NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Cybersecurity Workforce Inventory Program

U.S. Department of Homeland Security
Michael Koehler, Ph.D.

NICE Cybersecurity Workforce Inventory Program (CWIP)

Understanding the Nation's Cybersecurity Workforce

- Lead – U.S. Department of Homeland Security
- Initiated to support the activities of:
  - NICE Component 3 - Cybersecurity Workforce Structure
  - NICE Component 4 - Cybersecurity Workforce Training and Professional Development

Purpose – Facilitate an improved understanding of the composition and capability of the Nation's cybersecurity workforce

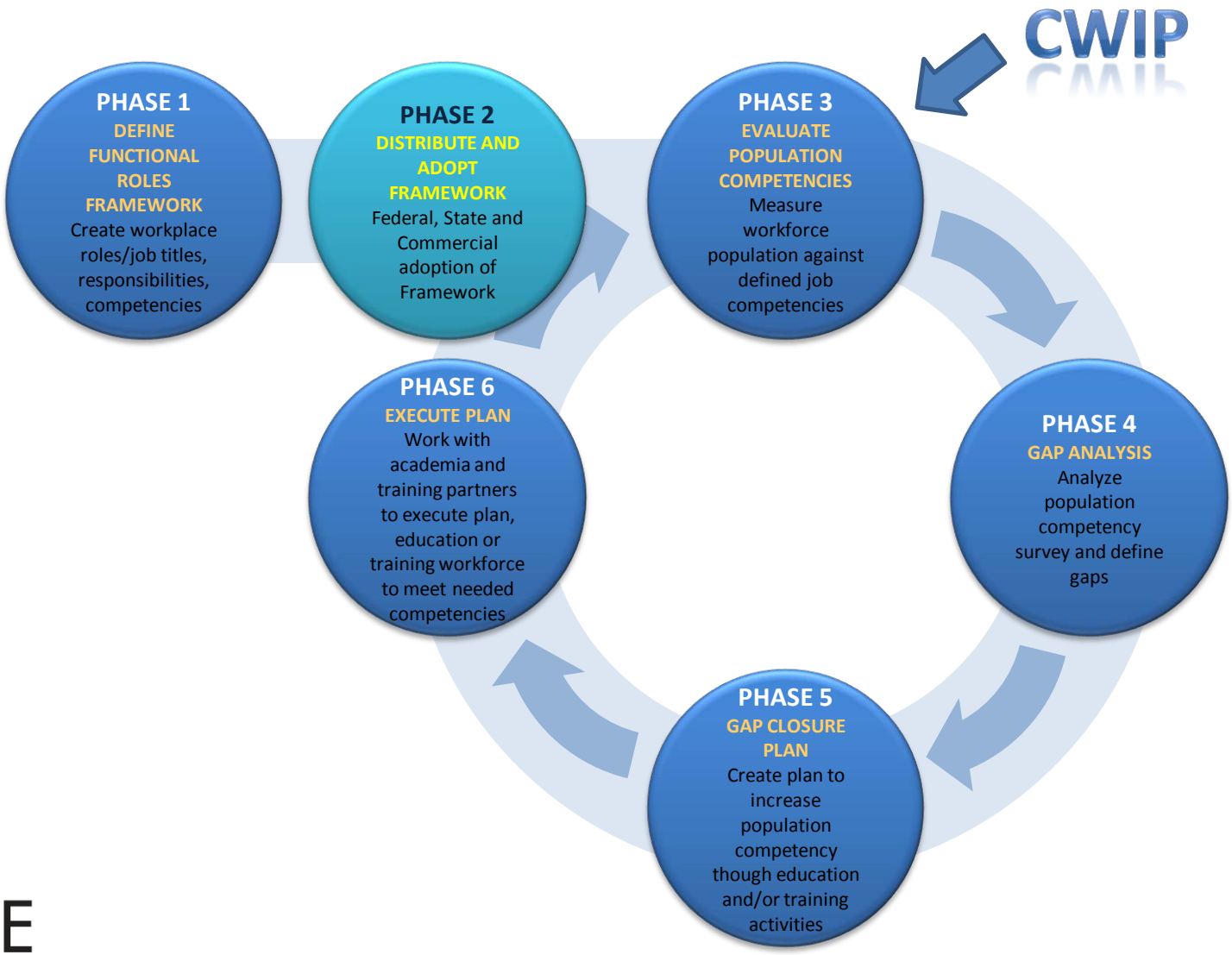
Background

National Initiative for Cybersecurity Education (NICE)

Works to enhance the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources

- **Goal 1**: Raise awareness about the risks of online activities.
- **Goal 2**: Broaden the pool of skilled workers capable of supporting a cyber-secure nation.
- **Goal 3**: Develop and maintain an unrivaled, globally competitive cybersecurity workforce.

NICE National Workforce Health Measurement Process



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Foundation

The NICE Cybersecurity Workforce Framework

A validated taxonomy of the functional roles associated with cybersecurity work

- 7 Categories
- 31 Specialty Areas
- Numerous Associated Tasks, Knowledge, Skills, and Abilities

CWIP Mission

Support the strengthening of the cybersecurity posture of the United States by collecting data that captures the current state of the cybersecurity capabilities of the Nation's IT workforce.

CWIP Vision

Provide an understanding of the capabilities of the Nation's cybersecurity professionals to inform the development of a workforce capable of defending the infrastructure and interests of the United States.

CWIP Program Structure

- Program divided into two data collection projects
  - Federal IT Workforce
  - Non-Federal IT Workforce
- Reasoning
  - Differing requirements for collecting data from federal vs. non-federal workforces.
- Will also develop an online tool individuals can use to assess their cybersecurity competencies against the Framework.

The Federal IT Workforce

Federal IT Workforce Data Collection

Objective

Understand the composition and capabilities of the federal IT workforce executing cybersecurity responsibilities.

- Will be achieved through a partnership with the Federal CIO Council (CIOC) to implement the IT Workforce Assessment for Cybersecurity (ITWAC).
- The NICE/CIOC ITWAC will help agencies examine their federal cybersecurity workforce and address its management to meet the cybersecurity challenges of the present and the future.
- The NICE will use the data collected to inform its efforts to support the education, development, and maintenance of the Nation's cybersecurity workforce.

NICE/CIOC ITWAC: General Information

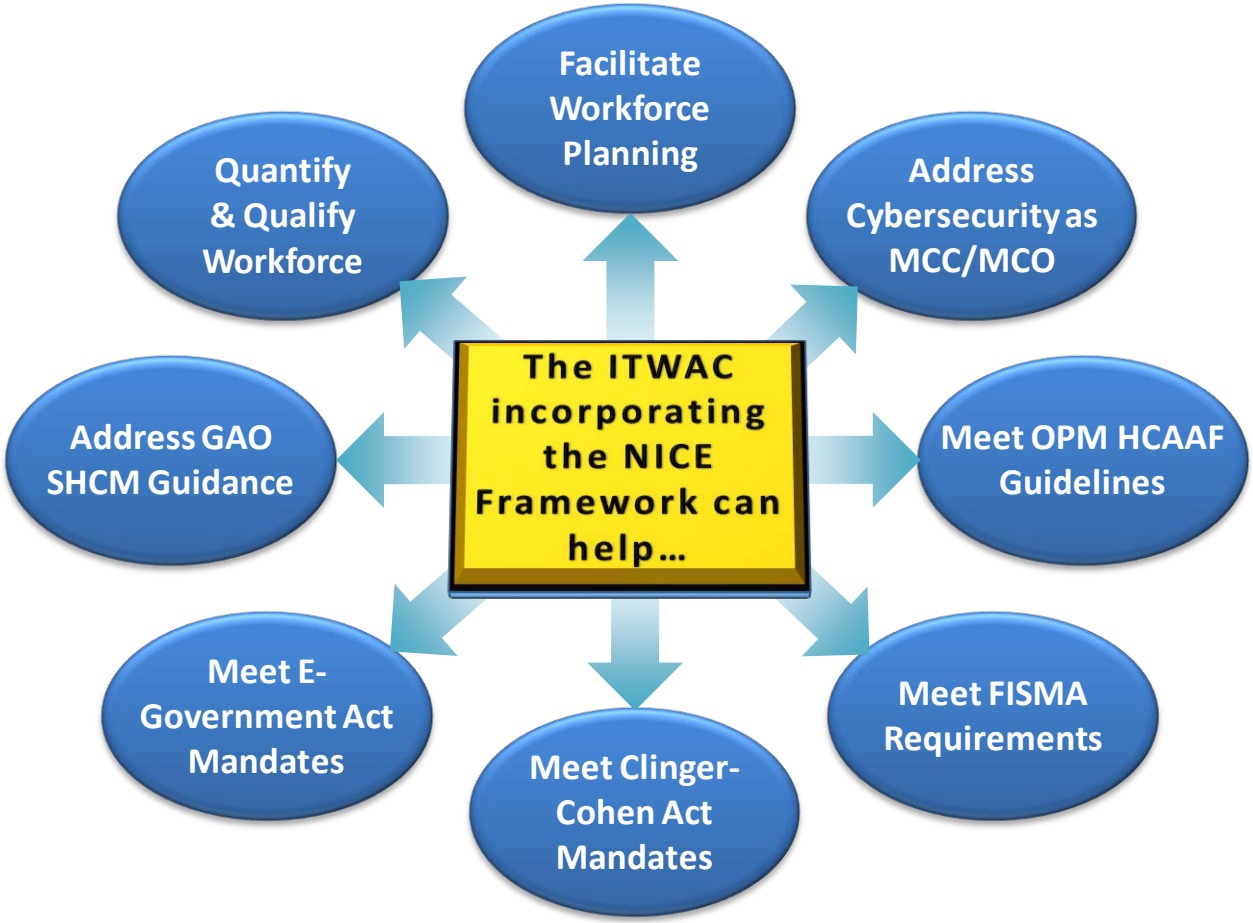
- **What:** An anonymous online survey collecting federal IT workforce characteristics and cybersecurity capabilities. Will supplement, but not replace, the CIOC IT Workforce Capability Assessment (ITWCA).
- **Who:** Targeted participants - federal employees with IT responsibilities, including investigation and intelligence, regardless of occupational series.
- **When:** Deployed in October 2012.

NICE/CIOC ITWAC: Planned Data Categories

- Cybersecurity Competencies
- Organization Identifiers
- Demographics
- Professional Characteristics
- Work Experience
- Education/Training/Certifications

NICE/CIOC ITWAC: What It Will Accomplish

- Will provide a foundation upon which human capital organizations can build cybersecurity workforce management efforts.
- Will report on the current state of cybersecurity workforce capability across the Federal Government.
- Will provide data and information to agencies that can assist in workforce planning and reporting activities.



NICE/CIOC ITWAC: Challenges

- Maximizing participation across the federal IT workforce
  - Participants should not be limited to the 2210 job series
  - Cybersecurity responsibilities as defined by the NICE Framework may fall under other job series
  - All employees with responsibilities related to the implementation of information technology solutions should participate in the ITWAC

The Non-Federal IT Workforce

Non-Federal IT Workforce Data Collection

Objective

Understand the composition and capabilities of the non-federal IT workforce executing cybersecurity responsibilities.

- To supply an understanding of the composition and capabilities of the non-federal cybersecurity workforce to inform present and future cybersecurity education, workforce structure, and training and professional development support efforts.

Non-Federal IT Workforce Data Collection

General Information

- **What:** An as yet undetermined method and vehicle to collect data capturing the composition and capabilities of the non-federal cybersecurity workforce.
- **Who:** IT workforce not employed by the Federal Government
  - Includes State, Local, Tribal, and Territorial governments, academia, and industry
- **When:** Data collection planned for Q3 FY 2013

Non-Federal IT Workforce Data Collection

Challenge

- How to collect the necessary data incorporating the NICE Framework?
  - How to identify and engage cybersecurity workforce?
  - Method to collect data?

Non-Federal IT Workforce Data Collection

Currently Exploring Potential Solutions

- Enlisting assistance from data collection experts at the Department of Labor and the Bureau of the Census to determine if such a collection can be executed via a single vehicle.
- Also welcoming any ideas of other collection methods.

Individual Assessment

Individual Assessment

Objective

Provide an online tool that allows individuals to assess their cybersecurity capabilities and provides feedback to inform individual career and development planning

- Will provide the user with a greater understanding of the field of cybersecurity, associated careers, and training and education opportunities to enhance their capabilities
- Based on the NICE Framework

Individual Assessment

General Information

- **What:** An online, interactive tool hosted on the National Institute for Cybersecurity Studies (NICS) portal.
- **Who:** All individuals interested in further development of their cybersecurity capabilities and careers
- **When:** Deployment planned for Q1 FY 2014

CWIP Summary

- Two data collection projects to capture IT workforce cybersecurity capabilities
  - Federal IT Workforce
  - Non-Federal IT Workforce

- A online tool allowing individuals to assess their cybersecurity capabilities and learn more about careers and development

Questions?

Dr. Michael Koehler (DHS)

Michael.Koehler@hq.dhs.gov