

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



**NICE 2016 Pre-Conference Seminar
NICE Cybersecurity Workforce Framework (NCWF)
October 31, 2016**

Bill Newhouse, Deputy Director of NICE

Using the NICE Cybersecurity Workforce Framework

Participants will learn about the [NICE Framework](#) by spending time with three different teachers who have used it to support specific cybersecurity workforce needs.

Expected Seminar Outcomes:

- Learn how to use the NICE Workforce Framework for workforce development and see examples of how it has been used to date.
- Learn about resources for cybersecurity workforce planning, recruiting, training, and retention supported by the NICE framework including the [DHS Education and Training Catalog](#) Portal with its [Workforce Development Toolkit](#).
- Network with representatives from other organizations who are building their cybersecurity workforce using the NICE framework and its associated tools.
- Learn how to create cyber-specific positions using the [DHS CMSI PushButtonPD Tool](#).

Using the NICE Cybersecurity Workforce Framework

Stage Setters:

- **Bill Newhouse**, NICE Deputy Director, NIST, will describe the new draft NIST Special Publication 800-181, the NICE Cybersecurity Workforce Framework, which is to be released for public comment on November 2, 2016.
- **Stephanie Keith**, Chief, Cyber Workforce Strategy & Policy Division, Office of the Deputy DoD Chief Information Officer – Cybersecurity, will describe future DoD Issuances that will be supported by the NICE Framework.

Teachers:

- **Kevin McDonald and Tim Herbert, CompTIA**, will offer a perspective of how the NICE Framework is used in various situations involving customers and partners and the use of the framework in the soon-to-be released cybersecurity jobs heat map.
- **Leo Van Duyn, JP Morgan Chase & Co.**, will describe his use of the NICE Framework to meet workforce needs within his company.
- **Keith T. Hall, DHS**, will describe how he built the DHS CMSI PushButtonPD tool to improve DHS's cybersecurity position descriptions (job announcements).

Draft NIST Special Publication 800-181

**NICE Cybersecurity Workforce
Framework (NCWF)**

National Initiative for Cybersecurity Education (NICE)

Bill Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

The NCWF will be available for public comment on November 2, 2016

<http://csrc.nist.gov/publications/PubsDrafts.html>

Deadline to submit comments: January 6, 2017

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

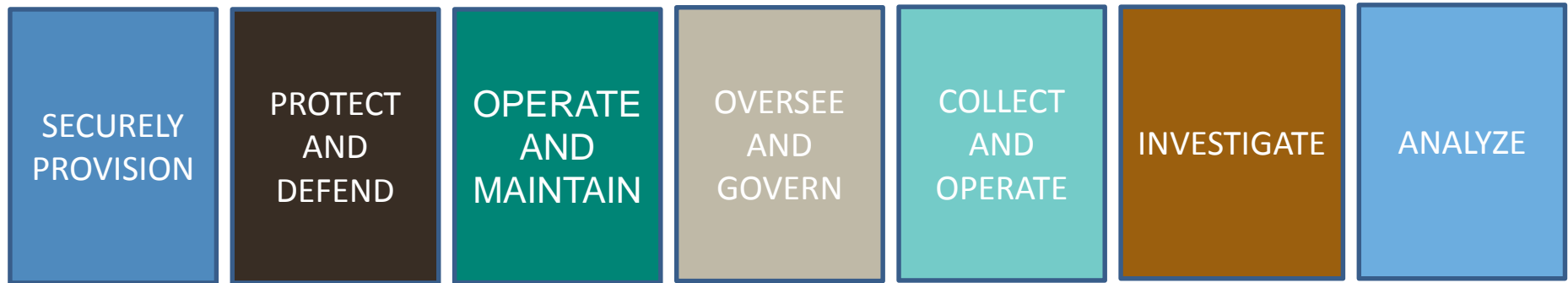
3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

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 Cybersecurity Workforce Framework

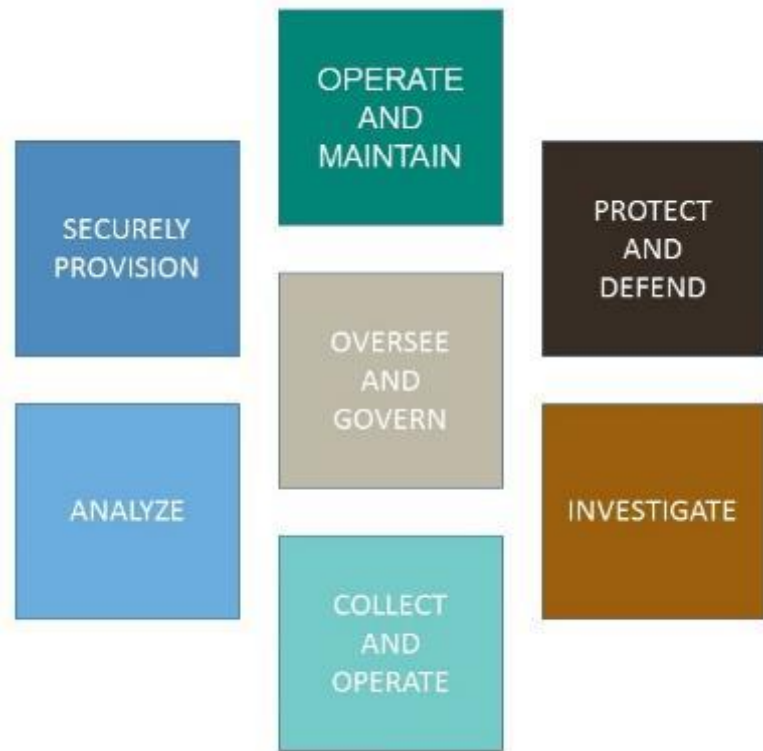
- 7 Categories, 30+ Specialty Areas, 50+ Work Roles
- Baselines Knowledge, Skills, and Abilities & Tasks
- Reference Resource for cybersecurity workforce development



- Version 1.0 (an interactive pdf and website) posted in April 2013
- Version 2.0 (a spreadsheet) posted in May 2014
- Draft NICE Special Publication 800-181 posted 2 Nov 2016

Key Audiences

- Employers
- Current and Future Cybersecurity Workers
- Training and Certification Providers
- Education Providers
- Technology Providers



As a mechanism to organize information technology (IT), cybersecurity, and cyber-related work, the NCWF helps organizations organize roles and responsibilities through the following components:

Categories – A high-level grouping of common cybersecurity functions;

Specialty Areas – Distinct areas of cybersecurity work;

Work Roles – 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.