NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Update for Software and Supply Chain Assurance Forum
July 14, 2016

Bill Newhouse, Deputy Director, National Initiative for Cybersecurity Education - NIST

NICE Workforce Framework

- The *NICE Workforce Framework* has been developed to provide a common understanding of cybersecurity work roles
  - Initially based on extensive job analyses
  - Describes cyber work roles
  - Uses consistent labels and definitions in a taxonomic structure
- This common understanding and approach is essential to educate, recruit, train, develop, and retain the workforce needed to protect the nation in an increasing cyber threat environment

NICE Framework Purpose and Structure

- Prior to the NICE Workforce Framework, cybersecurity work roles and workers have been described and defined inconsistently (and sometimes idiosyncratically) within and across organizations
- Although relevant within individual organizations these disparities preclude a comprehensive, systematic analysis and understanding
- The *Framework* is designed to transcend this variability and provide an overarching structure that will accommodate existing organizational structures while providing consistency needed for understanding and action

NICE Framework Purpose and Structure

- Categories provide overarching structure
- Within Categories, work roles further refine related work
  - Typically, work roles within a single Category are more inter-related than work roles in different Categories
  - Task and Knowledges, Skills, and Abilities (KSA) statement provide robust foundation for *Framework* and facilitate fidelity
- The new framework expands Specialty Areas into Work Roles

The Foundation for our Nation's Cyber Workforce

The National Cybersecurity Workforce Framework

- 7 Categories, 30+ Specialty Areas
- Baselines knowledge, skills, and abilities & tasks
- Support for strategic workforce development

- Version 1.0 posted in April 2013 after draft release with public comment period
- Version 2.0 posted in May 2014 after public private refinement of specific specialty areas identified during gov't-wide of version 1.0

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The new NICE Workforce Framework focuses on work roles

Work Role

- A specialized set of tasks/functions requiring specific knowledge, skills & abilities (KSAs).

Job/Position

- One or more work roles one regularly performs for pay.

Job Title

- A description of ones job/position in the organization.

Expansion into IT – Evolution from NCWF 2.0

- Supports DoDD 8140.01 Cyberspace Workforce Management (11 Aug 2015)
  - **Cyberspace IT Workforce:** Personnel, who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.
  - **Cybersecurity Workforce:** Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.
  - **Cyberspace Effects Workforce:** Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.
  - **Intelligence Workforce (Cyberspace):** Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities

Securely Provision

Category	Specialty Area	Work Role
Securely Provision	Risk Management	Authorizing Official/Designating Representative
		Security Control Assessor
	Software Development	Software Developer
		Secure Software Assessor
	Systems Architecture	Enterprise Architect
		Security Architect
	Technology R&D	Research & Development Specialist
	Systems Requirements Planning	Requirements Planner
	Test and Evaluation	Testing and Evaluation Specialist
	Systems Development	Information Systems Security Developer
		Systems Developer

Software Developer – Tasks (1 of 2)

Category	Specialty Area	Work Role	NOTES
Securely Provision	Software Development	Software Developer	
	Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.	Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.	

Tasks			NOTES
408	Task	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	
414	Task	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	
417	Task	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	
418	Task	Apply secure code documentation.	
432	Task	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	
446	Task	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	
459A	Task	Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.	
461	Task	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	
467	Task	Consult with engineering staff to evaluate interface between hardware and software.	
477	Task	Correct errors by making appropriate changes and rechecking the program to ensure desired results are produced.	
506	Task	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	
515A	Task	Develop software system testing and validation procedures, programming, and documentation.	
543	Task	Develop secure code and error handling.	
602	Task	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	
634	Task	Identify basic common coding flaws at a high level.	

Software Developer – Tasks (2 of 2)

644	Task	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	
645	Task	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	
709A	Task	Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	
756	Task	Perform integrated quality assurance testing for security functionality and resiliency attack.	
764	Task	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	
770	Task	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	
785	Task	Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.	
826	Task	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	
865	Task	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	
970A	Task	Apply cybersecurity functions (e.g., encryption, access control, identity management) to reduce exploitation opportunities.	
971	Task	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.	
972A	Task	Determine and document software patches or the extent of releases that would leave software vulnerable.	
1149A	Task	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	
1150A	Task	Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise AV solution) when appropriate.	
1151	Task	Identify and leverage the enterprise-wide version control system while designing and developing secure applications.	
2156	Task	Consult with customers about software system design and maintenance.	
2335	Task	Direct software programming and development of documentation.	
2839	Task	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	
2833	Task	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	

Software Developer – KSAs (1 of 3)

KSAs			NOTES
3	KSA	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	
20	KSA	Knowledge of complex data structures.	
23	KSA	Knowledge of computer programming principles such as object-oriented design.	
38	KSA	Knowledge of organization's enterprise information security architecture system.	
40	KSA	Knowledge of organization's evaluation and validation requirements.	
43A	KSA	Knowledge of embedded systems.	
56	KSA	Knowledge of cybersecurity principles and methods that apply to software development.	
63	KSA	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	
74	KSA	Knowledge of low-level computer languages (e.g., assembly languages).	
81	KSA	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	
90	KSA	Knowledge of operating systems.	
95A	KSA	Knowledge of penetration testing principles, tools, and techniques.	
100	KSA	Knowledge of Privacy Impact Assessments.	
102	KSA	Knowledge of programming language structures and logic.	
109	KSA	Knowledge of secure configuration management techniques.	
116	KSA	Knowledge of software debugging principles.	
117	KSA	Knowledge of software design tools, methods, and techniques.	
118	KSA	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	
119	KSA	Knowledge of software engineering.	
121	KSA	Knowledge of structured analysis principles and methods.	

Software Developer – KSAs (2 of 3)

123	KSA	Knowledge of system and application security threats and vulnerabilities.	
124	KSA	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	
149	KSA	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	
168	KSA	Skill in conducting software debugging.	
172	KSA	Skill in creating and utilizing mathematical or statistical models.	
174	KSA	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	
177	KSA	Skill in designing countermeasures to identified security risks.	
185A	KSA	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	
191	KSA	Skill in developing and applying security system access controls.	
197	KSA	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	
238A	KSA	Skill in writing code in a currently supported programming language (e.g., Java, C++).	
904	KSA	Knowledge of interpreted and compiled computer languages.	
905	KSA	Knowledge of secure coding techniques.	
968	KSA	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	
973A	KSA	Skill in using code analysis tools.	
974	KSA	Ability to tailor code analysis for application-specific concerns.	
976	KSA	Knowledge of software quality assurance process.	
978A	KSA	Knowledge of root cause analysis techniques.	
979	KSA	Knowledge of supply chain risk management standards, processes, and practices.	
980A	KSA	Skill in performing root cause analysis.	
1020A	KSA	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	

Software Developer – KSAs (3 of 3)

1034A	KSA	Knowledge of Personally Identifiable Information (PII) data security standards.	
1034B	KSA	Knowledge of Payment Card Industry (PCI) data security standards.	
1034C	KSA	Knowledge of Personal Health Information (PHI) data security standards.	
1037A	KSA	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	
1038	KSA	wledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	
1071A	KSA	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	
1072	KSA	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	
1131	KSA	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zackman, Federal Enterprise Architecture [FEA]).	
1135	KSA	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	
1140A	KSA	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	
22	KSA	* Knowledge of computer networking concepts and protocols, and network security methodologies.	
108	KSA	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	
1157	KSA	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	
1158	KSA	* Knowledge of cybersecurity principles.	
1159	KSA	* Knowledge of cyber threats and vulnerabilities.	
6900	KSA	* Knowledge of specific operational impacts of cybersecurity lapses.	
3370	KSA	Knowledge of local area network (LAN) and wide area network (WAN) principles.	
3080	KSA	Ability to use and understand complex mathematical concepts (e.g., discrete math).	

Operate and Maintain

Category	Specialty Area	Work Role
Operate and Maintain	Data Administration	Database Administrator
		Data Analyst
	Knowledge Management	Knowledge Manager
	Customer Service and Technical Support	Technical Support Specialist
	Network Services	Network Operations Specialist
	Systems Administration	System Administrator
	Systems Analysis	Systems Security Analyst

Oversee and Govern

Category	Specialty Area	Work Role
Oversee and Govern	Legal Advice and Advocacy	Legal Advisor
	Training, Education, and Awareness	Instructional Curriculum Developer
		Cyber Instructor
	Cybersecurity Management	Information Systems Security Manager
		COMSEC Manager
	Strategic Planning and Policy	Cyber Workforce Developer and Manager
		Cyber Policy and Strategy Planner
	Executive Cyber Leadership	Executive Cyber Leadership
	Acquisition and Program/Project Management	Program Manager
		IT Project Manager
		Product Support Manager
		IT Investment/Portfolio Manager
		IT Program Auditor

Protect and Defend

Category	Specialty Area	Work Role
Protect and Defend	Cyber Defense Analysis	Cyber Defense Analyst
	Cyber Defense Infrastructure Support	Cyber Defense Infrastructure Support Specialist
	Incident Response	Cyber Defense Incident Responder
	Vulnerability Assessment and Management	Vulnerability Analyst

Analyze

Category	Specialty Area	Work Role
Analyze	Threat Analysis	Warning Analyst
	Exploitation Analysis	Exploitation Analyst
	All-Source Analysis	All-Source Analyst
		Mission Assessment Specialist
	Targets	*Target Developer*
		Target Digital Network Analyst
		Target Analyst Reporter
	Language Analysis	*Multi-Disciplined Language Analyst*

Operate and Collect

Category	Specialty Area	Work Role
Operate and Collect	Collection Operations	*All Source-Collection Manager*
		All Source-Collection Requirements Manager
	Cyber Operational Planning	*Cyber Intel Planner*
		Cyber Ops Planner
		Interagency/International Integration Planner
	Cyber Operations	*Access Network Operator*
		Interactive Operator

Investigate

Category	Specialty Area	Work Role
Investigate	Cyber Investigation	Cyber Crime Investigator
	Digital Forensics	Forensics Analyst
		Cyber Defense Forensics Analyst

NICE Workforce Framework

- NIST SP 800-181 Drafting team includes:
  - NICE Program Office, Applied Cybersecurity Division, Information Technology Laboratory, NIST
  - Cyber Workforce Division in the Office of the Deputy DoD Chief Information Officer - Cybersecurity
  - Cybersecurity Education and Awareness Branch, Stakeholder Engagement and Cyber Infrastructure Resilience Division, Department of Homeland Security
  - NSA/DHS National CAE-CD Program National IA Education & Training Program (NIETP)
  - OPM

Contact info for the NICE Program Office

- Director, Rodney Petersen, rodney@nist.gov
- Deputy Director, Bill Newhouse, newhouse@nist.gov
- Program Manager, Danielle Santos, Danielle.Santos@nist.gov
- Education K-12, Davina Pruitt-Mentle, davina.Pruitt-mentle@nist.gov
- Industry, Celia Paulsen, celia.paulsen@nist.gov

Join Us

7th Annual

NICE 2016 Conference and Expo

November 1-2, 2016

Kansas City, Missouri

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Strategic Plan Draft – Vision & Mission

- Vision: A digital economy that is powered by secure technologies, enabled by a skilled cybersecurity workforce, and used by risk-aware citizens and organizations.

- Mission: To foster, energize, and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development.

NICE Strategic Plan Draft - Values (November 3, 2015)

- **Seek Evidence** –inform actions or decisions with data whenever possible or pursue objective and reliable sources of information
- **Pursue Action** – strive for concrete steps towards deliverable outcomes to achieve mission and goals
- **Challenge Assumptions** –examine rationale for past and present approaches and apply critical analysis to solutions
- **Embrace Change** – seek creative and innovative solutions that might disrupt or defy the status quo
- **Stimulate Innovation** – inspire and test new approaches to education, training, and skills development
- **Foster Communication** – engage in information sharing and encourage openness to build trust and enhance effectiveness
- **Facilitate Collaboration** – connect or combine similar efforts to avoid duplication and maximize use of limited resources
- **Share Resources** – communicate, leverage, and support community-developed approaches and solutions
- **Model Inclusion** – encourage participation from diverse stakeholders and represent diverse backgrounds and viewpoints
- **Measure Results** –quantitatively and qualitatively assess the effectiveness of deliverables and program outcomes based on explicit goals

NICE Strategic Goal #1:
Accelerate Learning and Skills Development

Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers

Objectives:

1.1 Stimulate the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers

1.2 Advance programs that reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles

1.3 Engage displaced workers or underemployed individuals who are available and motivated to assume cybersecurity work roles

1.4 Experiment with the use of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills

1.5 Explore methods to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce needs

NICE Strategic Goal #2:
Nurture a Diverse Learning Community

Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

Objectives:

2.1 Improve education programs, co-curricular experiences, and training and certifications

2.2 Encourage tools and techniques that effectively measure and validate individual aptitude, knowledge, skills, and abilities

2.3 Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school

2.4 Grow creative and effective efforts to increase the number of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce

2.5 Facilitate the development and dissemination of academic pathways for cybersecurity careers

NICE Strategic Goal #3: Guide Career Development and Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the National Cybersecurity Workforce Framework and encourage adoption

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

NICE Engagement

- Interagency Coordinating Committee
  - NSF, NSA, DHS, OPM, ED, DoC, DoL, DoD, and more . . .
- NICE Working Group
  - Collegiate Subgroup
  - K-12 Subgroup
  - Competitions Subgroup
  - Training and Certifications Subgroup
  - Career Development Subgroup
    - Workforce Framework

Key Programs and Activities

- Advanced Technological Education (ATE) Centers (NSF)
- Centers of Academic Excellence (DHS/NSA)
  - 2Y Cyber Defense
  - 4Y Cyber Defense
  - Cyber Research
  - Cyber Operations
- CyberCorps® : Scholarship for Service
- NICE 2016: November 1-2 in Kansas City, Missouri
- National Cybersecurity Workforce Framework

Outreach and Engagement: Government

- Government
  - Federal Departments and Agencies
  - State Governments
- Academia
  - Post-Secondary, 2 Year, 4 Year, Graduate, Research
  - Elementary and Secondary
- Industry
  - Employers of cybersecurity workforce
  - Specialized: IT sector, training and certification providers, etc.