NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The NICE Framework
The National Initiative for Cybersecurity Education (NICE)
Cybersecurity Apprenticeship Employer Summit - Charleston
November 14, 2018

Bill Newhouse, Deputy Director of NICE

Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)

NICE Strategic Goals

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*

Nurture A Diverse Learning Community

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

Guide Career Development & Workforce Planning

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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

https://nist.gov/nice

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 NICE Cybersecurity Workforce Framework and encourage adoption

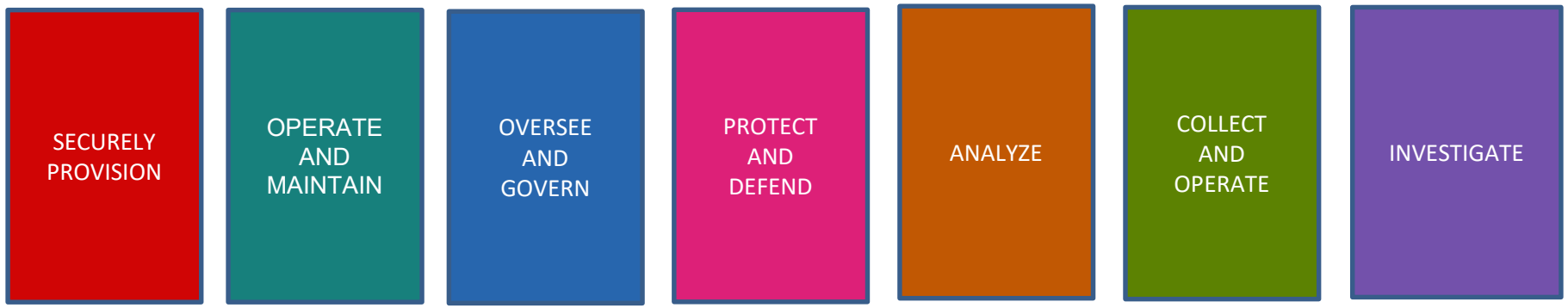
3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

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

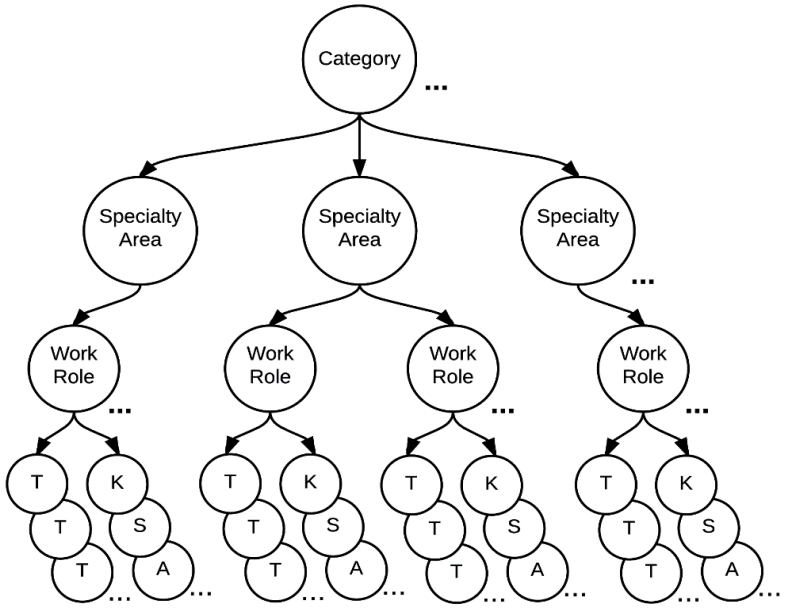
3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

NICE Framework - https://go.usa.gov/xnXsh

Categories of Cybersecurity Work



- Specialty Areas (33) – Distinct areas of cybersecurity work;
  - Work Roles (52) – The most detailed groupings of IT, cybersecurity or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks.
    - Tasks – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and,
    - Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.
- Audience:
  - Employers
  - Current and Future Cybersecurity Workers
  - Training and Certification Providers
  - Education Providers
  - Technology Providers



Building Blocks for a Capable and Ready Cybersecurity Workforce

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

NICE Cybersecurity Workforce Framework

The NICE Framework, NIST Special Publication 800-181, is a national focused resource that categorizes and describes cybersecurity work. The NICE Framework, establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.

The NICE Framework is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions.
- Specialty Areas (33) – Distinct areas of cybersecurity work.
- Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks

NICE Framework Supporting Materials

- NIST Special Publication 800-181, The NICE Cybersecurity Workforce Framework (August 2017)
- Reference Spreadsheet for the NICE Framework, NIST SP 800-181 (January 18, 2018)
- NICE Framework Revision Process and Documented Revisions

Search the NICE Framework

- Using Keywords via DHS's Cybersecurity Careers and Training Portal
- CyberWatch West database

Co-Author Resources

Securely Provision (7 Specialty Areas, 11 Work Roles)

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	Systems Requirements Planner
	Test and Evaluation	Testing and Evaluation Specialist
	Systems Development	Information Systems Security Developer
		Systems Developer

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Keyword Search

Search Descriptions

A0047: Ability to develop secure software according to secure so... Apply Reset

Abilities ID: A0047

Description: Ability to develop secure software according to secure software deployment methodologies, tools, and practices.

Work Roles:

Work Role ID: SP-DEV-001
Work Roles: Software Developer
Work Role Description: Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.
Category: Securely Provision
Specialty Area(s): Software Development

Work Role ID: SP-DEV-001

Software Developer

Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Category: Securely Provision **Specialty Area:** Software Development

Abilities

A0007: Ability to tailor code analysis for application-specific concerns.

A0021: Ability to use and understand complex mathematical concepts (e.g., discrete math).

A0047: Ability to develop secure software according to secure software deployment methodologies, tools, and practices.

A0123 : Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

A0170 : Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations.

Knowledge

K0001: Knowledge of computer networking concepts and protocols, and network security methodologies.

K0002: Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).

K0003: Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.

K0004: Knowledge of cybersecurity and privacy principles.

K0005: Knowledge of cyber threats and vulnerabilities.

K0006: Knowledge of specific operational impacts of cybersecurity lapses.

K0014: Knowledge of complex data structures.

K0016: Knowledge of computer programming principles

K0027: Knowledge of organization's enterprise information security architecture

Tasks

T0009: Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.

T0011: Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.

T0013: Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.

T0014: Apply secure code documentation.

T0022: 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.

T0026: Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.

T0034: Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.

T0040: Consult with engineering staff to evaluate interface between hardware and software.

T0046: Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.

T0057: Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.

T0077: Develop secure code and error handling.

T0100: Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.

T0111: Identify basic common coding flaws at a high level.

T0117: Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.

T0118: 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.

T0171: Perform integrated quality assurance testing for security functionality and resiliency attack.

T0176: Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.

TOP

REDUCING SOFTWARE VULNERABILITY

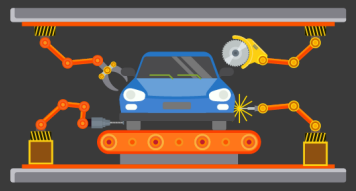
NIST National Institute of Standards and Technology U.S. Department of Commerce

New NIST interagency report (NISTIR) 8151 has five main sets of approaches for reducing vulnerabilities in software. In simple terms, according to NIST's Paul E. Black, these approaches are:

FORMAL METHODS

Math-based verification tools coders can easily apply.

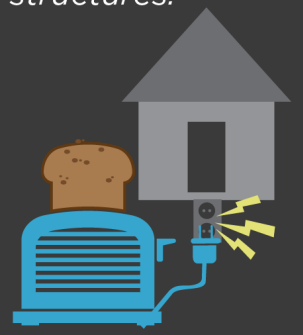
"I drive a car. But even though I know nothing about hi-temperature steel or tire rubber, it just works."



SYSTEM LEVEL SECURITY

Modularizing a computer's programs so if one piece breaks the whole thing doesn't collapse.

"If my toaster breaks it shouldn't fry my house's circuit. But computers don't always have these 'circuit breaker' type structures."



ADDITIVE SOFTWARE ANALYSIS

Connecting analysis tools that currently operate in isolation.

"You get a better suit if the guy who measures your chest and the guy measuring your inseam communicate with each other."

DOMAIN SPECIFIC FRAMEWORKS

Use a more appropriate programming language for the task.

"Why not use a language that has words and concepts and data structures that are specific to that app? In fact they exist and are mature."

MOVING TARGET DEFENSE AND AUTOMATIC SOFTWARE DIVERSITY

"If someone's attacking you, instead of building walls while they find out where you are and drop bombs, it would be nice to be able to pick up and move rather than wait for the airstrike."

Design by Natasha Hanacek/NIST

Useful Links (for use when you get these slides as an event follow-up

- NICE Framework - google “NIST NICE Framework”

Software Quality Group in the Software and Systems Division in Information Technology Laboratory at NIST – google NIST SSD

- National Software Reference Library (NSRL)
- Computer Forensics Tool Verification (CFTT)
- Software Performance
- Software Assurance Metrics And Tool Evaluation (SAMATE)
- Software Assurance Reference Dataset (SARD)
- Computer Forensic Reference Data Sets (CFReDS)