NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Keynote Project: National Cybersecurity Workforce Framework

Roy Burgess
NICE Cybersecurity Professional Development
National Cybersecurity Education & Awareness (CE&A) Branch

Our Framework is Dynamic

NICE developed the National Cybersecurity Workforce Framework (the Framework) to categorize cybersecurity work and to identify the Specialty Areas of cybersecurity professionals. The Framework is:

A Dictionary	A Tool	A Collaborative Effort
▪ Defines 31 common types of cybersecurity work, called Specialty Areas (SAs). ▪ Places each SA into 1 of 7 high-level categories. ▪ Identifies SA-related common tasks and knowledge, skills, and abilities (KSAs).	▪ Enables organizations to develop their cybersecurity workforce. ▪ Helps the Federal Government, private, public, and academic sectors better describe cybersecurity work and their workforces.	▪ Addresses the White House's need to identify, quantify, and develop an effective cyber workforce. ▪ Incorporates inputs from over 1,000 subject matter experts (SMEs) from organizations across government, academia, and the private sector.

The Framework assists strategic human capital efforts:

- Workforce Planning
- Recruitment and Selection
- Training and Development
- Succession Planning

Where Can You Find the Framework?

The National Initiative for Cybersecurity Careers and Studies (NICCS™) website is the Nation's online resource for cybersecurity awareness, education, careers, training, and professional development. The NICCS website:

- Serves as an implementation tool for NICE and the Framework.
- Builds an online portal for cybersecurity professionals and interested parties to gain knowledge related to their field.
- Raises cybersecurity awareness and will affect a change in the American public to adopt a culture of cyberspace security.
- Provides up-to-date material related to cybersecurity awareness, education, careers, and training programs.

www.niccs.us-cert.gov

So … Find the Framework at:

www.niccs.us-cert.gov/training/national-cybersecurity-workforce-framework

What We Do in Cybersecurity

Organizations can use the Framework Specialty Areas to identify, build, and customize cybersecurity roles based on mission requirements.

Investigate	Collect and Operate	Analyze	Protect and Defend	Oversight and Development	Operate and Maintain	Securely Provision
						Systems Requirement Planning
					System Administration	Systems Development
				Legal Advice and Advocacy	Network Services	Software Assurance and Security Engineering
		Cyber Threat Analysis	Computer Network Defense (CND)	Education and Training	Customer Service and Technical Support	Technology Research and Development
	Collection Operations	All Source Intelligence	Vulnerability Assessment and Management	Strategic Planning and Policy	Systems Security Analysis	Test and Evaluation
Digital Forensics	Cyber Operations Planning	Targets	Incident Response	Information Systems Security Operations	Data Administration	Systems Security Architecture
Investigation	Cyber Operations	Exploitation Analysis	CND Incident Response	Security Program Management (CISO)	Knowledge Management	Information Assurance (IA) Compliance

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The Path to Implementation

To assist organizations with interpreting the Framework, NICE developed an interactive Implementation How-To Guide with instructions on how organizations can adopt the Framework to maintain consistency with this national standard.

The How-To Guide provides information on:

- Framework characteristics and the benefits of its use, and
- The importance of adopting the Framework.
- Human capital activities that are influenced by the Framework.
- Specific steps to apply the Framework to human capital activities.
- Cybersecurity roles, built by the Federal Chief Information Officer's Council. These roles are based on the Framework.
- Examples of how to define the workforce by using these Specialty Areas.
- A sample process to customize work roles based on the unique needs of an organization.

The benefits of the How-To Guide include:

- Helping streamline human capital efforts and fulfill the requirements of federal mandates.
- Detailing the Human Capital Lifecycle and how the framework will impact its development.
- Describing the OPM Data Element and how it will assist the organization and analysis of the cybersecurity workforce.
- Interactive functionality which simplifies navigating the guide.

The interactive Implementation How-To Guide can be found on NICCS:
http://niccs.us-cert.gov/training/framework-how-guide

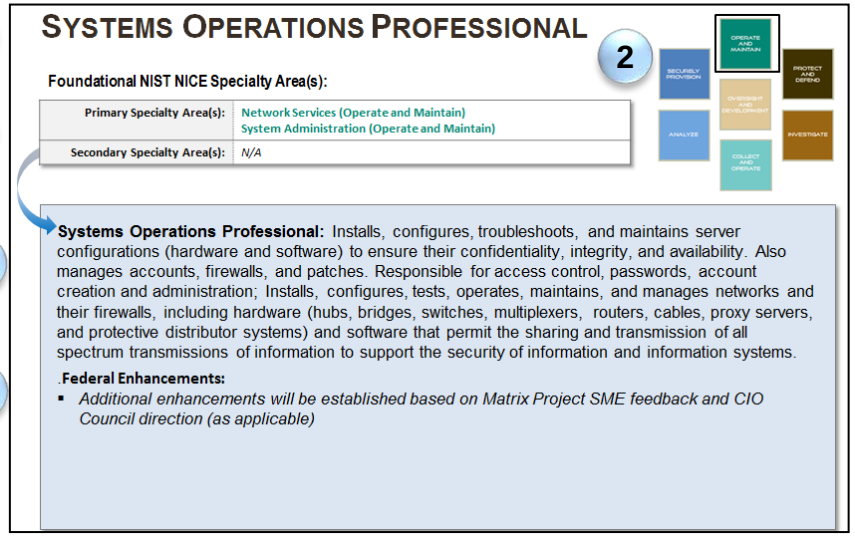
When Building Cybersecurity Roles …

If your organization has a limited number, or type, of cybersecurity positions, you may prefer to use the streamlined roles. The Federal Chief Information Officers Council (CIOC) developed 13 Framework-based roles to promote consistency and standardization of the cybersecurity workforce.

Each role consists of sample job titles and definition, the related Framework category, the Framework Specialty Areas, and any enhancements that pertain specifically to the Federal workforce.

1. Role Name
2. Framework Category
3. Framework Specialty Area
4. Sample Job Tasks
5. Federal Enhancements, if any

Streamlined Cybersecurity Role Example



The streamlined cyber roles developed by Fed CIOC:

- Systems Operations Professional
- Data Administrator
- Computer Network Defense (CND) Specialist
- Digital Forensics and Incident Response Analyst
- Information Security Auditor
- Information Systems Security Officer
- Information Systems Security Manager
- Information Security Architect
- Risk and Vulnerability Analyst
- Software Developer
- Information Systems Security Engineer
- Strategic Planning and Policy Development Professional
- Chief Information Security Officer (CISO)

What We're Working on Right Now

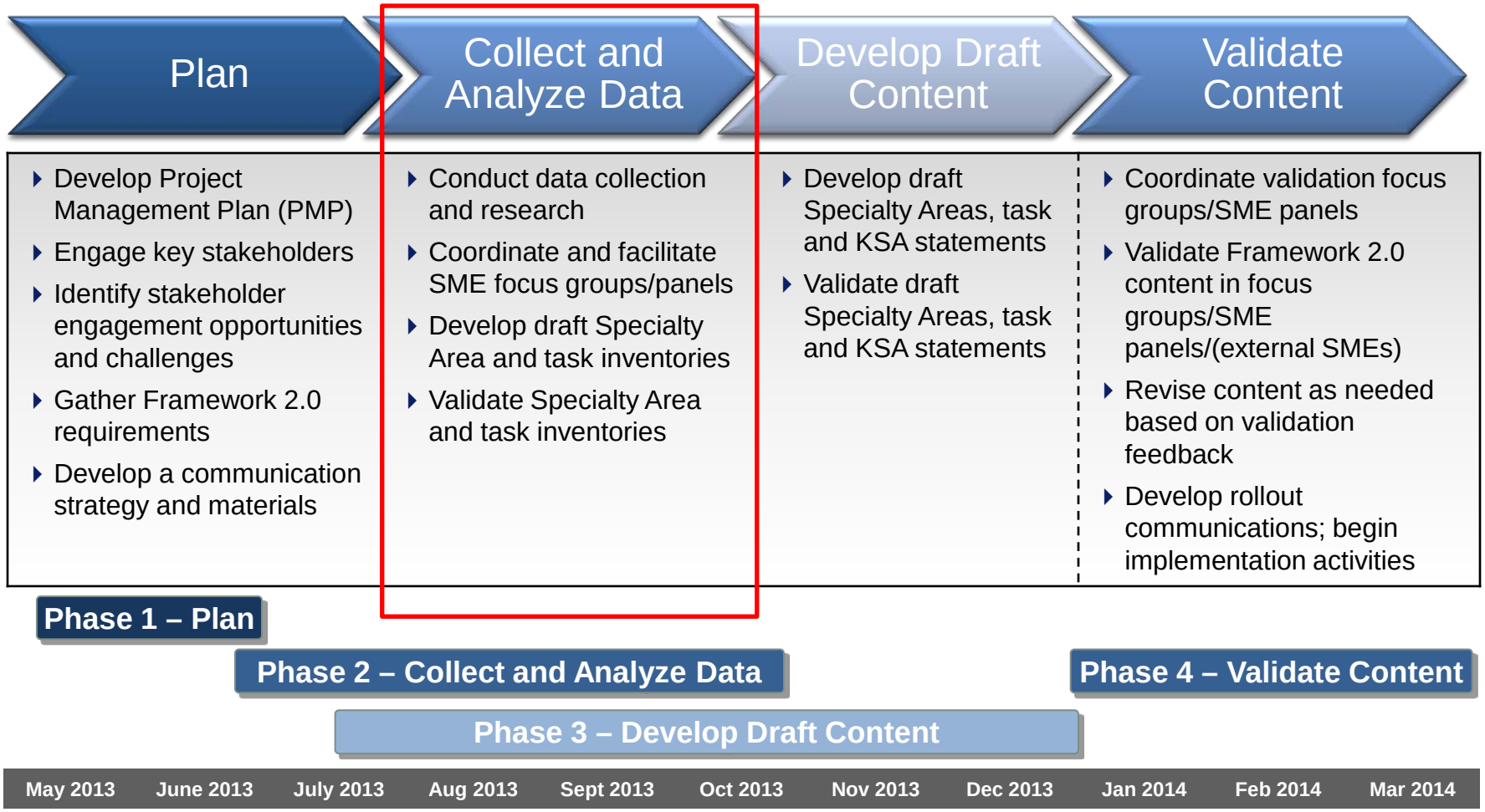
- NICE is updating the Framework to address feedback received from cross-sector stakeholders after the release of Framework 1.0 in 2011.
- Focus groups comprise 5 private sector, 5 academic, and 5 government (Fed, SLTT) subject matter experts.
- NICE has held 5 focus groups to date, with the following focus groups on the schedule:

Focus Group	Date
Investigate	Sep 24th
Oversight & Development #2	Sep 25th
Operate & Maintain #1	Oct 8th
Operate & Maintain #2	Oct 9th

- If your agency has available cybersecurity subject matter experts who can participate in Framework 2.0 focus groups, please contact Roy Burgess (roy.burgess@dhs.hq.gov).

Where We're Going

The Framework's scheduled update is underway!



What are the OPM Data Elements?

Data elements are two-digit cybersecurity codes that can be assigned to positions within OPM's Enterprise Human Resources System (EHRI) data warehouse.

Why were the data elements developed?

- To identify and quantify federal employees performing cybersecurity work.

How were the data elements derived?

- From the Framework's Categories and Specialty Areas.
- Data elements should be assigned based upon the duties in which the incumbent is primarily engaged.

What will the data elements do?

- Identify Federal Government positions for which the primary function is cybersecurity.
- Allow HR Professionals to better understand and plan for their workforces.

Track 3 NICE Workshop Activities

Track 3 will hold sessions to highlight cybersecurity workforce training & professional development efforts:

Day, Time	Title	Speakers
D1, 1:00 - 1:55pm	Cyber Intelligence Workforce	Troy Townsend, Melissa Ludwick
D1, 2:00 - 2:55pm	Cybersecurity Education for the Next Generation - Emerging Best Practices	Marisa Viveros (IBM)
D1, 3:00 - 3:55pm	Training and Professional Development for Law Enforcement and Counterintelligence	Joshua Black (DC3)
D1, 4:00 - 4:55pm	Digital Tutoring and Accelerating Expertise in Information Technology: Crossing the 2-Sigma Threshold and Beyond	Dr. Dexter Fletcher (IDA)
D2, 11:55 - 12:45pm	The Cybersecurity Online Learning Program at Department of State… Continuous Training for All	Michael Petock (AGS), Michael Riley (EC)
D2, 1:55 - 2:45pm	Implementation of the NICE Framework (panel)	Renee Forney (DHS), Chris Kelsall (DoD CIO), Stephanie Keith (DoD), Dagne Fulcher (FedCIOC)
D2, 2:50 - 3:45pm	How to Plan for Your Cybersecurity Workforce	Montana Williams (DHS)
D2, 3:50 - 4:45pm	National Security Professional Development Initiative	Gerald Talbot (OPM)
D3, 10:50 - 11:45am	Identification, Tracking and Development of the Cybersecurity Workforce (panel)	Roy Burgess (DHS), George Bieber (DoD CIO), Chris Kelsall (DoN CIO), Kevin Duffer (Skillsoft)
D3, 1:00 - 2:00pm	Hiring and Managing a Cyber Security Workforce	Scott Cameron (R3GS)
D3, 2:05 - 3:00pm	How the Department of Veteran Affairs is Implementing the NICE Cybersecurity Framework	Terri Cinnamon (VA)
D3, 3:05 - 4:00pm	Professionalizing the Nation's Cybersecurity Workforce (panel)	Montana Williams (DHS), Dr. Diana Burley (GWU), Dr. Ron Sanders (BAH), Mischel Kwon (MKA)

Implementation of the Framework and the OPM Data Element are the focus of Track 3 sessions at 1:55 today and 10:50 tomorrow!

*Note: **All** Track 3 Sessions are held in **Lecture Room A**.*

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Stay Tuned and Stay in Touch!

- We look forward to your continued support as the Framework is updated with its national focus and the OPM Data Element efforts expand across the Federal Government!
- NICE will continue to share materials with cybersecurity professionals across the nation in the public, private, and academic sectors.
- Please pass along any questions about NICE, the Framework, and other initiatives please contact:

Roy Burgess

NICE Cybersecurity Professional Development

National Cybersecurity Education & Awareness Branch

Roy.Burgess@hq.dhs.gov