NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION (NICE)

Cybersecurity Workforce Training and Professional Development

"Building Capacity for a Digital Nation" --
The President's Cyberspace Policy Review

Track 4 Mission

In collaboration with the private sector and state, local and tribal partners, Track 4 will establish, provide or otherwise set standards and strategies for ***national*** *cybersecurity training and professional development.*

Track 4 Leadership

Track Co-Leads

Jane Homeyer, PhD ODNI/CHCO	Peggy Maxson DHS/NCSD	John Mills DoD/CIO

FA1: General IT Use

Leads

Roy Burgess, DHS

Chris Kelsall, DoN

FA2: IT Infrastructure, Operations, Maintenance, and Information Assurance

Leads

George Bieber, DoD

Roy Burgess, DHS

FA3: Domestic Law Enforcement and Counterintelligence

Leads

Matt Parsons, DC3

Ron Sinkler, NCIX

Jason Chipman, DOJ

Jim Florio, USSS

FA4: Specialized Cybersecurity Operations

Lead

CAPT Jill Newton, NSA

Task Overview

- Task 1 – Population Review
- Task 2 – Training Catalog
- Task 3 – Workforce Baseline Study
- Task 4 – Workforce & Training Analysis (Identification of gaps)
- Task 5 – Professional Development Roadmaps
- Task 6 – Communication

Multiple federal efforts

NIST SP 800-16, Rev. 1 (NIST)

Development of a Department of Defense Cybersecurity Workforce Framework and Preliminary Training Gap Analysis, July 2010 (DOD)

Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies, July 2010 (DOD, DHS)

IT Security Workforce Matrix Project (FED CIO IT Workforce Committee)

Competency Model for Cybersecurity, 16 Feb 2011 (OPM – NICE Track 3)

Comprehensive National Cyber Initiative #8 Expand Cyber Education Activities (Leads: DHS, NSA)

ISS LOB Tier 1 Awareness Training Initiative (Lead: DHS)

ISS LOB Tier 2 Role-Based Training Initiative (Lead: DHS)

Essential Body of Knowledge (Lead: DHS)

CNSS Education Training and Awareness Working Group & Training Standards (Lead: CNSS)

Focusing all National Efforts

- NICE effort serves as the focal point for existing and future cybersecurity workforce development initiatives.
- Compilation of all previous Federal efforts; collaborating with SLT, academia and private sector.
- A single touch point for the nation that is recognized as the “go to” point for cybersecurity education and training.
- NICE, partnering with all of those who strive to improve the capabilities and effectiveness of cybersecurity professionals, can begin to build to the future.

Focusing all National Efforts

- Federal – guidelines and standards
- State, Local, Tribal – encourage participation in building and common acceptance
- Academia – collaborate and ensure best practices, encourage common adoption or crosswalk
- Industry – collaborate and ensure best practices, encourage common adoption or crosswalk

Category: Operate and Maintain

Functional Role: Systems Security Analyst

Responsible for the integration/testing, operations, and maintenance of systems security.

Typical OPM Classification: 2210, Information Technology Management
(Actual information provided by OPM)

Example Job Titles: Information assurance security; Information systems security; Information system security; IA Operational Engineer

Job tasks

1. Implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
2. Implement approaches to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.
3. Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.
4. Implement and/or integrate security measures for use in system(s) and ensure that system designs incorporate security configuration guidelines.
5. Discover organizational trends with regard to the security posture of systems.
6. **etc.**

Competency	KSAs
Information Assurance: Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.	Skill in designing countermeasures to identified security risks.
	Knowledge of existing IA security principles, policies, and procedures.
	Knowledge of IT security principles and methods, such as firewalls, DMZ, and encryption.
Risk Management: Knowledge of the principles, methods, and tools used for risk assessment and mitigation, including assessment of failures and their consequences.	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
	Knowledge of network access and authorization (e.g., public key infrastructure).
	Skill in assessing the robustness of security systems and designs.
Systems Life Cycle: Knowledge of systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems.	Knowledge of embedded systems.
	Knowledge of how system components are installed, integrated, and optimized.
	Skill in designing the integration of hardware and software solutions.
Etc.	**Etc.**

Color Key:	Track 3	Track 4	Both

Focusing all National Efforts

- NICE effort serves as the focal point for existing and future cybersecurity workforce development initiatives.
- Compilation of all previous Federal efforts; collaborating with SLT, academia and private sector.
- A single touch point for the nation that is recognized as the “go to” point for cybersecurity education and training.
- NICE, partnering with all of those who strive to improve the capabilities and effectiveness of cybersecurity professionals, can begin to build to the future.