January 2018

Information Security Fundamentals Curriculum Standards Panel (CSP) Special Interest Group (SIG)

New Member Welcome Packet

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

www.nationalcyberwatch.org

Welcome Packet for ISF Curriculum Standards SIGs

Welcome to the ongoing Cybersecurity Foundation Series Curriculum Standards Panel – specifically the Special Interest Groups (SIGs) for the Information Security Fundamentals (ISF) course, working on content development for course modules. The purpose of this packet is to provide you with background on the NCC efforts up to this point, and give you some guidance on participating in one or more of the SIGs.

There are links on the following pages for joining the necessary online groups.

Questions may be directed to: Casey O'Brien at **cobrien [at] nationalcyberwatch [dot] org**

Definitions of Acronyms and Abbreviations

- **CSEC-2017**: Cybersecurity Curriculum Guidelines v.0.95 (by Joint Task Force on Cybersecurity Education)
- **CSF**: "Cybersecurity Framework" (NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.0)
- **CSP**: Curriculum Standards Panel (National CyberWatch Center)
- **ISF**: Information Security Fundamentals Course
- **JP-CMM**: Job Performance Capability Maturity Model (U.S. Dept. of Homeland Security)
- **KSAs**: Knowledge, Skills, and Abilities
- **NCC**: National CyberWatch Center
- **NCWF**: NICE Cybersecurity Workforce Framework
- **NICE**: National Initiative for Cybersecurity Education (under NIST)
- **NIST**: National Institute of Standards and Technology (U.S. Dept. of Commerce)
- **NSA CAE**: National Security Agency, Centers for Academic Excellence in Cybersecurity Defense
- **SIG**: Special Interest Group
- **TAWG**: Topic Area Working Group

Curriculum Standards Panel – Phases

NCC Core Curriculum Mapping

This phase was conducted from September through December 2016. This effort mapped topics and learning objectives from five NCC foundational information security courses to NSA CAE Knowledge Units, NCWF Knowledge Areas, NSA/NICE skills, national cybersecurity maturity model tasks and concepts, and situational judgements and abilities. The result was a mapping from NCC foundational courses to NCWF Specialty Areas and maturity model competencies.

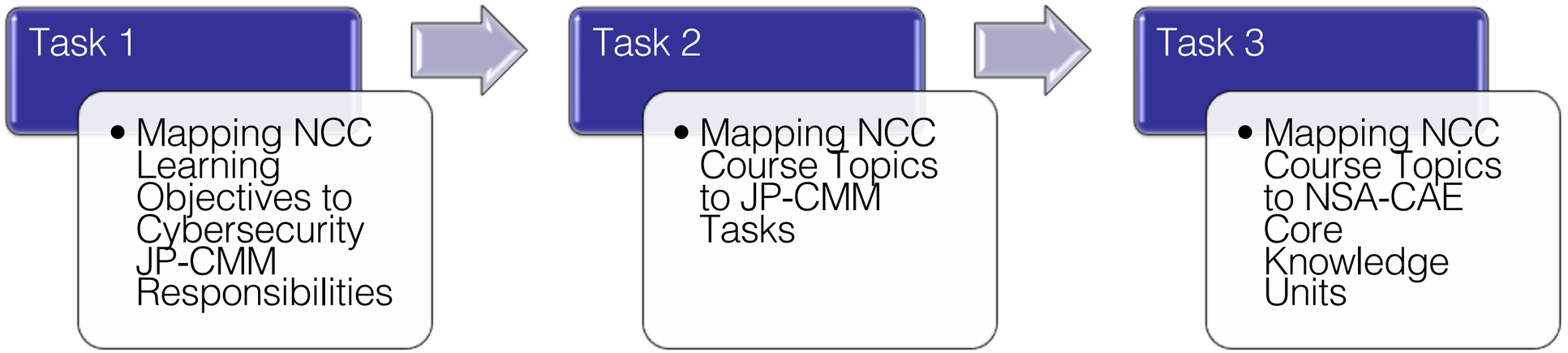
Information Security Fundamentals Curriculum

This phase was conducted from September through November 2017.This effort focused on further mapping and prioritizing course topics and learning objectives from several academic and certification courses with categories from the NIST Cybersecurity Framework, knowledge units from the CSEC-2017 curriculum guidance, job responsibilities, and responsibility areas. The result is identification of seven key learning objectives to start creating learning modules.

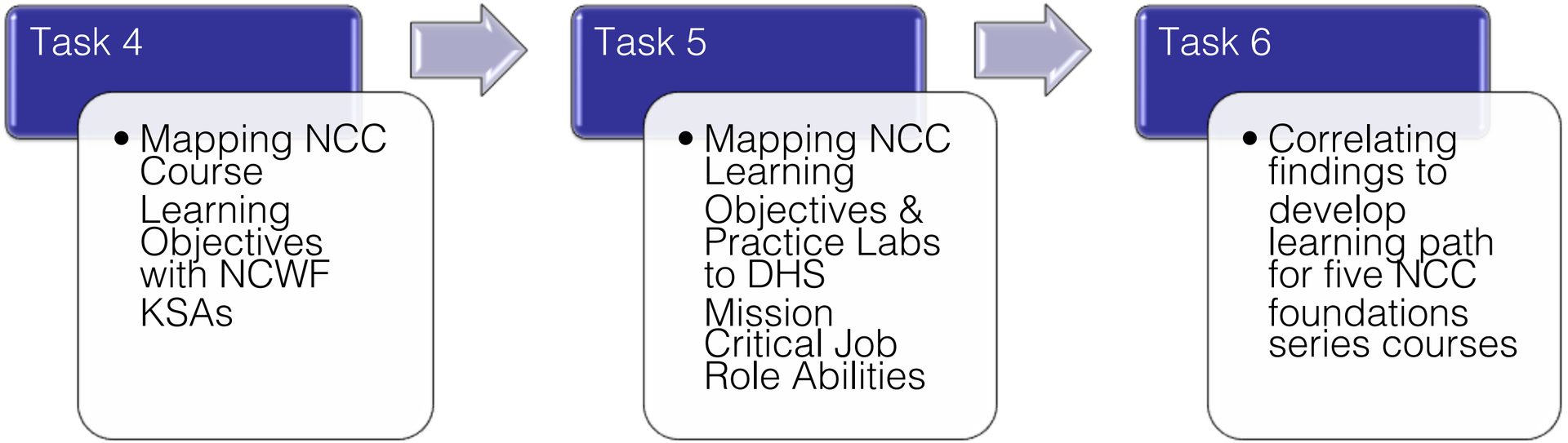
ISF Curriculum Content Development

This current phase started in January 2018 and will be ongoing until further notice. The tasks being performed are the creation of instructional design materials to develop learning modules based on the Learning Objectives mapped and prioritized within the NCWF domains in the prior phase. This phase consists of one Special Interest Group (SIG) per Learning Objective. Panel members may participate in one or more SIGs.

Flow of Tasks – 2016 Core Curriculum Mapping

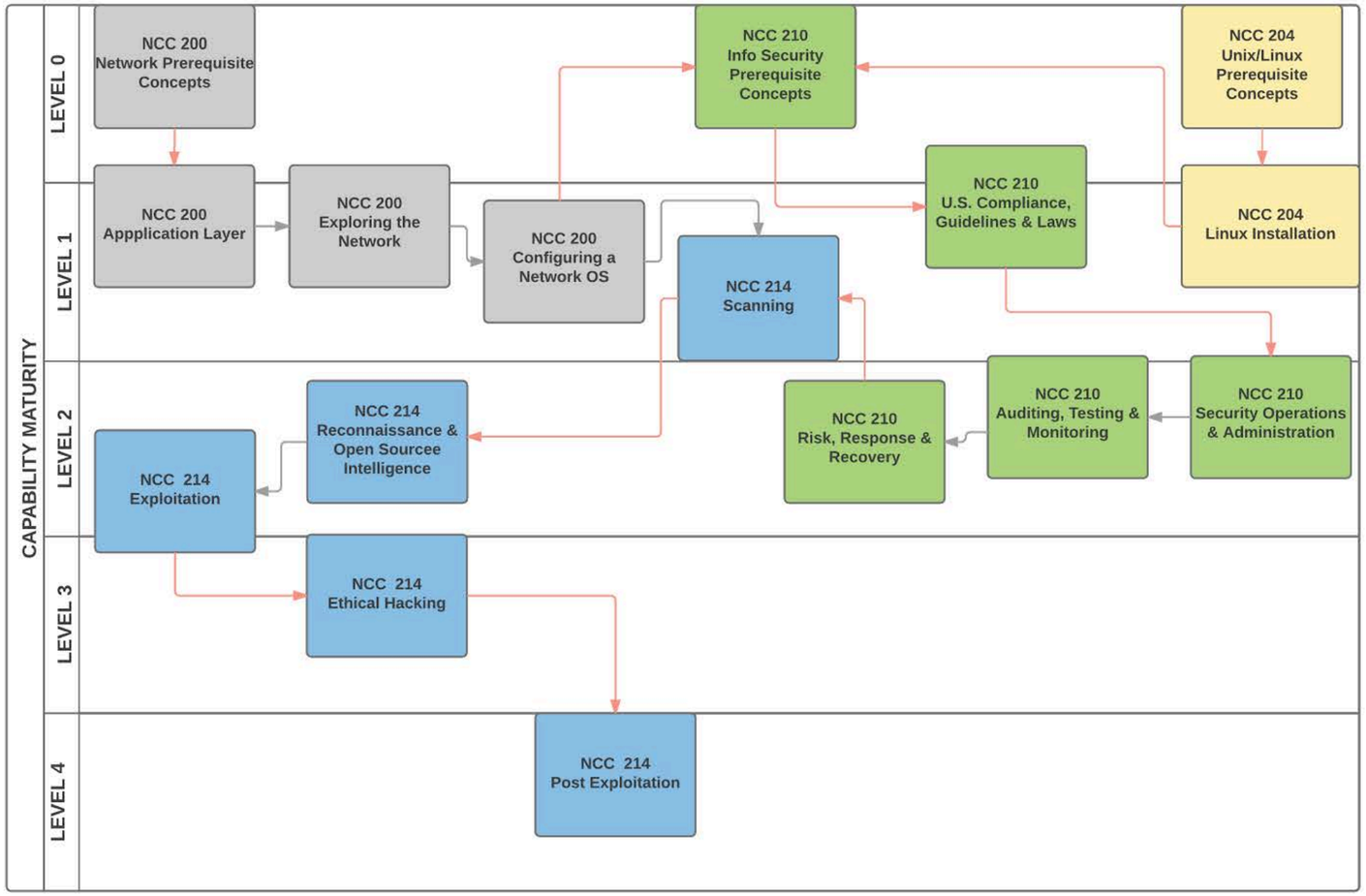


Flow of Tasks – 2016 Core Curriculum Mapping (cont'd)



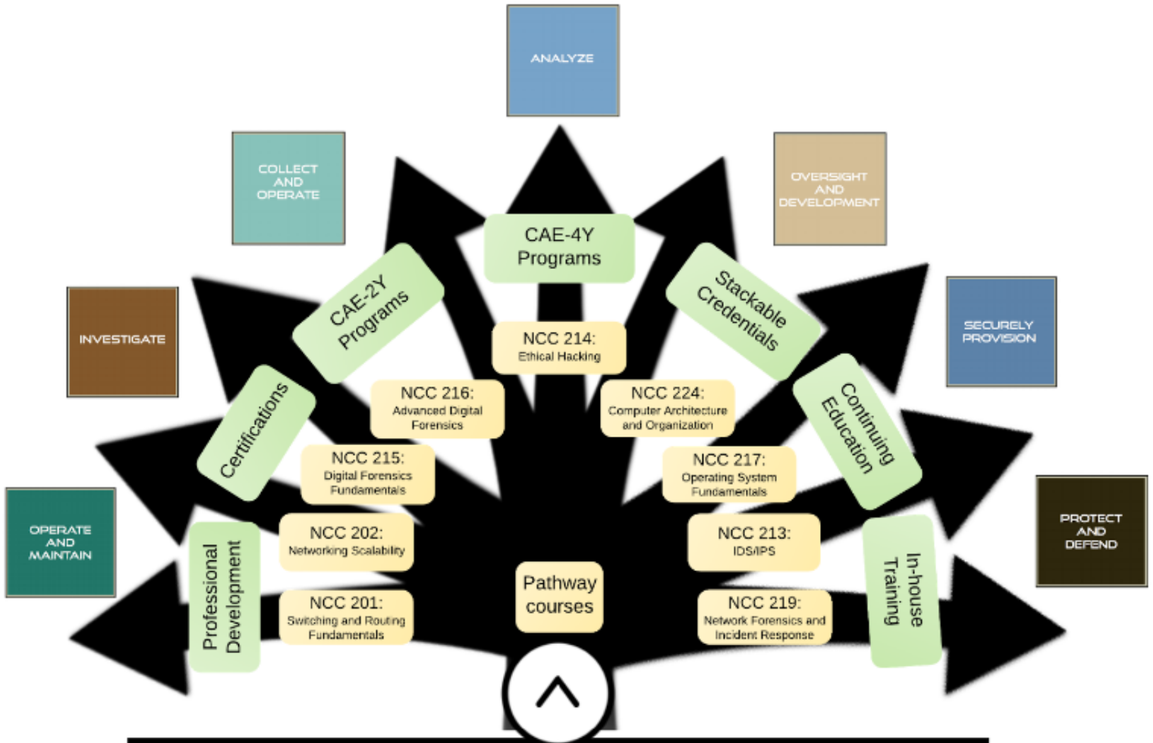
Core Curriculum Learning Paths

This Figure 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). 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.



Pathways to Learning

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). This Figure depicts an example of how the existing library of NCC 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 NCWF.



Cybersecurity Foundations Series (NSA CAE-CD Core Knowledge Units, 2Y/4Y)				
NCC 204: Linux Fundamentals	NCC 206: Windows Server Fundamentals	NCC 200: Networking Fundamentals	NCC 212: Scripting Fundamentals	NCC 210: Information Security Fundamentals

Conclusion of Phase 1 – Next Steps

The full NCC CSP Core Curriculum Mapping Report is available from: https://www.nationalcyberwatch.org/resource/mapping-national-cyberwatch-centers-curriculum-national-workforce-competency-requirements.

The results of Phase 1 led to the proposal for Phase 2, which involves developing competency-based curriculum for up to five NCC Foundation Series courses.

2017 Information Security Fundamentals Grant Proposal

The main goal of this effort is to produce an adaptive, performance-based, psychometrically valid, formative curriculum design that is aligned with the NSA Centers of Academic Excellence (CAE) Knowledge Units (KUs), NICE Cybersecurity Workforce Framework, and industry competency and capability maturity models. The proposed Core Curriculum Development Process will enable rapid deployment of adaptive curriculum that raises learner capability maturity in the foundational cybersecurity concepts, principles, and practices. The formative assessments will provide valuable pedagogical resources to cybersecurity instructors to raise learner competency levels towards mastery in each of the foundational course domains. The competency profiles produced for each learner will assist industry recruiters seeking to match talent requirements with candidate capabilities, and will facilitate articulation agreements between two-year and four-year CAE postsecondary education institutions. Finally, the adaptation of concept inventory assessment to cybersecurity education will enhance national program evaluation/accreditation and workforce planning by permitting valid aggregation and data mining of student and workforce competencies.

2017 ISF Panel – Topic Area Working Groups

NSA Grant limited the effort to one course. A new panel was convened and divided into three Topic Area Working Groups (TAWGs), based on the five Functions from the NIST Cybersecurity Framework – (1) Identify, (2) Protect & Detect, and (3) Respond & Recover. The goal was to develop competency-based course learning modules for the key (threshold) learning objectives identified through the TAWG's tasks and conduct a pilot project with several academic institutions.

2017 ISF Panel – Planned Outcomes

1. Demonstrate the rapid development and renewal of instructional materials that closely aligns with the National Institute of Standards and Technology's National Cybersecurity Workforce Framework (NCWF) by implementing effective practices in crowdsourced, competency-based instructional design, supporting scaling of the full program across both Foundations and Pathway Course designs.

2. Demonstrate the feasibility and agile development benefits of inductive, psychometric classification methods for identifying common misunderstandings and misconceptions of concepts, procedures, conditions, or situations, which must be remedied for accumulation of cybersecurity expertise to occur. These competency-based assessment models will apply Diagnostic Classification Modeling to produce detailed competency profiles and personalized (differentiated) learning paths for each learner as a complement to current grade-based or portfolio-based assessments.

2017 ISF Panel – Planned Outcomes (cont'd)

3. Demonstrate the platform independence of the differentiated instruction modules through use in both hosted and locally established infrastructure learning environments.

4. Demonstrate the feasibility of raising the cybersecurity capability maturity levels of learners, both traditional and non-traditional, through the application of formative, mastery-based learning techniques.

2017 ISF Panel – Outcomes & Deliverables

Outcome #1: Crowdsourced Instructional Designs Aligned with NCWF

Deliverables: Library of conceptual, procedural, conditional and situational instructional modules covering all NCWF Competency Areas that were designated by the National CyberWatch Center CSP as applicable for the course (draft syllabi available upon request).

Outcome #2: Inductive Concept Inventory Development

Deliverables: A minimum of three concept inventory assessment items will be identified for each instructional module discussed above. These will be validated and improved throughout the prototype development period.

2017 ISF Panel – Outcomes & Deliverables (cont'd)

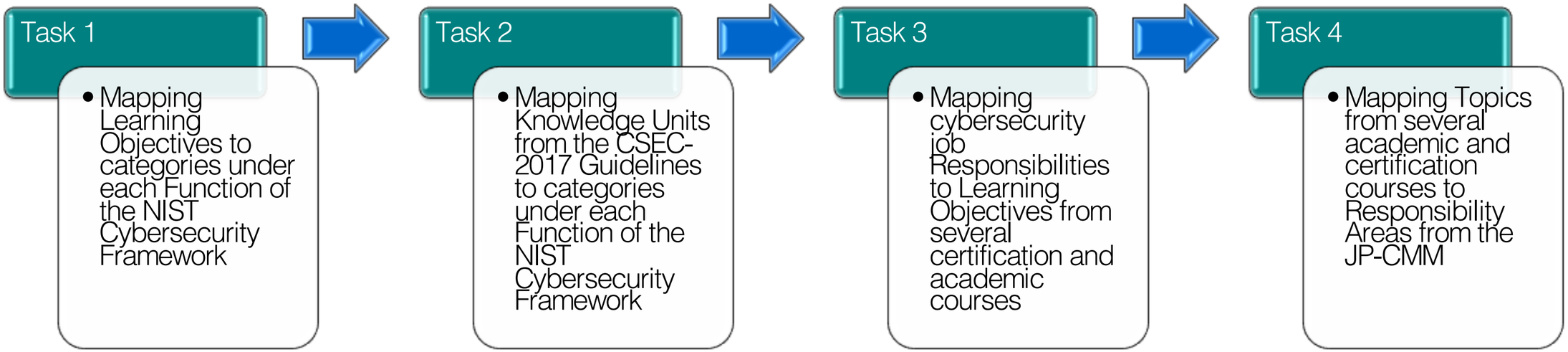
Outcome #3: Platform Independence

Deliverables: The demonstration of this platform independence will be evidenced by three use-case implementations of the Fundamentals of Information Security course: 1) selective module use as a supplement to existing course syllabi using textbook or other traditional instructional techniques; 2) implementation in a standard off-the-shelf LMS which offers differentiated or mastery learning paths; and 3) implementation in a hosted environment which provides integrated, adaptive learning.

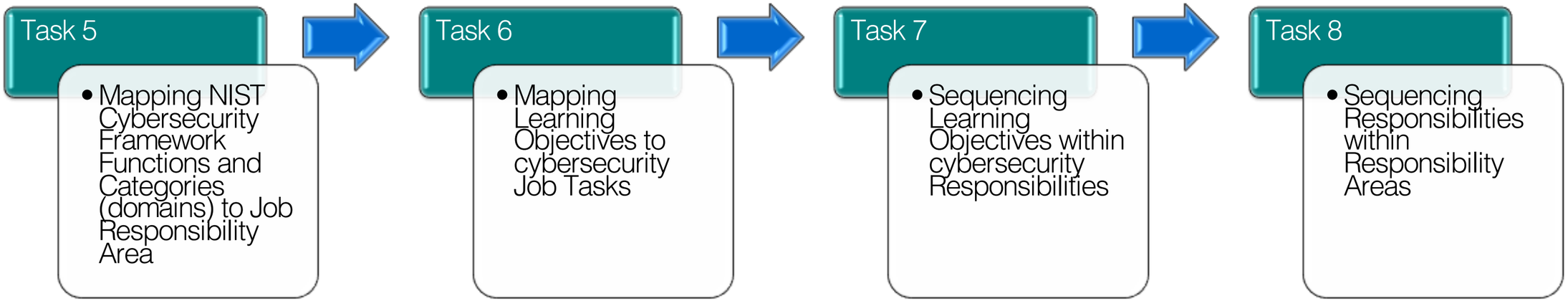
Outcome #4: Increasing Capability Maturity

Deliverables: Each participant in the pilot will receive a personalized competency profile showing their capability maturity within the NCWF model. This data will be aggregated to support workforce planning. Finally, a pre-post analysis will permit evaluation of maturity level increase.

2017 ISF Panel – Tasks



2017 ISF Panel – Tasks (cont'd)



2017 ISF Panel – Initial Results

The results from the first 8 tasks is the identification of seven key (threshold) Learning Objectives, linked with their respective functional domains (Responsibility Areas). These 7 Learning Objectives form the basis for creating learning modules for a pilot program to implement competency-based learning in a post-secondary academic setting.

Resulting Threshold Learning Objectives

Domains/Categories:

(1) Risk Assessment

(2) Risk Management Strategy

Learning Objectives: (one per SIG)

#1748 – Understand the fundamentals of network and application vulnerability scanners, common commercial and open source tools, and how to defend against them

#1351 – Understand penetration testing (PT)

Resulting Threshold Learning Objectives (cont'd)

Domains/Categories:

(3) Awareness and Training

(4) Business Environment

Learning Objectives: (one per SIG)

#7682 – Explain the importance of security related awareness and training

#1468 – Understand processes, for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices

#879 – Understand and align security function to goals, mission, and objectives of the organization

Resulting Threshold Learning Objectives (cont'd)

Domains/Categories:

(5) Information Protection Processes

(6) Response Processes

Learning Objectives: (one per SIG)

#1741 – Understand the general approaches to get rid of the attacker's artifacts on compromised machines, the general strategy to safely restore operations, and the importance of the incident report and "lessons learned" meetings

#1738 – Understand what incident handling is, why it is important, and the best practices to take in preparation for an incident

Next Steps – The Continuing Path Forward

Special Interest Groups (SIGs) are being formed for each of the threshold Learning Objectives, and there will be several topics which comprise each one. The purpose of the SIGs is to have subject matter experts (SMEs) create learning modules for each topic, which will consist of various curricular materials. After the learning modules for the first seven Learning Objectives have been completed, additional Learning Objectives, which follow a sequence of dependencies (learning pathways), will be brought forward into new SIGs to develop learning modules.

SIG Task – Develop Learning Modules

Typical content:

- Self-paced, personalized micro-learning modules (one concept)
- Formative pre-assessment to determine learner's readiness for mastering modules concepts and skills
- Competency-based (performance-based) instructional materials
  - Lectures (recorded)
  - Reading assignments
  - Skills-based, step-by-step procedures
  - Writing assignments (research and analysis)
  - Demonstrations (recorded)

SIG Task – Develop Learning Modules (cont'd)

Typical content (cont'd):

- Evidence-based, skill development labs (learning step-by-step processes)
- Ability-enhancing, incident simulations/challenges (practical application of learned concepts/skills to solve a given scenario/problem)
- Competency-based post assessments to determine learner's mastery of modules concepts and skills

NOTE: SIGs will only develop outline requirements for labs and challenges, not actual creation of them (which requires a dedicated virtual environment).

For More Information (NCC ISF-CSP Leadership Team):

Casey O'Brien – cobrien@nationalcyberwatch.org

David H. Tobey – dhtobey@vivoworks.com

Alan B. Watkins – abwatkins.consulting@gmail.com

Robin Gandhi – rgandhi@unomaha.edu

TAWG Chairs:

TAWG-1 (Identify) Terrance Campbell – terrance.Campbell@yc4w.org

TAWG-2 (Protect & Detect) Vini Nithianandam – vnithiana@ccbcmd.edu

TAWG-3 (Respond & Recover) Angelo Thalassinidis – athalassinidis@southuniversity.edu