Ensure penetration testing clients are adequately informed and trained
Ensure all vulnerable applications have been exploited
Ensure all vulnerable desktops/workstations have been exploited
Ensure all vulnerable networks have been exploited
Ensure all vulnerable security monitoring systems have been exploited
Ensure all vulnerable servers have been exploited
Ensure all vulnerable web applications have been exploited
Ensure use of all methods of exploitation
Ensure a penetration strategy has been developed and executed
Ensure all penetration targets have been analyzed
Ensure all penetration targets have been identified

The other three courses (Networking Fundamentals (NCC 200), Linux Fundamentals (204) and Scripting Fundamentals (212)) did not have any unique mappings to a responsibility. The table below lists the six responsibilities that were shared with NCC 210. NCC 204 also shared one responsibility with NCC 214 ("Ensure hardening of operating system, services, and applications on custom or third-party solutions").

JP-CMM Responsibility	Course other than 210 which addressed the responsibility
Ensure a baseline of normal/expected activity is available or can be quickly assembled to support analysis	NCC 200
Ensure log sources are time-synced to a local NTP server	NCC 200
Ensure maintenance of an accurate picture of utility systems deployed, architectures, communication protocols employed and business functions and processes	NCC 200
Ensure hardening of operating system, services, and applications on custom or third-party solutions	NCC 204
Ensure maintenance of security profiles for operational system components	NCC 204
Ensure monitoring can be automated or scripted	NCC 212

Primary Course Mapping

NCC 210 was determined to be the primary course to contain learning objectives related to 64 (70.3%) of the responsibilities. NCC 214 was determined to be the primary course to contain learning objectives related to 25 (27.5%) of the responsibilities. The remaining two responsibilities were primarily related to NCC 200 ("Ensure log sources are time-synced to a local NTP server") and NCC 212 ("Ensure monitoring can be automated or scripted"). The complete primary course mappings are provided in the Appendix.

Summary

Figure 2 below summarizes the findings from the first panel session. This chart shows the coverage by course of each of the fourteen responsibility areas that comprise the Cybersecurity Job Performance and Capability Maturity Model (JP-CMM). This chart clearly shows that NCC 210 course provides a core foundation for cybersecurity education. The NCC 214 course fills in some gaps in the areas of identifying and exploiting targets, but otherwise served to enhance the foundation created by the Information Security Fundamentals course. The remaining three courses provide limited coverage of the responsibilities of a cybersecurity professional as defined by the JP-CMM, suggesting that they may be more appropriately considered as prerequisite courses developing competencies in related Information Technology disciplines.

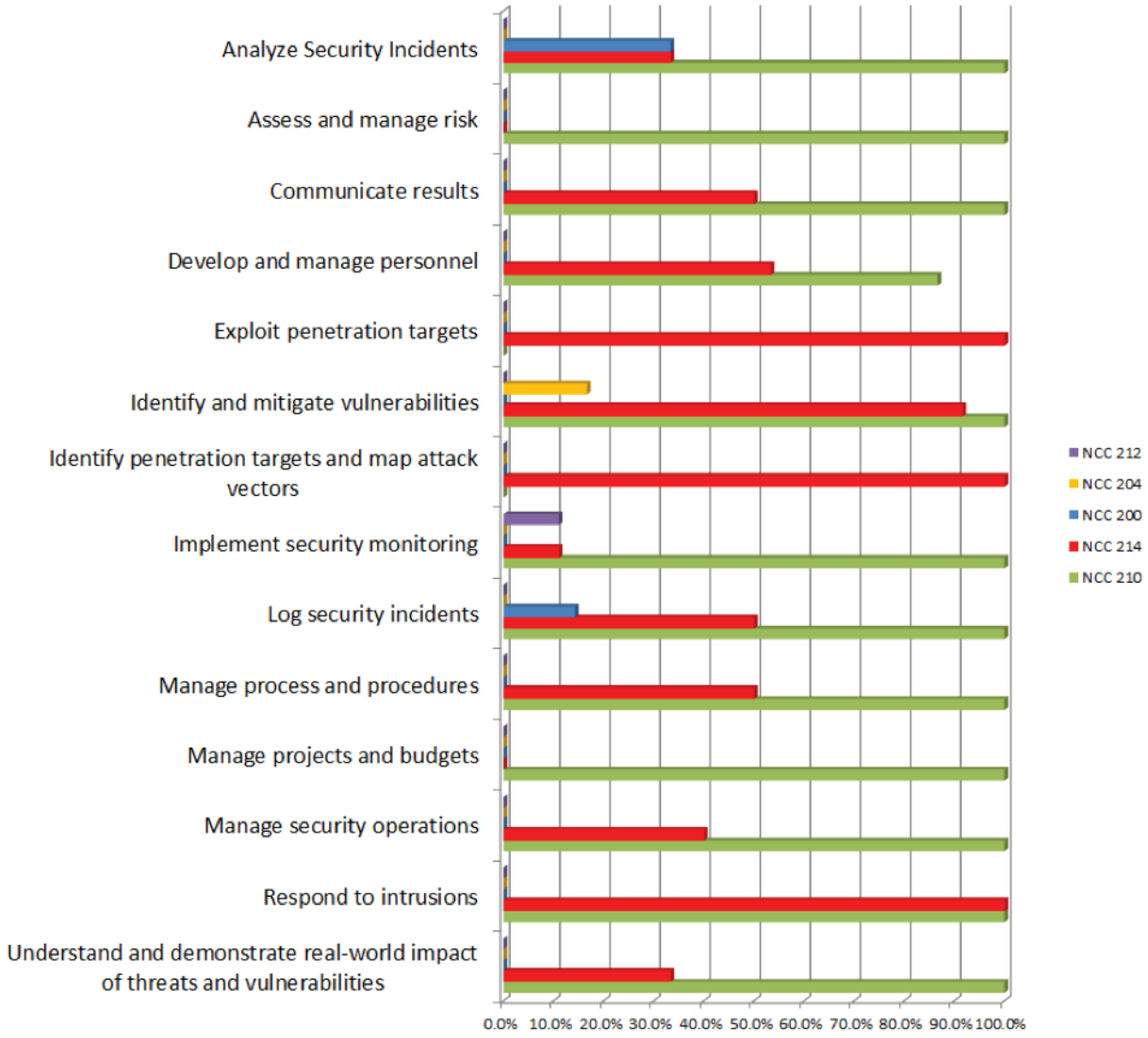


Figure 2. Course Coverage of JP-CMM Responsibility Areas

As shown in the table on the next page, the level of agreement among the panelists in mapping each of the JP-CMM responsibility areas was highly significant ($p < .0001$). Interrater agreement may differ from a lack of agreement (ICC < .3) to very strong agreement (> .9) (LeBreton & Senter, 2008). Six of the JP-CMM responsibility areas showed very strong agreement and the remaining eight showed strong agreement among the panelist course mappings.

Responsibility Area	Intraclass Correlation Coefficient (ICC-2)	Level of agreement
Analyze Security Incidents	.86	Strong
Assess and manage risk	.90	Strong
Communicate results	.94	Very Strong
Develop and manage personnel	.80	Strong
Exploit penetration targets	.97	Very Strong
Identify and mitigate vulnerabilities	.87	Strong
Identify penetration targets and map attack vectors	.99	Very Strong
Implement security monitoring	.75	Strong
Log security incidents	.84	Strong
Manage process and procedures	.98	Very Strong
Manage projects and budgets	.81	Strong
Manage security operations	.80	Strong
Respond to intrusions	.98	Very Strong
Understand and demonstrate real-world impact of threats and vulnerabilities	.95	Very Strong

Each of the JP-CMM responsibilities are defined in terms of tasks required to be performed to fulfill the responsibility. Therefore, to more accurately portray the mapping between courses and the responsibilities of a cybersecurity professional, the panel was divided into task forces based on self-assessed expertise in specific course topics. The results of the task mappings created based on agreement analysis of these Topic Area Working Groups (TAWG) is described next.

II. Mapping Course Topics to Job Performance and Capability Maturity Model Tasks

Network Fundamentals Course (NCC 200)

A significant and moderate level of interrater agreement (ICC = .544; $p < .0001$) was found among the panelists who rated the NCC 200 course topic to JP-CMM task mappings. Thirty tasks were found to relate to the NCC 200 course topics. Five tasks were related to the first topic discussed in the course, Exploring the Network. The second course topic, Network Protocols and Communications, was mapped to one task. Eighteen tasks were related to the second topic discussed in the course, Configuring a Network Operating System. Finally, two tasks were related to the last topic discussed in the course, Application Layer, respectively. The remaining course topics may contain prerequisite concepts that are necessary but not sufficient to perform tasks typically required in cybersecurity operations.

The Fleiss Kappa agreement indices for these task mappings and the level of agreement this signifies are shown in the tables below. Collectively, these tasks are aligned with the Beginner Level of the JP-CMM, averaging a JP-CMM Level 1.35. The tables below list the tasks mapped by the panel.

TOPIC 1. Exploring the Network

JP-CMM Task	Fleiss Kappa	Level of Agreement
Access an up to date component inventory and asset list.	0.251	Fair
Scan internal and external networks for new and unauthorized systems	0.21	Fair
Analyze which systems are being regularly scanned and which systems are being missed	0.178	Slight
Scan systems to establish baseline	0.165	Slight
Map activities observed in the network to systems to help establish the baseline	0.124	Slight

TOPIC 2. Configuring a Network Operating System

JP-CMM Task	Fleiss Kappa	Level of Agreement
Configure system against the baseline configuration manual	0.368	Fair
Test implementation with planned configurations to determine any deployment issues	0.309	Fair
Schedule periodic reviews to determine when patches and updates are required	0.308	Fair
Subscribe to vendor notifications and alerts	0.279	Fair
Configure security tools to automatically apply patches and apply updates	0.271	Fair
Subscribe to vendor publications relevant to the product line at hand	0.268	Fair
Review daily, weekly and monthly reports for systems that are not updating and/or are out of baseline with the rest of the system population	0.26	Fair
Test installation against the functional and performance requirements	0.246	Fair
Review updates and version and confirm with vendor	0.246	Fair
Scan for gaps in system configuration against a benchmark configuration manual	0.231	Fair

Implement a reference time source to remove external dependencies for Network Time Protocol	0.214	Fair
Scan systems regularly in an attempt to detect the use of unacceptable software	0.21	Fair
Collect existing device configurations	0.2	Slight
Verify that all systems are logging to a central location	0.185	Slight
Implement solution to identify new devices connecting to the network(s)	0.175	Slight
Scan against configuration anomalies	0.171	Slight
Test server periodically to make sure NTP service is operating	0.168	Slight
Collect existing device configurations	0.165	Slight

TOPIC 3. Network Protocols and Communications

JP-CMM Task	Fleiss Kappa	Level of Agreement
Analyze system logs for NTP synchronization anomaly messages	.134	Slight

TOPIC 10. Application Layer

JP-CMM Task	Fleiss Kappa	Level of Agreement
Implement application (layer 7) firewalls	.233	Fair
Implement Web content filtering	.223	Fair

Linux Fundamentals Course (NCC 204)

A significant and strong interrater agreement (ICC = .799; $p < .0001$) was found among the TAWG panelists who rated the NCC 204 course topics to JP-CMM task mappings. One of the four course topics, Linux Installation and Package Management, was found to be sufficient to perform the task Configure system against the baseline configuration manual (a JP-CMM Level 1 task). Similar to some of the course topics in NCC 200, the results suggest that panelists believed most of the course topics may be focused on topics that are necessary prerequisites, but not sufficient by themselves to be able to perform cybersecurity functions. This course is therefore associated with the Beginner Level of cybersecurity capability maturity.

Information Security Fundamentals Course (NCC 210)

A significant, but weak overall interrater agreement (ICC = .439; $p < .0001$) was found among the TAWG panelists who rated the NCC 210 course topics to JP-CMM task mappings. However, the weakness of the agreement may be related to the fact that 50 tasks were found to map to this course across eight of the thirteen course topics. The course topics that did not map to any JP-CMM tasks were topics: 1) Information Security; 3) The Drivers of the Information Security Business; 4) Access Controls; 8) Cryptography; 9) Networks and Telecommunications; 11) Information Security Standards; and 12) Information Security Professional Certifications. Most of the task mappings were associated with two topics: Security Operations and Administration (23 tasks) and Auditing, Testing, and Monitoring (17 tasks). Collectively, these task mappings averaged a JP-CMM Level 1.8. Thus, NCC 210 should be considered an Advanced Beginner course. The topic to JP-CMM task mappings are listed in the tables below.

TOPIC 2. Changing How People and Business Communicate

JP-CMM Task	Fleiss Kappa	Level of Agreement
Communicate with new staff or external stakeholders	.14	Slight

TOPIC 5. Security Operations and Administration

JP-CMM Task	Fleiss Kappa	Level of Agreement
Monitor security tool vendors for updates and patches	0.285	Fair
Configure security tools to automatically apply patches and apply updates	0.283	Fair
Configure system against the baseline configuration manual	0.246	Fair
Subscribe to vendor notifications and alerts	0.242	Fair
Document current patch levels and updates before use in critical situations	0.233	Fair
Schedule periodic reviews to determine when patches and updates are required	0.227	Fair
Collect existing device configurations	0.225	Fair
Understand the process by which security tools are updated before use	0.217	Fair
Define reports on the current patch and update status of all security tools and identify any variances against vendor releases	0.216	Fair

Establish a systems and tools patching program and schedule	0.214	Fair
Monitor vendor feeds for published patches	0.209	Slight
Review updates and version and confirm with vendor	0.206	Slight
Subscribe to vendor publishing's relevant to the product line at hand	0.194	Slight
Update security tools (SIEM, Intrusion Defense/Protection Systems, Firewalls) with information pertinent to net tools or attacks	0.186	Slight
Verify versions of security tools periodically against vendors latest release version or review exceptions for not updating the software	0.184	Slight
Review signatures (for the tools that use them) to determine applicability once implemented	0.178	Slight
Monitor security tool providers for updates and patches for tools that are in use	0.173	Slight
Develop a policy which requires system administrators to follow company procedures related to download and install third-party software	0.165	Slight
Coordinate with administrators from other departments (i.e. networking, operating systems, servers) to identify strengths and weaknesses in the organization's logging of implementations	0.158	Slight
Identify primary support resources for each of the production tools to ensure team members understand their responsibilities	0.156	Slight
Define criticality levels for all tool types and identify security tools as some of the most critical security tools that need to be patched and updated properly	0.15	Slight
Configure signatures for host and network based IPS to ensure optimal configuration and reduce likelihood of business disruption	0.148	Slight
Create policy/procedures for how to patch tools	0.136	Slight

TOPIC 6. Auditing, Testing, and Monitoring

JP-CMM Task	Fleiss Kappa	Level of Agreement
Scan systems regularly in an attempt to detect the use of unacceptable software	0.376	Fair
Analyze which systems are being regularly scanned and which systems are being missed	0.324	Fair
Monitor new systems installed on the network	0.315	Fair
Test toolset upgrades against old version to ensure new patches doesn't adversely affect results or impair performance	0.31	Fair
Implement replica production (i.e. lab) environment for testing of patches prior to production release	0.285	Fair
Scan for gaps in system configuration against a benchmark configuration manual	0.283	Fair
Monitor software installed on end-points for compliance the company policy	0.23	Fair
Review daily, weekly and monthly reports for systems that are not updating and/or are out of baseline with the rest of the system population	0.211	Fair
Review closed tickets for false positives for unacceptable results	0.183	Slight
Establish a sandbox in which experimental software may be installed and analyzed for malevolent behavior	0.178	Slight
Monitor software utilized in the infrastructure and correlate it to a list of acceptable software	0.172	Slight
Review healthy-log collection metrics to understand baseline from which to measure normal performance	0.167	Slight
Review latest penetration test tools	0.164	Slight
Identify current patch level of security tools	0.143	Slight
Scan for gaps in system configuration against a benchmark configuration manual	0.133	Slight
Verify health status of host security tools	0.125	Slight

TOPIC 7. Risk, Response, and Recovery

JP-CMM Task	Fleiss Kappa	Level of Agreement
Report risk level of vulnerabilities	0.33	Fair
Document shortcomings and lessons learned from incident exercises and formulate action plans to ensure they're corrected as rapidly as possible	0.219	Fair
Review assessment results in accordance with defined risk categorization model	0.15	Slight
Communicate key risks to users of a system, application, device, or other components impacted by threats or vulnerabilities	0.139	Slight
Communicate risks to internal stakeholders (within your group or department)	0.136	Slight

TOPIC 10. Malicious Attacks, Threats, and Vulnerabilities

JP-CMM Task	Fleiss Kappa	Level of Agreement
Develop attack trees of attack vectors against vulnerable systems	.186	Slight
Explain results of attacks to clients/users	.12	Slight

TOPIC 13. U.S. Compliance Guidelines & Laws

JP-CMM Task	Fleiss Kappa	Level of Agreement
Understand current status of relevant legislation	.86	Almost perfect
Understand how federal regulations apply to security testing	.756	Substantial

Scripting Fundamentals Course (NCC 212)

A significant and very strong interrater agreement (ICC = .901; $p < .0001$) was found among the TAWG panelists who rated the NCC 212 course topics to JP-CMM task mappings. However, the agreement was that the NCC 212 course topics were not related to any JP-CMM task. One possible explanation for this result is that focus of the JP-CMM is on cybersecurity operations, rather than secure coding or other forms of secure programming/scripting. Thus, these results may imply a need to develop a job performance model related to these specialized aspects of cybersecurity.

Ethical Hacking and Systems Defense Course (NCC 214)

Overall, 44 tasks mapped to the Ethical Hacking and Systems Defense Course (NCC 214) and it was the only course to have each of its seven course topics map to at least one task. The interrater agreement for this course was very strong and significant (ICC = .903; $p < .0001$) Similar to the other course mappings, the distribution of task mappings was not equally distributed. The first two topics, Introduction to Ethical Hacking and Penetration testing professional certifications were mapped to three and two tasks, respectively. The fifth (Enumeration) and seventh (Post-Exploitation) topics mapped to two tasks each. The bulk of the JP-CMM tasks were found to be distributed across three course topics: Exploitation (20 tasks); Reconnaissance/Open Source Intelligence Gathering (9 tasks); and Scanning (6 tasks). Collectively, these task mappings averaged a JP-CMM Level 2.56. Thus, NCC 214 should be considered a Proficiency course most appropriately sequenced after the foundational concepts and principles have been mastered. This course may be of most value to those learners seeking to develop a career pathway in operational security testing (Tobey, Assante, King, & Ziegler, 2010). The specific task mappings for each course topic are provided in the tables below.

TOPIC 1. Introduction to Ethical Hacking

JP-CMM Task	Fleiss Kappa	Level of Agreement
Mentor employees interested in learning about security	0.238	Fair
Conduct mission brief for all team members to ensure clear understanding of project	0.172	Slight
Train all employees on security/attack/monitoring courses to increase general awareness	0.155	Slight

TOPIC 2. Penetration testing professional certifications

JP-CMM Task	Fleiss Kappa	Level of Agreement
Document all team member training/certification	.209	Slight
Provide opportunities for new entrants into security to develop competencies	.176	Slight

TOPIC 3. Reconnaissance/Open Source Intelligence Gathering

JP-CMM Task	Fleiss Kappa	Level of Agreement
Survey environment to gain situational awareness	0.499	Moderate

Search online sources for useful information about a target	0.433	Moderate
Identify recon that is within project scope	0.267	Fair
Develop a clear picture of scope and specific hardware, software, policies, practices in use	0.218	Fair
Identify major attack targets and assets	0.18	Slight
Identify ownership of gateway devices	0.176	Slight
Identify users with high levels of access on target systems	0.155	Slight
Capture legit websites	0.151	Slight
Identify targets for potential exploitation	0.135	Slight

TOPIC 4. Scanning

JP-CMM Task	Fleiss Kappa	Level of Agreement
Identify which ports are open through a firewall	0.329	Fair
Decide if a service is alive using packet captures	0.275	Fair
Review vulnerability scan results	0.242	Fair
Review scanning schedule results for anomalies	0.226	Fair
Configure vulnerability scanners to operate in the targeted environment in a safe and effective manner	0.176	Slight
Configure vulnerability scanners to operate in the targeted environment in a safe and effective manner	0.151	Slight

TOPIC 5. Enumeration

JP-CMM Task	Fleiss Kappa	Level of Agreement
Map and exploit wireless networks	.18	Slight
Analyze data found on compromised machines to enable exploitation deeper into the network	.135	Slight

TOPIC 6. Exploitation

JP-CMM Task	Fleiss Kappa	Level of Agreement
Exploit web applications	0.574	Moderate
Attack network storage environments	0.499	Moderate
Attack corporate PKI	0.495	Moderate
Compromise individual host or service	0.445	Moderate
Attack using pass the hash to compromise additional systems and privilege escalation to gain root access	0.441	Moderate
Exploit custom non-web software	0.433	Moderate
Attack standard data protection mechanisms	0.433	Moderate
Attack virtualized environments	0.433	Moderate
Attack using an organization's secure protocols (i.e. SSL)	0.424	Moderate
Bypass security mechanisms intended to prevent attacks	0.42	Moderate
Attack using operating system commands to further compromise systems without the need of third-party tools	0.329	Fair
Bypass Web Application Firewalls	0.317	Fair
Exploit multiple systems concurrently	0.313	Fair
Create new processes on remote computers	0.267	Fair
Establish control of Windows machines	0.267	Fair
Access locked workstations	0.263	Fair
Attack Layer-2 network isolation mechanisms	0.255	Fair
Establish control of remote access mechanisms from inside	0.168	Slight
Establish Man-in-the-Middle (MITM) control on a desktop network	0.164	Slight
Install stealth software to control and collect information	0.164	Slight

TOPIC 7. Post-Exploitation

JP-CMM Task	Fleiss Kappa	Level of Agreement
Analyze data found on compromised machines for strategic value as seen by a worst case actual attacker	0.247	Fair
Exfiltrate data for analysis	0.122	Slight

Summary

The task mappings reveal a recommended learning path between the five courses evaluated by the panel. Figure 3 below shows the results of analysis of mapping course topics to JP-CMM capability maturity levels: Level 0 (Novice); Level 1 (Beginner); Level 2 (Proficient); Level 3 (Competent); and Level 4 (Expert). Each course with mapping to the JP-CMM tasks is distinguished by colored boxes: NCC 200 (gray); NCC 204 (tan); NCC 210 (green); and NCC 214 (blue). The black arrow lines between boxes indicate when the learning progression is within the same maturity level. The red arrow lines in the diagram indicate when a learning path crosses a maturity level.

One important implication of this analysis is that upon completing a course in the learning path, the learner usually will retrace a maturity level to begin the next course. This occurs because the learner's capability in the new topic is less advanced than their capability in the topic that preceded it. Finally, prerequisite topics are indicated at Level 0. These topics were not found to be directly related to tasks that define cybersecurity capability maturity. However, the concepts presented in these topics must be fully understood prior to a learner beginning the capability maturity learning path. Thus, the learning path indicates topics which may form a bridge with adjacent disciplines, such as Information Technology, as well as identifying conceptual domains that could comprise a pre-qualification assessment of learner readiness.

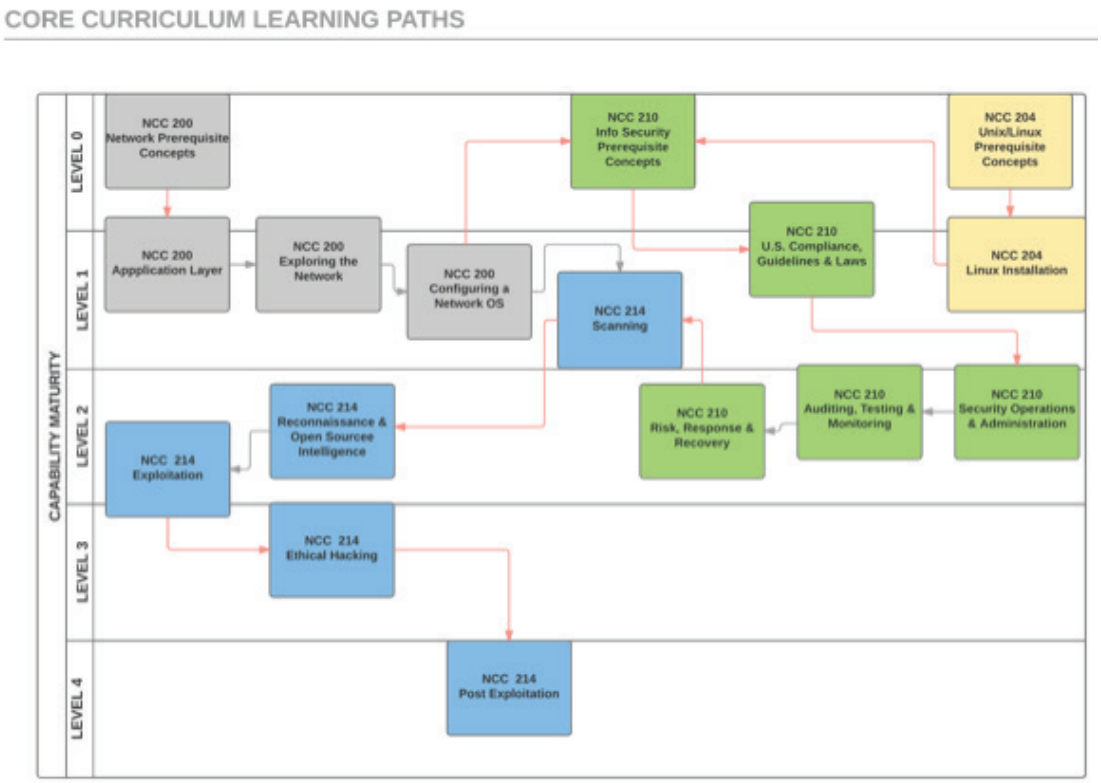


Figure 3. Mapping of Course Topics to Capability Maturity Levels

III. Mapping NSA CAE-CD Core Knowledge Units

Network Fundamentals Course (NCC 200)

Six of the NSA CAE-CD Core Knowledge Units (KUs) were found to be mapped to the NCC 200 course: *IT Systems Components; Networking Concepts; System Administration; Network Defense; Networking Technology and Protocols; and Operating Systems Concepts*. The results suggest that three of the six mapped KUs were only briefly covered by this course. *IT Systems Components and Operating Systems Concepts* were each mapped to only one course topic, *Network Layer and Configuring a Network*, respectively. *System Administration* was mapped to two course concepts: *Configuring a Network and IP Addressing*. Primarily, the course was found to address three KUs. *Networking Concepts and Networking Technology and Protocols* were addressed by all the course topics. Finally, *Network Defense* was addressed by 7 of the 10 course topics. The topics that did not map to *Network Defense* were *Configuring a Network, Ethernet, and Subnetting*. Interrater agreement for these mappings was very strong and significant ($ICC = .92$, $p < .0001$).

Linux Fundamentals Course (NCC 204)

Two of the NSA CAE-CD Core Knowledge Units (KUs) were found to be mapped to the NCC 204 course: *IT Systems Components and Operating Systems Concepts*. The *System Architecture and Linux Filesystems, Filesystem Hierarchy Standard* course topics were rated by the panelists as related to the *IT Systems Components* KU. The *Operating Systems Concepts* KU was rated to be related to the other two course topics: *Linux Installation and Package Management and GNU and Unix Commands*. Interrater agreement for these mappings was moderate and significant ($ICC = .614$, $p < .0001$).

Information Security Fundamentals Course (NCC 210)

Ten of the seventeen NSA CAE-CD Core Knowledge Units (KUs) were found to be mapped to the NCC 210 course: *IA Fundamentals; Introduction to Cryptography; Policy, Legal, Ethics, and Compliance; Networking Concepts; System Administration; Cyber Defense; Cyber Threats; Fundamental Security Design Principles; Network Defense; and Networking Technology and Protocols*. Of the 13 topics covered by NCC 210, ten were reported by the panelists as related to *IA Fundamentals*, excepting *Changing How People and Business Communicate; Networks and Telecommunications; and U.S. Compliance Guidelines & Laws*. The remaining KUs received limited coverage across the topics. Three KUs were covered by only one course topic: *Introduction to Cryptography; Networking Concepts; and Networking Technology and Protocols*. Six KUs were covered by two topic areas: *Policy, Legal, Ethics, and Compliance; System Administration; Cyber Defense; Cyber Threats; Fundamental Security Design Principles; and Network Defense*. Interrater agreement for these mappings was weak, but significant ($ICC = .393$, $p < .0001$).

Scripting Fundamentals Course (NCC 212)

Three of the seventeen NSA CAE-CD Core Knowledge Units (KUs) were found to be mapped to the NCC 212 Course: *Basic Scripting or Introductory Programming; Programming; and Databases.* The first two of these KUs were covered by most of the course topics. The course topic *Accessing Databases* did not map to *Programming*. The KU *Basic Scripting* was rated the panelists as covered in all topic areas except *Accessing Databases, Network Programming, and Web Applications*. Databases was only mapped by the panelists to the course topic *Accessing Databases*. Thus, all course topics mapped to at least one KU. Interrater agreement for these mappings was strong and significant ($ICC = .723$, $p < .0001$).

Ethical Hacking and Systems Defense Course (NCC 214)

Five of the seventeen NSA CAE-CD Core Knowledge Units (KUs) were found to be mapped to the NCC 214 course: *Policy, Legal, Ethics, and Compliance; Cyber Defense; Cyber Threats; Network Defense; and Networking Technology and Protocols*. Two of the KUs, *Cyber Threats and Network Defense*, were mapped to three course topics. Both of these KUs were mapped to the topics Introduction to *Ethical Hacking and Exploitation*. Additionally, the topic *Scanning* mapped to the KU *Cyber Threats* while the topic *Post-Exploitation* mapped to the KU *Network Defense.* The *Cyber Defense* KU was mapped to two course topics, *Introduction to Ethical Hacking* and *Exploitation and Exploitation*. The *Introduction to Ethical Hacking* was the only topic mapped to the *Policy, Legal, Ethics, and Compliance* KU while the *Scanning* topic was the only topic mapped to *Networking Technology and Protocols*. Interrater agreement for these mappings was borderline moderate and significant ($ICC = .499$, $p < .0001$).

Summary

The panel evaluation of the mapping between the Core Curriculum Course Topics and the National Security Agency's Centers of Academic Excellence Cyber Defense KUs revealed at least some coverage for all but two KUs, *Basic Data Analysis and Probability and Statistics*, that likely would be covered in general education courses. However, the degree of coverage for each KU differed substantially across the courses. As shown in the Table below, the greatest breadth of KU coverage is available from the NCC 210 course while the other courses offer greater depth of coverage in specialized knowledge domains.

NSA CAE-CD Core Knowledge Units	Percent of Course Topics Covering Core Knowledge Units				
	NCC 200	NCC 204	NCC 210	NCC 212	NCC 214
IA Fundamentals	-	-	76.9%	-	-
Intro to Cryptography	-	-	7.7%	-	-
IT Systems Components	10.0%	50.0%	-	-	-
Policy, Legal, Ethics, and Compliance	-	-	15.4%	-	-
Networking Concepts	100.0%	-	7.7%	-	-
System Administration	20.0%	-	15.4%	-	-
Basic Data Analysis	-	-	-	-	-
Basic Scripting or Introductory Programming	-	-	-	72.7%	-
Cyber Defense	-	-	15.4%	-	16.7%
Cyber Threats	-	-	15.4%	-	33.3%
Fundamental Security Design Principles	-	-	15.4%	-	-
Databases	-	-	-	9.1%	-
Network Defense	70.0%	-	15.4%	-	33.3%
Networking Technology and Protocols	100.0%	-	7.7%	-	16.7%
Operating Systems Concepts	10.0%	50.0%	-	-	-
Probability and Statistics	-	-	-	-	-
Programming	-	-	-	90.9%	-

IV. Mapping NCWF Knowledge, Skills, and Abilities

The panel evaluated the alignment of course learning objectives with the knowledge, skills and abilities (KSAs) identified by the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework (NCWF). Overall, the panel ratings across all courses and all NICE KSAs showed significant, but weak agreement (ICC = .374, $p < .0001$). However within NICE competencies that had several knowledge, skills and abilities included within the Framework the interrater agreement was much higher. For example, for Computer Network Defense (29 KSAs) the agreement was strong (ICC = .858, $p < .0001$). The interrater agreement for Vulnerability Assessment (22 KSAs) was moderate (ICC = .69, $p < .0001$). Each of the course mappings to KSAs within the associated NICE Competencies is detailed in the tables below.

Network Fundamentals Course (NCC 200)

Competency: Capacity Management

Skill	Fleiss Kappa	Level of Agreement
Skill in analyzing network traffic capacity and performance characteristics [KSA ID: 154]	.33	Fair

Competency: Configuration Management

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of collection management processes, capabilities, and limitations [KSA ID: 912]	.2	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in determining the effects of various router configurations on traffic patterns and network performance in both LAN and WAN environments [KSA ID: 357]	0.36	Fair
Skill in configuring and utilizing network protection components (e.g., firewalls, Virtual Private Networks [VPNs], network Intrusion Detection Systems [IDSs]) [KSA ID: 985]	0.14	Slight

Competency: Encryption

Skill	Fleiss Kappa	Level of Agreement
Skill in using Virtual Private Network (VPN) devices and encryption [KSA ID: 237]	.136	Slight

Competency: Enterprise Architecture

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of enterprise messaging systems and associated software [KSA ID: 44]	.245	Fair

Competency: Hardware

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware [KSA ID: 15]	0.681	Substantial
Knowledge of network hardware devices and functions [KSA ID: 83]	0.559	Moderate
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]) [KSA ID: 281]	0.155	Slight

Competency: Identity Management

Skill	Fleiss Kappa	Level of Agreement
Skill in maintaining directory services [KSA ID: 209]	.187	Slight

Competency: Information Systems/Network Security

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of logging services for network devices [KSA ID: 313]	0.202	Slight
Knowledge of front-end collection systems, including network traffic collection, filtering, and selection. [KSA ID: 915]	0.144	Slight
Knowledge of network traffic analysis methods [KSA ID: 87]	0.136	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in installing, configuring, and troubleshooting local area network (LAN) and wide area network (WAN) [KSA ID: 207]	.425	Moderate

Competency: Information Technology Architecture

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of remote access technology concepts [KSA ID: 106]	.155	Slight

Competency: Infrastructure Design

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of networking protocols [KSA ID: 1059]	1	Perfect
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 [KSA ID: 139]	0.929	Almost Perfect
Knowledge of computer networking fundamentals [KSA ID: 22]	0.929	Almost Perfect
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection model [OSI], Information Technology Infrastructure Library, v3 [ITIL]) [KSA ID: 92]	0.861	Almost Perfect
Knowledge of local area network (LAN) and wide area network (WAN) principles and concepts, including bandwidth management [KSA ID: 72]	0.861	Almost Perfect

Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services [KSA ID: 81]	0.861	Almost Perfect
Knowledge of how network services and protocols interact to provide network communications [KSA ID: 50]	0.737	Substantial
Knowledge of common network tools (e.g., ping, traceroute, nslookup) [KSA ID: 271]	0.733	Substantial
Knowledge of router and routing processes, connections, protocols, and configuration (including their effects on operations) [KSA ID: 322]	0.69	Substantial
Knowledge of organization's Local Area Network (LAN)/Wide Area Network (WAN) pathways [KSA ID: 41]	0.681	Substantial
Knowledge of communication methods, principles, and concepts (e.g., cryptography, dual hubs, time multiplexers) that support the network infrastructure [KSA ID: 12]	0.476	Moderate
Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs [KSA ID: 82]	0.279	Fair

Competency: Network Management

Knowledge	Fleiss Kappa	Level of Agreement
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]) [KSA ID: 902]	0.737	Substantial
Knowledge of Wireless Fidelity (WI-FI) [KSA ID: 903]	0.523	Moderate
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) [KSA ID: 901]	0.489	Moderate
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools [KSA ID: 1073]	0.345	Fair
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in diagnosing connectivity problems [KSA ID: 194]	0.63	Substantial
Skill in using traceroute analysis tools [KSA ID: 385]	0.519	Moderate
Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol) [KSA ID: 231]	0.36	Fair
Skill in testing and configuring network workstations and peripherals [KSA ID: 221]	0.271	Fair

Skill in survey, collection, and analysis of wireless LAN metadata [KSA ID: 375]	0.221	Fair
Skill in correcting physical and technical problems which impact server performance [KSA ID: 171]	0.209	Slight
Skill in diagnosing failed servers [KSA ID: 195]	0.151	Slight

Competency: Operating Systems

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Windows/Unix ports and services [KSA ID: 1121]	0.239	Fair
Knowledge of Windows command line (e.g., ipconfig, netstat, dir, nbtstat) [KSA ID: 347]	0.234	Fair
Knowledge of virtualization technologies and virtual machine development and maintenance [KSA ID: 344]	0.161	Slight
Knowledge of file system Implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]) [KSA ID: 287]	0.157	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in utilizing virtual networks for testing [KSA ID: 1117]	.123	Slight

Competency: Requirements Analysis

Ability	Fleiss Kappa	Level of Agreement
Ability to apply network programming towards client/server model [KSA ID: 1042]	.161	Slight

Competency: Systems Integration

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of how system components are installed, integrated, and optimized [KSA ID: 51]	.206	Slight

Competency: Systems Life Cycle

Skill	Fleiss Kappa	Level of Agreement
Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation [KSA ID: 204]	.166	Slight

Competency: Telecommunications

Knowledge	Fleiss Kappa	Level of Agreement
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]) [KSA ID: 278]	0.733	Substantial
Knowledge of basic concepts, terminology, and operations of a wide range of communications media (computer and telephony networks, satellite, fiber, wireless) [KSA ID: 261]	0.559	Moderate
Knowledge of telecommunications concepts [KSA ID: 133]	0.523	Moderate
Knowledge of Voice over Internet Protocol (VoIP) [KSA ID: 989]	0.467	Moderate
Knowledge of Global Systems for Mobile Communications (GSM) architecture [KSA ID: 1052]	0.258	Fair
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 [KSA ID: 1074]	0.168	Slight

Competency: Vulnerabilities Assessment

Skill	Fleiss Kappa	Level of Agreement
Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump) [KSA ID: 214]	.206	Slight
Skill in using protocol analyzers [KSA ID: 233]	.206	Slight

Linux Fundamentals Course (NCC 204)

Competency: Computer Languages

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep) [KSA ID: 342]	.733	Substantial

Competency: Information Technology Performance Assessment

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of performance tuning tools and techniques [KSA ID: 96]	.159	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in monitoring and optimizing server performance [KSA ID: 211]	0.176	Slight
Skill in identifying and anticipating server performance, availability, capacity, or configuration problems [KSA ID: 202]	0.147	Slight

Competency: Network Management

Skill	Fleiss Kappa	Level of Agreement
Skill in conducting server planning, management, and maintenance [KSA ID: 167]	.179	Slight

Competency: Operating Systems

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications) [KSA ID: 1063]	0.737	Substantial
Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems. [KSA ID: 122]	0.407	Fair
Knowledge of UNIX and Windows systems that provide radius authentication, Domain Name Server, mail, web service, FTP server, DHCP, firewall, and simple network management protocol [KSA ID: 341]	0.117	Slight

Skill	Fleiss Kappa	Level of Agreement
Skill in system administration for Unix/Linux operating systems [KSA ID: 219]	0.681	Substantial
Skill in identifying, modifying, and manipulating applicable system components (Window and/or Unix/Linux) (e.g., passwords, user accounts, files) [KSA ID: 364]	0.166	Slight
Skill in using virtual machines [KSA ID: 386]	0.129	Slight

Competency: Systems Life Cycle

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of server administration and systems engineering theories, concepts, and methods [KSA ID: 112]	.121	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in installing computer and server upgrades [KSA ID: 206]	.149	Slight

Competency: Technology Awareness

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of new technological developments in server administration [KSA ID: 89]	.166	Slight

Information Security Fundamentals Course (NCC 210)

Competency: Computer Network Defense

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of different operational environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], third generation [nation state sponsored] [KSA ID: 992]	0.281	Fair
Knowledge of defense in-depth principles and network security architecture [KSA ID: 277]	0.264	Fair
Knowledge of and experience in Insider investigations, reporting, investigative tools and laws/regulations [KSA ID: 252]	0.219	Fair
Knowledge of Intrusion Detection System (IDS) tools and applications [KSA ID: 59]	0.209	Slight
Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities) [KSA ID: 270]	0.161	Slight
Knowledge of the types of Intrusion Detection System (IDS) hardware and software [KSA ID: 146]	0.161	Slight
Knowledge of computer network defense (CND) policies, procedures, and regulations [KSA ID: 984]	0.139	Slight

Competency: Criminal Law

Knowledge	Fleiss Kappa	Level of Agreement
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., in 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 [KSA ID: 1036]	.271	Fair
Knowledge of relevant laws, policies, procedures ,or governance as they relate to work that may impact critical infrastructure [KSA ID: 1040]	.264	Fair

Competency: Cryptography

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of encryption methodologies [KSA ID: 1114]	0.527	Moderate
Knowledge of cryptology [KSA ID: 27]	0.307	Fair
Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES). [KSA ID: 25]	0.134	Slight

Competency: Data Management

Skill	Fleiss Kappa	Level of Agreement
Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Direct Algorithm [MD5]) [KSA ID: 1091]	.174	Slight

Competency: Encryption

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of digital rights management [KSA ID: 35]	.236	Fair
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in verifying the integrity of encrypted files [KSA ID: 387]	.189	Slight

Competency: External Awareness

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of external organizations and academic institutions dealing with cybersecurity issues [KSA ID: 320]	.292	Fair
Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise [KSA ID: 296]	.219	Fair
Knowledge of social dynamics of computer attackers in a global context [KSA ID: 917]	.206	Slight

Competency: Human Factors

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of human-computer interaction principles [KSA ID: 52]	.232	Fair

Competency: Incident Management

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of enterprise incident response program, roles, and responsibilities [KSA ID: 966]	0.316	Fair
Knowledge of disaster recovery and continuity of operations plans. [KSA ID: 37]	0.275	Fair
Knowledge of incident response and handling methodologies [KSA ID: 61]	0.266	Fair
Knowledge of incident categories, incident responses, and timelines for responses [KSA ID: 60]	0.226	Fair

Competency: Identity Management

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control) [KSA ID: 986]	0.465	Moderate
Knowledge of access authentication methods [KSA ID: 8]	0.416	Moderate
Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]) [KSA ID: 79]	0.348	Fair
Knowledge of policy-based and risk adaptive access controls [KSA ID: 98]	0.348	Fair

Competency: Information Assurance

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation). [KSA ID: 63]	0.523	Moderate

Knowledge of Information assurance (IA) principles used to manage risks related to the use, processing, storage, and transmission of information or data [KSA ID: 55]	0.333	Fair
Knowledge of security management [KSA ID: 110]	0.328	Fair
Knowledge of organization's enterprise information security architecture system [KSA ID: 38]	0.283	Fair
Knowledge of the Security Assessment and Authorization (SA&A) process [KSA ID: 53]	0.258	Fair
Knowledge of information assurance (IA) principles and methods that apply to software development [KSA ID: 56]	0.239	Fair
Skill	Fleiss Kappa	Level of Agreement
Skill in applying confidentiality, integrity, and availability principles [KSA ID: 156]	0.316	Fair
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 [KSA ID: 183]	0.219	Fair
Skill in designing security controls based on information assurance (IA) principles and tenets [KSA ID: 179]	0.198	Slight

Competency: Information Systems/Network Security

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption) [KSA ID: 70]	0.675	Substantial
Knowledge of security system design tools, methods, and techniques [KSA ID: 111]	0.309	Fair
Knowledge of information security systems engineering principles [KSA ID: 64]	0.264	Fair
Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins [KSA ID: 58]	0.26	Fair
Knowledge of what constitutes a network attack and the relationship to both s and vulnerabilities [KSA ID: 150]	0.241	Fair
Knowledge of host/network access controls (e.g., access control list) [KSA ID: 49]	0.221	Fair
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 [KSA ID: 77]	0.213	Fair

Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth) [KSA ID: 1072]	0.164	Slight
Knowledge of current and emerging security vectors [KSA ID: 967]	0.159	Slight
Knowledge of software-related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization) [KSA ID: 968]	0.144	Slight
Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation [KSA ID: 326]	0.142	Slight
Knowledge of security event correlation tools [KSA ID: 923]	0.117	Slight
Skill	Fleiss Kappa	Level of Agreement
Skill in implementing, maintaining, and improving established security practices [KSA ID: 205]	0.245	Fair
Skill in discerning the protection needs (i.e., security controls) of information systems and networks [KSA ID: 197]	0.204	Slight
Skill in reading and interpreting signatures (e.g., Snort) [KSA ID: 1118]	0.181	Slight

Competency: Information Systems Security Certification

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Risk Management Framework (RMF) requirements [KSA ID: 69]	.318	Fair

Competency: Information Technology Architecture

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of information technology (IT) architectural concepts and frameworks [KSA ID: 68]	.202	Slight

Competency: Information Technology Performance Assessment

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of measures or indicators of system performance and availability [KSA ID: 76]	.11	Slight

Competency: Legal, Government and Jurisprudence

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of legal governance related to Computer Network Defense (e.g., Chairman of the Joint Chief of Staff Manual, Executive Order 12333), computer monitoring, and collection. [KSA ID: 105]	.196	Slight

Competency: Mathematical Reasoning

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of information theory [KSA ID: 65]	0.288	Fair
Knowledge of computer algorithms [KSA ID: 21]	0.151	Slight

Competency: Project Management

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of information security program management and project management principles and techniques [KSA ID: 299]	.264	Fair

Competency: Public Safety and Security

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of operations security [KSA ID: 1056]	.236	Fair

Competency: Requirements Analysis

Ability	Fleiss Kappa	Level of Agreement
Ability to interpret and translate customer requirements into operational cyber actions [KSA ID: 911]	.239	Fair
Knowledge	**Fleiss Kappa**	**Level of Agreement**
Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design [KSA ID: 126]	.155	Slight

Competency: Risk Management

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of risk management processes, including steps and methods for assessing risk [KSA ID: 108]	0.367	Fair
Knowledge of organization's risk tolerance and/or risk management approach [KSA ID: 965]	0.275	Fair
Knowledge of assessment [KSA ID: 1021]	0.253	Fair

Competency: Security

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Personally Identifiable Information (PII) and Payment Card Industry (PCI) data security standards [KSA ID: 1034]	.572	Moderate
Knowledge of processes for reporting network security related incidents [KSA ID: 1011]	.224	Fair

Competency: Software Engineering

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of secure software deployment methodologies, tools, and practices [KSA ID: 1071]	.176	Slight

Competency: Systems Life Cycle

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of systems lifecycle management principles, including software security and usability [KSA ID: 129]	.161	Slight
Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly. [KSA ID: 145]	.161	Slight

Competency: Technology Awareness

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of emerging security issues, risks, and vulnerabilities [KSA ID: 952]	.418	Moderate
Knowledge of new and emerging information technology (IT) and information security technologies [KSA ID: 88]	.305	Fair
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 [KSA ID: 321]	.275	Fair

Competency: Vulnerabilities Assessment

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of system and application security and vulnerabilities [KSA ID: 123]	.226	Fair

Scripting Fundamentals (NCC 212)

Competency: Computer Languages

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of programming language structures and logic [KSA ID: 102]	0.36	Fair
Knowledge of interpreted and compiled computer languages [KSA ID: 904]	0.318	Fair
Knowledge of secure coding techniques [KSA ID: 905]	0.256	Fair
Skill	**Fleiss Kappa**	**Level of Agreement**
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) [KSA ID: 1116]	.125	Slight

Competency: Infrastructure Design

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of Extensible Markup Language (XML) schemas [KSA ID: 1064]	.26	Fair

Competency: Object Technology

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of computer programming principles such as object-oriented design [KSA ID: 23]	.253	Fair

Competency: Operating Systems

Skill	Fleiss Kappa	Level of Agreement
Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and UNIX systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data) [KSA ID: 371]	.504	Moderate

Competency: Software Development

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of software debugging principles [KSA ID: 116]	0.262	Fair
Knowledge of debugging procedures and tools [KSA ID: 1094]	0.129	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in conducting software debugging [KSA ID: 168]	.262	Fair
Skill in developing applications that can log errors, exceptions, and application faults and logging [KSA ID: 185]	.204	Slight

Competency: Software Testing and Evaluation

Skill	Fleiss Kappa	Level of Agreement
Skill in creating programs that validate and process multiple inputs, including command line arguments, environmental variables, and input streams [KSA ID: 174]	.198	Slight

Ethical Hacking and Systems Defense Course (NCC 214)

Competency: Computer Languages

Skill	Fleiss Kappa	Level of Agreement
Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump) [KSA ID: 1088]	.147	Slight

Competency: Computer Network Defense

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of general attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks) [KSA ID: 1069]	0.412	Moderate
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution) [KSA ID: 991]	0.322	Fair
Knowledge of evasion strategies and techniques (e.g., noise, stealth, situational awareness, bandwidth throttling) [KSA ID: 285]	0.232	Fair
Knowledge of concepts, principles, methods, and tools related to processing and exploitation [KSA ID: 274]	0.225	Fair
Knowledge of virtual machine aware malware, debugger aware malware, and packing [KSA ID: 1097]	0.198	Slight
Knowledge of common attack vectors on the network layer [KSA ID: 990]	0.181	Slight
Knowledge of CNE/CNA/CNO methodologies [KSA ID: 269]	0.151	Slight
Knowledge of Computer Network Defense tools, including open source tools, and their capabilities [KSA ID: 19]	0.151	Slight
Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro) [KSA ID: 1096]	0.151	Slight
Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies [KSA ID: 66]	0.134	Slight
Knowledge of malware analysis concepts and methodology [KSA ID: 1029]	0.132	Slight

Skill	Fleiss Kappa	Level of Agreement
Skill in mimicking behaviors [KSA ID: 210]	0.35	Fair
Skill in identifying obfuscation techniques [KSA ID: 1100]	0.324	Fair
Skill in analyzing anomalous code as malicious or benign [KSA ID: 1098]	0.241	Fair
Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures [KSA ID: 1101]	0.17	Slight
Skill in collecting data from a variety of Computer Network Defense resources (e.g., signals intelligence, open source intelligence, Computer Network Defense tools) [KSA ID: 353]	0.166	Slight
Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort) [KSA ID: 181]	0.164	Slight
Skill in handling malware [KSA ID: 153]	0.164	Slight
Skill in protecting a network against malware [KSA ID: 896]	0.161	Slight

Competency: Computer Skills

Skill	Fleiss Kappa	Level of Agreement
Skill in navigating mapping tools [KSA ID: 368]	.157	Slight

Competency: Human Factors

Skill	Fleiss Kappa	Level of Agreement
Skill in the use of social engineering techniques [KSA ID: 226]	.339	Fair

Competency: Information Assurance

Skill	Fleiss Kappa	Level of Agreement
Skill in recognizing and categorizing types of vulnerabilities and associated attacks [KSA ID: 895]	.245	Fair

Competency: Information Management

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of how passive and active collections supplement each other [KSA ID: 913]	.125	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in gathering information from cyber social networks (e.g., MySpace, Facebook etc.) [KSA ID: 899]	.309	Fair

Competency: Information Systems/Network Security

Skill	Fleiss Kappa	Level of Agreement
Skill in developing and deploying signatures [KSA ID: 175]	.161	Slight

Competency: Information Technology Performance Assessment

Skill	Fleiss Kappa	Level of Agreement
Skill in conducting audits or reviews of technical systems [KSA ID: 1002]	.168	Slight

Competency: Reasoning

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing intelligence [KSA ID: 338]	.189	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in analyzing data from a variety of Computer Network Defense resources (e.g., signals intelligence, open source intelligence, Computer Network Defense tools) [KSA ID: 349]	0.245	Fair
Skill in gathering and analyzing all-source information in support of indications and warnings [KSA ID: 361]	0.213	Fair
Skill in analyzing memory dumps to extract information [KSA ID: 350]	0.187	Slight

Competency: Software Development

Skill	Fleiss Kappa	Level of Agreement
Skill in using code analysis tools to eradicate bugs [KSA ID: 973]	.198	Slight

Competency: Strategic Thinking

Skill	Fleiss Kappa	Level of Agreement
Skill in determining tactics, techniques, and procedures [KSA ID: 358]	.307	Fair
Skill in identifying gaps in cyber collection capabilities [KSA ID: 914]	.168	Slight

Competency: Surveillance

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of hacking methodologies in Windows or Unix/Linux environment [KSA ID: 294]	.47	Moderate
Knowledge of surveillance detection and countermeasures [KSA ID: 329]	.275	Fair

Competency: Technology Awareness

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of emerging computer-based technology that has potential for exploitation by adversaries [KSA ID: 282]	.189	Slight
Ability	**Fleiss Kappa**	**Level of Agreement**
Ability to identify possible actor uses of a new technology [KSA ID: 921]	.187	Slight

Competency: Vulnerabilities Assessment

Knowledge	Fleiss Kappa	Level of Agreement
Knowledge of penetration testing principles, tools, and techniques (e.g., metasploit, neosploit) [KSA ID: 95]	0.737	Substantial
Knowledge of certified ethical hacking principles and techniques [KSA ID: 17]	0.733	Substantial
Knowledge of application vulnerabilities [KSA ID: 10]	0.206	Slight
Knowledge of packet-level analysis [KSA ID: 93]	0.185	Slight
Knowledge of how different file types can be used for anomalous behavior [KSA ID: 1095]	0.121	Slight
Skill	**Fleiss Kappa**	**Level of Agreement**
Skill in the use of penetration testing tools and techniques [KSA ID: 225]	0.795	Substantial
Skill in applying white hat hacking/security auditing techniques, procedures and tools [KSA ID: 352]	0.675	Substantial
Skill in utilizing exploitation tools (e.g., Foundstone, fuzzers, packet sniffers, debug) to identify system/software vulnerabilities (penetration and testing) [KSA ID: 1066]	0.673	Substantial
Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems [KSA ID: 3]	0.617	Substantial
Skill in using network analysis tools to identify vulnerabilities [KSA ID: 922]	0.566	Moderate
Skill in designing countermeasures to identified security risks [KSA ID: 177]	0.395	Fair
Skill in utilizing network analysis tools to identify software communications vulnerabilities [KSA ID: 1067]	0.286	Fair
Skill in wireless network target analysis, templating, and geolocation [KSA ID: 886]	0.226	Fair
Skill in assessing the robustness of security systems and designs [KSA ID: 160]	0.181	Slight
Skill in evaluating the adequacy of security designs [KSA ID: 199]	0.168	Slight
Ability	**Fleiss Kappa**	**Level of Agreement**
Ability to identify systemic security issues based on the analysis of vulnerability and configuration data [KSA ID: 4]	.273	Fair

Summary

An analysis of the KSAs that were mapped with moderate or higher agreement provide further insights into how the courses relate to the development of cybersecurity capability maturity. The table below summarizes the findings of the KSA mapping by indicating the percentage of the course mappings associated with developing declarative knowledge of cybersecurity concepts and principles. The panel results suggest that NCC 200 and NCC 204 are best positioned in the beginning of the learning path where the focus is conceptual understanding. NCC 210 is best positioned as an intermediate step with a nearly equal balance between declarative and more advanced forms of knowledge (i.e., procedural, conditional and situational). NCC 214 is the most advanced course with only 11% of its content found to be related to declarative understanding. NCC 212 did not have sufficient mappings to determine its appropriate position. These results verify the learning path findings reported in Section II above.

Course	Declarative Knowledge
NCC 200	69.6%
NCC 204	66.6%
NCC 210	57.1%
NCC 212	0.0%
NCC 214	11.0%

V. Mapping DHS Mission Critical Role Abilities

The final activity for the panel was to map the instructional learning objectives and the practice activities (tutorial labs) to a list of abilities (or types of intelligence) that align with the Taxonomy of Educational Objectives (Bloom, 1956; Krathwohl, Bloom, & Masia, 1964). The list of abilities resulted from a study of mission critical cybersecurity job roles conducted for the U.S. Department of Homeland Security (Assante, Tobey, & Vanderhorst, 2013).

Learning Objectives

Each ability (i.e., action verb) rated by the panel relates to a one of the six levels of Bloom's (1956) Taxonomy of Educational Objectives, as revised by subsequent research (Anderson, Krathwohl, & Bloom, 2001). All courses incl learning objectives that align with multiple Bloom levels. On average, the Bloom Level suggests the ideal position of a course in a learning path. Conceptual courses (Bloom Levels 1 and 2) should appear in the beginning phases of learning as

they focus primarily on declarative knowledge development. Applied courses (Bloom Level 3 and 4) focus primarily on procedural application or analysis of declarative knowledge. Accordingly, applied courses typically occupy the central portion of a learning path. Finally, Mastery courses (Bloom Level 5 and 6) focus on conditional or situational knowledge that differentiate experts in a field (Benner, 1984). Mastery courses typically occupy the final step in a learning path.

Two analyses were conducted of abilities identified as mission critical. First, we analyzed the panel ratings to determine which abilities may be needed to perform well in the course. Second, we analyzed where each course should fit within a sequence of educational objectives. The Bloom Level was calculated alternatively based on a minimum of fair or moderate agreement of required ability.

Network Fundamentals Course (NCC 200)

Overall, a significant, but weak level of agreement was found for the mapping of the learning objectives for NCC 200 (ICC = .402, $p < .0001$). The abilities listed in the table below are sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities was between 2.5 (moderate agreement) and 2.67 (fair agreement). These average Bloom Levels suggest this course is focused on developing understanding of fundamental concepts and principles.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Diagramming (clarifying relationships through visual representation)	.505	Moderate	2
Planning (deciding how to use resources to achieve goals)	.454	Moderate	3
Selecting tools (finding methods to facilitate solution)	.444	Moderate	3
Contextualizing (connecting related parts to the environment)	.427	Moderate	2
Summarizing (representing the whole in a condensed statement)	.407	Fair	2
Identifying inconsistency (detecting outliers/anomalies)	.318	Fair	4

Linux Fundamentals Course (NCC 204)

Overall, a moderate and significant level of agreement was found for the mapping of the learning objectives for NCC 200 (ICC = .668, $p < .0001$). The abilities listed in the table below are sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 3.25 based on fair agreement and 3.0 based on a moderate level of agreement. Both of these Bloom Level

ratings suggest that this course is focused on applying prior learning in new and more concrete situations to develop procedural knowledge.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Inventorying (retrieving from collective memory)	.510	Moderate	1
Defining team roles (deciding on roles that support a goal)	.496	Moderate	5
Identifying similarities (recognizing common attributes of parts)	.352	Fair	2
Deducing (arriving at conclusions from general principles)	.325	Fair	6

Information Security Fundamentals Course (NCC 210)

Overall, there was significant, but poor agreement found for the mapping of the learning objectives for NCC 210 (ICC = .249, $p < .0001$). The abilities listed in the table below are sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 2.73 based on fair agreement and 3.0 based on a moderate level of agreement. These Bloom Level ratings suggest that this course is focused on establishing an advanced conceptual understanding in preparation for developing procedural, conditional and situational knowledge.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Selecting tools (finding methods to facilitate solution)	.488	Moderate	3
Planning (deciding how to use resources to achieve goals)	.419	Moderate	3
Recognizing patterns (perceiving consistent repetitive occurrences)	.387	Fair	2
Summarizing (representing the whole in a condensed statement)	.386	Fair	2
Reusing solutions (adapting existing methods/results)	.371	Fair	3
Contextualizing (connecting related parts to the environment)	.367	Fair	2
Identifying differences (recognizing/distinguishing attributes)	.355	Fair	2
Simplifying (representing only primary features)	.349	Fair	4
Deducing (arriving at conclusions from general principles)	.341	Fair	6
Identifying similarities (recognizing common attributes)	.337	Fair	1
Diagramming (clarifying relationships through visual representation)	.335	Fair	2

Scripting Fundamentals (NCC 212)

Overall, there was moderate and significant agreement found for the mapping of the learning objectives for NCC 210 (ICC = .665, $p < .0001$). The abilities listed in the table below are sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 3.75 based on fair agreement and 4.0 based on a moderate level of agreement. These Bloom Level ratings suggest that this course is focused on developing mostly procedural and some conditional expertise.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Planning (deciding how to use resources to achieve goals)	.486	Moderate	3
Deducing (arriving at conclusions from general principles)	.486	Moderate	6
Selecting tools (finding methods to facilitate solution)	.441	Moderate	3
Diagramming (clarifying relationships through visual representation)	.375	Fair	2
Linear thinking (generating new ideas from previous ideas)	.372	Fair	6
Reusing solutions (adapting existing methods/results)	.363	Fair	3
Recognizing patterns (perceiving consistent repetitive occurrences)	.355	Fair	2
Lateral thinking (generating new ideas from associations)	.352	Fair	6
Choosing alternatives (selecting alternatives using criteria)	.345	Fair	5
Identifying differences (recognizing/distinguishing attributes of parts)	.326	Fair	2
Ensuring sufficiency (verifying data quantity/quality to suit the context)	.321	Fair	5
Contextualizing (connecting related parts to the environment)	.316	Fair	2

Ethical Hacking and Systems Defense Course (NCC 214)

Overall, moderate and significant agreement was found for the mapping of the learning objectives for NCC 210 (ICC = .644, $p < .0001$). The abilities listed in the table below are sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 3.47 based on fair agreement and 3.0 based on a moderate level of agreement. These Bloom Level ratings suggest that this course is focused on developing procedural knowledge.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Selecting tools (finding methods to facilitate solution)	.642	Substantial	3
Planning (deciding how to use resources to achieve goals)	.479	Moderate	3
Choosing alternatives (selecting alternatives using criteria)	.472	Moderate	5
Contextualizing (connecting related parts to the environment)	.471	Moderate	4
Identifying differences (recognizing/distinguishing attributes of parts)	.457	Moderate	2
Reusing solutions (adapting existing methods/results)	.452	Moderate	3
Inferring (drawing conclusions from evidence and logic)	.401	Fair	5
Deducing (arriving at conclusions from general principles)	.398	Fair	6
Identifying similarities (recognizing common attributes of parts)	.385	Fair	1
Lateral thinking (generating new ideas from associations)	.364	Fair	6
Recognizing patterns (perceiving consistent repetitive occurrences)	.363	Fair	2
Diagramming (clarifying relationships through visual representation)	.349	Fair	2
Predicting (forecasting from experience)	.342	Fair	4
Identifying inconsistency (detecting outliers/anomalies)	.313	Fair	4
Experimenting (inferring from empirical study)	.313	Fair	4

Practice Labs

Only three of the five courses have labs related to them: NCC 200, NCC 210, and NCC 214. A significant, but weak level of agreement was found for the mapping of the labs to mission critical abilities (ICC = .468, $p < .0001$). The highest agreement was found for the Network Fundamentals (NCC 200) and Ethical Hacking and Systems Defense (NCC 214) courses. The tables below indicate the abilities found to be most related (ranked by agreement) to the labs used in each course.

Network Fundamentals Course (NCC 200)

The NCC 200 course uses two of the fifteen labs in the curriculum library: Exploiting Wireless Security and Implementing NAT and Allowing Remote Access V2. Six abilities were mapped based on the level of panelist agreement. These abilities are listed in the table below,

sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 3.17 based on fair agreement and 3.5 based on a moderate level of agreement. These Bloom Level ratings suggest that the labs for this course are focused on the application of procedural knowledge to develop skills through practice.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Selecting tools (finding methods to facilitate solution)	.615	Substantial	3
Contextualizing (connecting related parts to the environment)	.468	Moderate	4
Recognizing patterns (perceiving consistent repetitive occurrences)	.408	Fair	2
Experimenting (inferring from empirical study)	.394	Fair	4
Planning (deciding how to use resources to achieve goals)	.349	Fair	3
Reusing solutions (adapting existing methods/results)	.329	Fair	3

Information Security Fundamentals Course (NCC 210)

The NCC 210 course uses all fifteen labs in the curriculum library. The two abilities mapped to this course are listed in the table below sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 3.00 based a fair level of agreement found for the panel ratings. This Bloom Level suggests that the labs for this course are focused primarily on the application of declarative knowledge to validate conceptual understanding as a foundation upon which to build cybersecurity expertise in future courses.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Selecting tools (finding methods to facilitate solution)	.384	Fair	3
Planning (deciding how to use resources to achieve goals)	.357	Fair	3

Ethical Hacking and Systems Defense Course (NCC 214)

The NCC 214 course uses five of the fifteen labs in the curriculum library: Implementing Security Policies on Windows and Linux; Vulnerability Scanners and Penetration Testing; Exploiting Wireless Security; Implementing NAT and Allowing Remote Access V2; and Implementing Common Protocols and Services. Six abilities were mapped based on the level of

panelist agreement. These abilities are listed in the table below, sorted by the level of agreement which may suggest how important each ability may be to performing well in this course. The average Bloom Level for this list of abilities is 3.13 based on fair agreement and 3.33 based on a moderate level of agreement. These Bloom Level ratings suggest that the labs for this course are focused on the application of procedural knowledge to develop skills through practice.

Ability	Fleiss Kappa	Level of Agreement	Bloom Level
Selecting tools (finding methods to facilitate solution)	.545	moderate	3
Contextualizing (connecting related parts to the environment)	.423	moderate	4
Planning (deciding how to use resources to achieve goals)	.413	moderate	3
Identifying differences (recognizing/distinguishing attributes of parts)	.373	fair	1
Recognizing patterns (perceiving consistent repetitive occurrences)	.354	fair	2
Identifying similarities (recognizing common attributes of parts)	.321	fair	1
Deducing (arriving at conclusions from general principles)	.317	fair	6
Filtering (selecting data based on criteria)	.314	fair	5

Summary

The table below provides a summary comparison that integrates the findings from Sections II, IV, V and VI of the report. Since the Bloom Taxonomy begins at level 1 while the JP-CMM begins with level 0, the Bloom Level was adjusted downward to facilitate the comparison. Applying three methods of classifying courses by level within a learning path reduces common method bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Comparing the results of the three methods enables validation of the estimated learning path provided in Section II and reproduced in the Discussion section below. Overall, a comparison of results from the three methods support the learning path estimates for three courses: NCC 200, NCC 210, and NCC 214. The three course sequence shows a decreasing focus on knowledge development corresponds with increasing capability maturity and ability.

Findings for the other two courses were significantly limited by the fewer mappings that met cutoff requirements. These results suggest that these courses may provide complementary competency development that does not map to current definitions of cybersecurity capability maturity in the existing workforce frameworks. In conclusion, NCC 204 and NCC 212 may be excellent additions to the Foundation Series of courses. The findings also suggest that NCC 214 contains more advanced content and assumes more advanced abilities in the learner. These

findings suggest NCC 214 may be best positioned as a Pathway Course that is targeted towards individuals seeking to develop specialized expertise in operational security and penetration testing.

Course	Knowledge Focus	Maturity Level	Bloom Level (adjusted)
Network Fundamentals (NCC 200)	69.6%	1.35	1.50 - 1.67
Linux Fundamentals (NCC 204)[3]	66.7%	1.00	2.00 - 2.25
Information Security Fundamentals (NCC 210)	57.1%	1.80	1.73 - 2.00
Scripting Fundamentals (NCC 212)[2]	0.0%	N/A	2.75 -3.00
Ethical Hacking and Systems Defense (NCC 214)	11.1%	2.56	2.13 - 2.33

DISCUSSION

The National CyberWatch Center (NCC) Curriculum Standards Panel (CSP) curriculum mapping project was undertaken to initiate the development of the nation's first competency-based, mastery learning curriculum for cybersecurity education. This innovation in cybersecurity education is needed to close a widening skills gap based on an estimated need in the next three years for 25% more workers who possess the capability maturity to protect and defend our nation's computing infrastructure. A panel of over 100 subject matter experts was assembled to map five courses projected as components of a core curriculum. Over the course of two months the panelists deliberated over the alignment of the content of these courses with four national competency frameworks: the Job Performance and Capability Maturity Model; the Core Knowledge Units for the Centers of Academic Excellence in Cyber Defense; the National Cybersecurity Workforce Framework KSAs; and the Department of Homeland Security's Mission Critical Abilities. The analysis produced a recommended learning path (Figure 3 reproduced below) that is consistent with a holistic model for enhancing the capability maturity of the cybersecurity workforce (Assante and Tobey, 2011). An evidence-based development model was proposed to guide the analysis and refinement of existing course content into competency-based modules that are consistent with this learning path. This report examines the results of the first three steps in this eleven-step model:

1. Recruitment and selection of renowned educators/instructional designers in the course content domain to provide subject matter expertise necessary to ensure validation of instructional designs.

2. A panel of 20-40 subject matter experts (instructors, industry practitioners, and instructional designers) participates in identifying, defining, and reaching a consensus about important competencies to which the curriculum is aligned.

3. Competencies are clearly defined, understood, and accepted by relevant stakeholders through a systematic process of public review and comment.

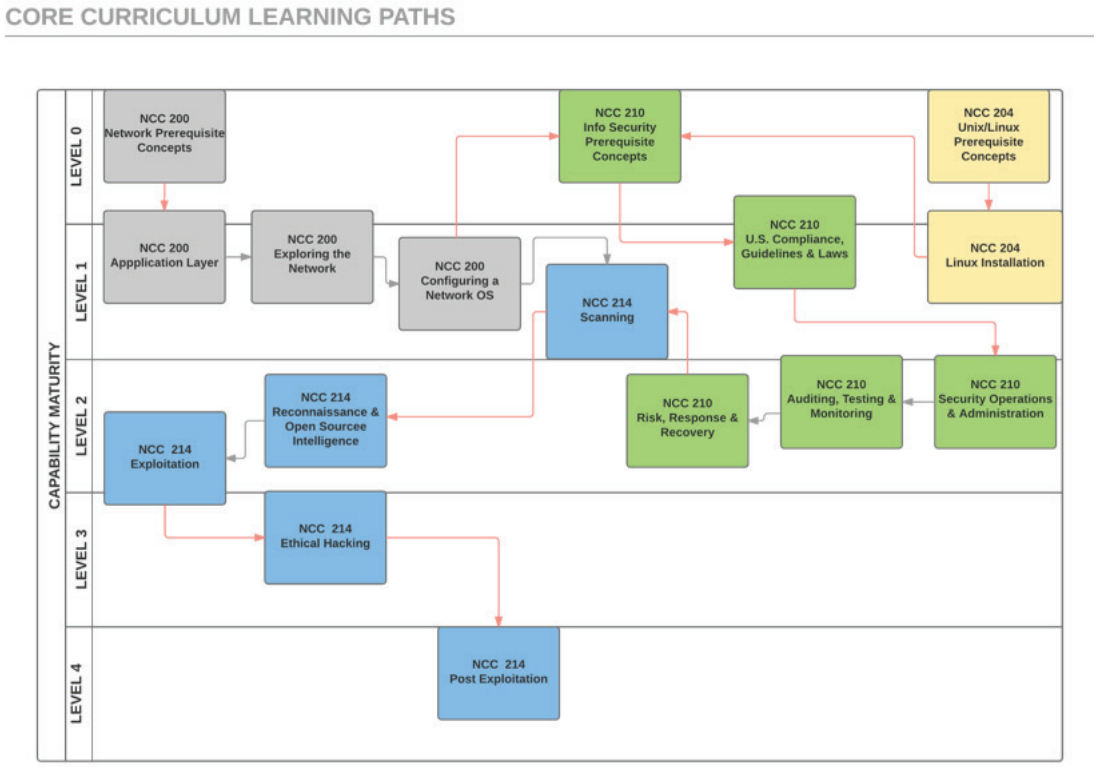


Figure 3. Mapping of Course Topics to Capability Maturity Levels

The primary insight gained from the NCC-CSP analysis was the need for two distinct groups of cybersecurity courses: a Foundation Series that develops mastery in the fundamental concepts, principles and procedures and a Pathway Series that extends and applies this understanding to develop the skills and abilities that differentiate experts in the field (Tobey, Reiter-Palmon, & Callens, 2012). Figure 4 depicts an example of how the existing library of National CyberWatch Center instructional content might be arranged. This graphic shows how the Foundation Series is designed to cover the NSA CAE-CD Core Knowledge Units while the Pathway Series extends this foundation to address the broad array of specialty areas defined in the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework.

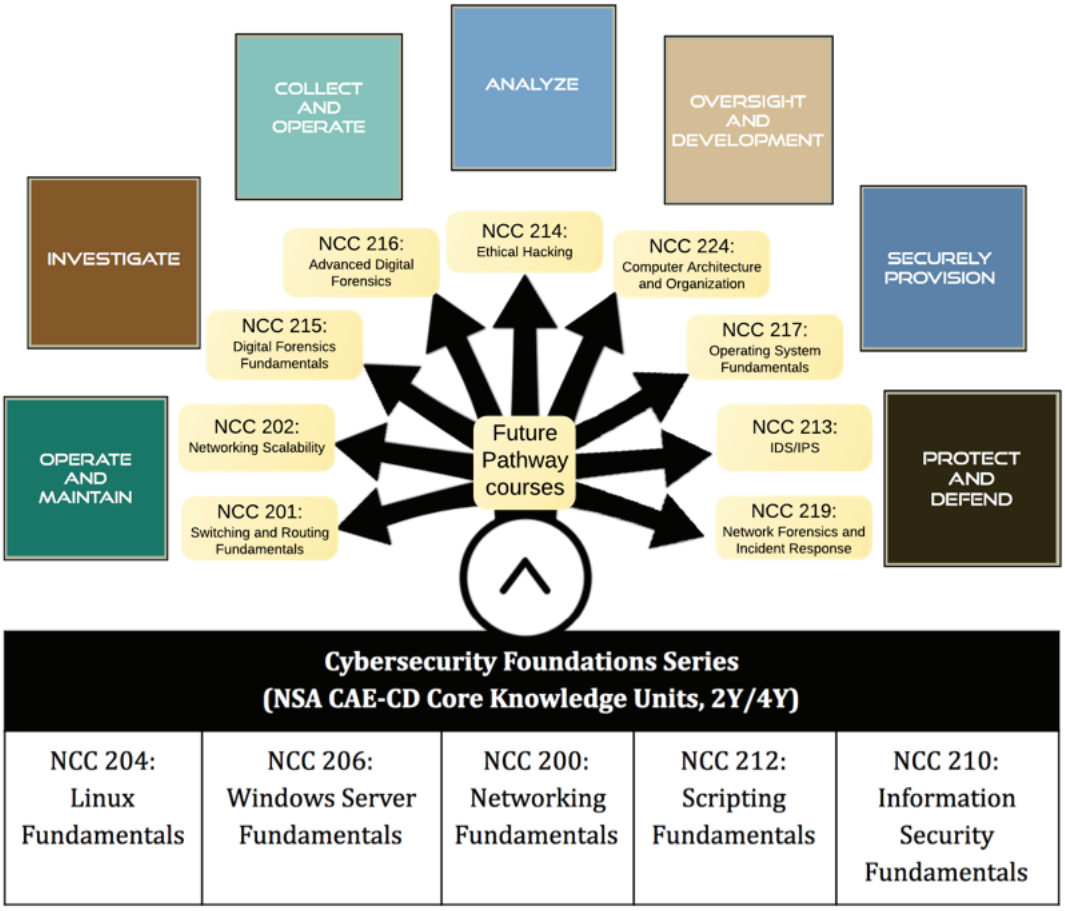


Figure 4. Pathway from Foundation Series through Pathway courses to NCWF Specialty Area Competencies

Based on the findings reported here the NCC 214 course was removed from the core curriculum which was renamed the Foundation Series. In its place, another fundamentals course, NCC 206: Windows Server Fundamentals, was added to address a gap in network operating system coverage. The mapping of the five courses to the NSA's CAE-CD Core Knowledge Units described in Section II above suggested that NCC 214 was deepening, but not adding to coverage of the Core KUs. This finding was further supported by evidence from an analysis of the capability maturity levels and relative focus on knowledge vs. skill development found to be mapped to each course. These findings may inform future mapping beyond that already conducted (Burley, Tobey, Pusey & Leary, 2014) between the KUs and the NICE KSAs.

Each of the mappings provide guidance for further development of the National CyberWatch Center Standard Curriculum in accordance with the 11-step process that will guide National CyberWatch Center instructional design practices. The need for additional or modified instructional modules and labs is suggested for any task, knowledge, skill, or ability mapping that found only slight agreement among the panel members. These areas are likely to be important for the course, but are not currently well developed to cover fully the content required to develop capability maturity in the listed item. There is much opportunity for improvement as all courses

have numerous areas which meet this criteria. Below is a review of the most salient improvements required.

The mapping of learning objectives to the JP-CMM responsibility areas suggests additional instruction modules should be developed in the area of Develop and Manage Personnel. These "soft skills" have not been well covered in prior course designs. The JP-CMM indicates that these skills predict approximately 45% of cybersecurity professional job performance (Tobey, Reiter-Palmon, & Callens, 2012).

The mapping to the JP-CMM tasks which resulted in the learning path model shown in Figure 3 above suggests that formative assessments be developed to ensure learners are ready for the instructional material that raises maturity levels. Research shows that without adequate preparation learners may become disengaged (Tobey, Pusey, & Burley, 2014). Each task that is mapped to a course should be related to tutorial and challenge labs that enable the learner to practice the procedures required to execute the task. Most of these labs have yet to be developed.

The mapping to the knowledge areas (KUs and knowledge components of NICE) similarly suggests a need for additional instructional modules. Some of these may exist outside traditional information technology or cybersecurity courses, such as in Basic Data Analysis and Probability and Statistics. The mapping to the National Cybersecurity Workforce Framework (NCWF) could be used as a guide to develop formative assessments of prerequisite knowledge. These assessments would indicate the degree to which learners are mastering:

1. declarative understanding necessary for proficiency
2. procedural understanding necessary for competence
3. conditional and situational understanding necessary to become an expert

The course KSA mappings with at least a moderate level of panelist agreement could also guide development of assessment instruments that could verify the maturity levels identified as obtainable for each course in Section II above. Concept inventory assessments have been used for many years assess proficiency and the misconceptions which limit conceptual mastery in the related domain of computer science (e.g., Almstrum, Henderson, Harvey, et al., 2006; Bayman & Mayer, 1983; Goldman, Gross, Heeren et al., 2008; Sudol & Jaspan, 2010). Recently, a concept inventory development process has begun for assessing core conceptual knowledge in cybersecurity (Parekh, DeLatte, Herman, et al., 2016). The results of this curriculum mapping should inform these efforts.

Finally, the mapping to the DHS Mission Critical Role abilities suggests that the alignment of prerequisites applies not only to knowledge but also to ability. These results showed that the instructional content for NCC 200 and NCC 210 was well aligned. For these two courses the capability maturity level and the Bloom Taxonomy level were within the same range. A cautionary note was suggested by this analysis for NCC 204 and NCC 214. In the former case, the Bloom level

was far above the capability maturity level suggesting that a linux fundamentals course should include much more procedural, conditional and situational knowledge modules. Including these modules may also address the poor alignment of this course with the four workforce competency frameworks analyzed in this study. The NCC 214 course may have the opposite issue. The panel mappings suggest that the capability maturity level targeted by the extensive skill focus of this course may require higher ability than was being developed by the content. Accordingly, NCC 214 should include more scenario-based challenge labs or planned integration of the National Cyber League or other relevant cybersecurity competitions where detailed score reports can facilitate formative assessment of ability development.

The remainder of this discussion section will analyze the comments received from the panel review of this report. Once all the comments from the panel have been collected and analyzed, this draft report will be distributed for public review and comment. A final revision of the report will incorporate both the panel and public commentary.

REFERENCES

Almstrum, V. L., Henderson, P. B., Harvey, V., Heeren, C., Marion, W., Riedesel, C., … Tew, A. E. (2006). Concept inventories in computer science for the topic discrete mathematics. In ACM SIGCSE Bulletin (Vol. 38, pp. 132–145). ACM.

Anderson, J. R., Corbett, A. T., Koedinger, K. R., & Pelletier, R. (1995). Cognitive tutors: Lessons learned. The Journal of the Learning Sciences, 4(2), 167–207.

Anderson, L. W., Krathwohl, D. R., & Bloom, B. S. (2001). A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. New York: Longman.

Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. IEEE IT Professional, 13, 12–15.

Assante, M. J., Tobey, D. H., Conway, T. J., Leo, R., Januszewki, J., & Perman, K. (2013). Developing secure power systems professional competence: Alignment and gaps in workforce development programs (Technical Report No. 2013- SGC-02). Idaho Falls, ID: National Board of Information Security Examiners.

Banta, T. W., & Palomba, C. A. (2014). Assessment essentials: Planning, implementing, and improving assessment in higher education (Second Edition). San Francisco: Jossey-Bass & Pfeiffer Imprints. Retrieved from http://BZ6FJ9FL8E.search.serialssolutions.com/?V=1.0&L=BZ6FJ9FL8E&S=JCs&C=TC0001332444&T=marc

Bayman, P., & Mayer, R. E. (1983). A diagnosis of beginning programmers' misconceptions of BASIC programming statements. Communications of the ACM, 26(9), 677–679.

Benner, P. E. (1984). From novice to expert: Excellence and power in clinical nursing practice. Menlo Park, CA: Addison-Wesley.

Bloom, B. S. (1956). Taxonomy of educational objectives: The classification of educational goals. New York,: Longmans, Green.

Boehm, B., Grünbacher, P., & Briggs, R. O. (2001). EasyWinWin: A groupware-supported methodology for requirements negotiation. In Proceedings of the 23rd International Conference on Software Engineering (pp. 720–721). IEEE Computer Society. Retrieved from http://sci-hub.cc/http://dl.acm.org/citation.cfm?id=381607

Bransford, J., Brown, A., & Cocking, R. R. (2000). How people learn: Brain, mind, experience, and school. Washington, D.C.: National Academy Press.

Briggs, R. O., & Gruenbacher, P. (2002). EasyWinWin: Managing complexity in requirements negotiation with GSS. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS). IEEE. Retrieved from https://www.researchgate.net/profile/Robert_Briggs/publication/3942602_EasyWinWin_Managing_Complexity_in_Requirements_Negotiation_with_GSS/links/0a85e530bf09c4a361000000.pdf

Briggs, R. O., Vreede, G.-J. de, Nunamaker, J. F. J., & Tobey, D. H. (2001). ThinkLets: Achieving predictable, repeatable patterns of group interaction with group support systems (GSS). Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 1057–1065.

Brown, P. C., Roediger III, H. L., & McDaniel, M. A. (2014). Make it stick: The science of successful learning. Cambridge, MA: The Belknap Press of Harvard University Press.

Burley, D. L., Tobey, D. H., Pusey, P., & Leary, M. (2014). Mapping Report: Centers of Academic Excellence (CAE) Knowledge Units (KUs) to the National Initiative for Cybersecurity Education (NICE) Knowledge, Skills, and Abilities (KSAs) (Technical Report). Washington, DC: Department of Homeland Security.

Chi, M. T. H. (2005). Commonsense conceptions of emergent processes: Why some misconceptions are robust. Journal of the Learning Sciences, 14(2), 161–199. https://doi.org/10.1207/s15327809jls1402_1

Chi, M. T. H., & Ohlsson, S. (2005). Complex declarative learning. In K. J. Holyoak & R. G. Morrison (Eds.), The Cambridge handbook of thinking and reasoning (pp. 371–399). New York: Cambridge University Press.

Craig, R. (2013). The skills gap and the spit-take. University Ventures Letter, 3(21). Retrieved from http://us2.campaign-archive1com/?u=928797bbde35bedb144213a5c&id=ae1ed0bd32&e=80df6124d4

Feltovich, P. J., Coulson, R. L., & Spiro, R. J. (2001). Learners' (mis)understanding of important and difficult concepts: A challenge to smart machines in education. In K. D. Forbus & P. J. Feltovich (Eds.), Smart machines in education (pp. 349–375). Menlo Park, CA: MIT Press.

Fletcher, J. D., & Morrison, J. E. (2015). Accelerating development of expertise: A digital tutor for Navy technical training. Alexandria, VA: Institute for Defense Analyses.

Goldman, K., Gross, P., Heeren, C., Herman, G., Kaczmarczyk, L., Loui, M. C., & Zilles, C. (2008). Identifying important and difficult concepts in introductory computing courses using a delphi process. ACM SIGCSE Bulletin, 40(1), 256–260.

Gray, G. L., Evans, D., Cornwell, P., Costanzo, F., & Self, B. (2003). Toward a nationwide dynamics concept inventory assessment test. In American Society for Engineering Education Annual Conference & Exposition. Retrieved from http://www.esm.psu.edu/dci/papers/asee-dci-nashville.pdf

Grossman, R., Spencer, J. M., & Salas, E. (2013). Enhancing naturalistic decision making and accelerating expertise in the workplace: Training strategies that work. In S. Highhouse, R. S. Dalal, & E. Salas (Eds.), Judgment and decision making at work (pp. 277–325). New York: Routledge.

Hake, R. R. (1998). Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. American Journal of Physics, 66(1), 64–74.

Hammer, D. (1996). Misconceptions or p-prims: How may alternative perspectives of cognitive structure influence instructional perceptions and intentions. The Journal of the Learning Sciences, 5(2), 97–127.

Harpstead, E., Myers, B. A., & Aleven, V. (2013). In search of learning: Facilitating data analysis in educational games. In CHI '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 79–88). Paris, France: Association of Computing Machinery.

Herman, G. L., Loui, M. C., & Zilles, C. (2010). Creating the digital logic concept inventory. In Proceedings of the 41st ACM technical symposium on Computer science education (pp. 102–106). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1734298

Higgs, J. (2013). Practice-Based education pedagogy: Professional pedagogy for professional education. In J. Higgs, D. Sheehan, J. B. Currens, W. Letts, & G. M. Jensen (Eds.), Realising Exemplary Practice-Based Education (pp. 3–12). SensePublishers.

Hoffman, R. R., Andrews, D., Fiore, S. M., Goldberg, S., Andre, T., Freeman, J., … Klein, G. (2010). Accelerated Learning: Prospects, Issues and Applications. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54(4), 399–402. https://doi.org/10.1177/154193121005400427

Hoffman, R. R., & Feltovich, P. J. (2010). Accelerated Proficiency and Facilitated Retention: Recommendations Based on an Integration of Research and Findings from a Working Meeting (p. 377). Mesa, AZ: Air Force Research Laboratory.

Jones, E. A., & Voorhees, R. A. (2002). Defining and assessing learning: Exploring competency-based initiatives. Report of the National Postsecondary Education Cooperative Working Group on Competency-Based Initiatives in Postsecondary Education. Washington, D.C.: National Center for Education Statistics, Office of Educational Research and Improvement, U.S. Dept. of Education.

Khan, S. (2012). The one world schoolhouse: Education reimagined. New York: Twelve Hatchett Book Group.

Klymkowsky, M. W., Taylor, L. B., Spindler, S. R., & Garvin-Doxas, R. K. (2006). Two-dimensional, implicit confidence tests as a tool for recognizing student misconceptions. Journal of College Science Teaching, 36(3), 44–48.

Kyllonen, P. C., & Shute, V. J. (1989). A taxonomy of learning skills. In P. L. Ackerman, R. J. Sternberg, & R. Glaser (Eds.), Learning and individual differences: Advances in theory and research (pp. 117–163). New York: W.H. Freeman.

LeBreton, J. M., & Senter, J. L. (2008). Answers to 20 questions about interrater reliability and interrater agreement. Organizational Research Methods, 11, 815–852.

Manske, M., & Conati, C. (2005). Modelling learning in an educational game. In C.-K. Looi, M. Gord, B. Bredeweg, & J. Breuker (Eds.), Artificial intelligence in education: Supporting learning through intelligent and socially informed technology (pp. 411–418). Amsterdam: Ios Press.

Morgan, S. (2016, January 2). One Million Cybersecurity Job Openings In 2016. Retrieved January 5, 2017, from http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/

O'Neil, L. R., Assante, M. J., & Tobey, D. H. (2012). Smart Grid Cybersecurity: Job Performance Model Report (Technical Report No. PNNL-21639). Alexandria, VA: National Technical Information Service.

Özdemir, G., & Clark, D. B. (2007). An overview of conceptual change theories. Eurasia Journal of Mathematics, Science & Technology Education, 3(4), 351–361.

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2016). Identifying core concepts of cybersecurity: Results of two Delphi processes. Working paper, University of Maryland, Baltimore County.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology, 88(5), 879–903.

Razzaq, L., Patvarczki, J., Almeida, S. F., Vartak, M., Feng, M., Heffernan, N. T., & Koedinger, K. R. (2009). The Assistment Builder: Supporting the life cycle of tutoring system content creation. IEEE Transactions on Learning Technologies, 2(2), 157–166.

Roediger, H. L., & Pyc, M. A. (2012). Inexpensive techniques to improve education: Applying cognitive psychology to enhance educational practice. Journal of Applied Research in Memory and Cognition, 1(4), 242–248.

Savinainen, A., & Scott, P. (2002). The Force Concept Inventory: A tool for monitoring student learning. Physics Education, 37(1), 45–52.

Soh, K. C. (2010). Grade point average: What's wrong and what's the alternative? Journal of Higher Education Policy and Management, 33(1), 27–36.

Soule, R., Tobey, D. H., & Gandhi, R. (2014). Assessing learner readiness for tough cases. Presented at the Academy of Management Annual Conference, Philadelphia, PA.

Sternberg, R. J. (2014). A model for instruction and assessment of cognitive readiness. In H. F. O'Neil, R. S. Perez, & E. L. Baker (Eds.), Teaching and measuring cognitive readiness (pp. 71–92). New York: Springer.

Sudol, L. A., & Jaspan, C. (2010). Analyzing the strength of undergraduate misconceptions about software engineering. In Proceedings of the Sixth international workshop on Computing education research (pp. 31–40). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=1839601

Tew, A. E., & Guzdial, M. (2010). Developing a validated assessment of fundamental CS1 concepts. In Proceedings of the 41st ACM technical symposium on Computer science education (pp. 97–101). ACM.

Tobey, D., Assante, M., King, S., & Ziegler, K. (2010, August 24). Developing Ground Truth Expertise in Smart Grid Security Specialists. National Board of Information Security Examiners.

Tobey, D. H. (2011a). A competency model of advanced threat response. ATR Working Group Report NBISE-ATR-11-02. Idaho Falls, ID: National Board of Information Security Examiners.

Tobey, D. H. (2011b, October). From cybersecurity competencies to a job peformance model. Presented at the First Annual National Initiative for Cybersecurity Education Workshop, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://www.academia.edu/1702967/NICE_-_From_cybersecurity_competencies_to_a_job_performance_model

Tobey, D. H. (2012). Certifying the Workforce of the Future: Legislative priorities. Presentation presented at the Congressional Research Service Seminar on Cybersecurity: Issues and Options for Workforce Recruitment, Education, and Development, Washington, D.C.

Tobey, D. H. (2013). A vignette-based method for improving cybersecurity talent management through cyber defense competition design (Working paper No. Mission Critical Role Project, Supplemental). Idaho Falls, ID: National Board of Information Security Examiners.

Tobey, D. H., Pusey, P., & Burley, D. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the National Cyber League. ACM InRoads, 5(1), 53–56.

Tobey, D. H., Reiter-Palmon, R., & Callens, A. (2012). Predictive Performance Modeling: An innovative approach to defining critical competencies that distinguish levels of performance. OST Working Group Report. Idaho Falls, ID: National Board of Information Security Examiners.

Van Den Broek, P., & Kendeou, P. (2008). Cognitive processes in comprehension of science texts: The role of co-activation in confronting misconceptions. Applied Cognitive Psychology, 22(3), 335–351.

Van Lehn, K. (1990). Mind bugs: The origins of procedural misconceptions. MIT Press.

Van Merrienboer, J. J., & Sweller, J. (2005). Cognitive load theory and complex learning: Recent developments and future directions. Educational Psychology Review, 17(2), 147–177.

Weise, M. R., & Christensen, C. M. (2014). Hire education: Mastery, modularization, and the workforce revolution. Clayton Christensen Institute for Disruptive Innovation.

Williamson, K. E., Willoughby, S., & Prather, E. E. (2013). Development of the Newtonian gravity concept inventory. Astronomy Education Review, 12(1).

Wu, Y., Siy, H., & Gandhi, R. (2011). Empirical results on the study of software vulnerabilities. In Proceedings of the International Conference on Software Engineering (pp. 964–967). Honolulu, HI: Association for Computing Machinery.

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

National CyberWatch Center
Prince George's Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org

National CyberWatch Center Curriculum Standards Panel
Technical Report: CSP-CM170201, Version 1.0
February 6, 2017