NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Presidential Executive Order on America's Cybersecurity Workforce: Enhancing Workforce Mobility and Supporting the Development of Cybersecurity Skills

May 15, 2019

Kevin Reifsteck

Director for Critical Infrastructure Cybersecurity

National Security Council

The White House

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Context for America's Cybersecurity Workforce Executive Order

Executive Order 13800: Strengthening Cybersecurity in Federal Networks and Critical Infrastructures (May 2017)

> . . . the United States seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace.

- **Assess the scope and sufficiency of efforts** to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education
- Provide a report to the President with **findings and recommendations** regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.

Context for EO (continued)

National Cyber Strategy (September 2018)

Pillar II: Promote American Prosperity

Strategic Objective: **Develop a Superior Cybersecurity Workforce**

Priority Actions:

Build and Sustain the Talent Pipeline

Expand Re-Skilling and Educational Opportunities for Workers

Enhance the Federal Cybersecurity Workforce

Use Executive Authority to Highlight and Reward Talent

America's Cybersecurity Workforce Executive Order (May 2, 2019)

Policy Statements:

- The cybersecurity workforce is a strategic asset
- Workforce mobility facilitates seamless movement among employers
- Programs and services must be designed to support skills development
- Organizational and technological tools are needed to develop and enhance cybersecurity talents and capabilities
- Agency heads will be held accountable to manage cybersecurity risks in their enterprise, including the risk or vulnerability associated with having a skilled workforce and the ongoing development of skills

Focus of the Executive Order

- Strengthening the **Federal** Cybersecurity Workforce (Section 2)

- Strengthening the **Nation's** Cybersecurity Workforce (Section 3)

Deliverables Under Executive Order

- Reports – one-time and annual

  e.g., Within **180 days** . . . the Director of OPM . . . shall **identify a list** of cybersecurity aptitude assessments for agencies to use in identifying current employees with the potential to acquire cybersecurity skills for placement in reskilling programs to perform cybersecurity work.

- Programs – ongoing and sustainable

  e.g., Within **1 year** of the date of this order, the Secretary of Education . . . shall **develop and implement** . . . an **annual** Presidential Cybersecurity Education Award to be presented to one elementary and one secondary school educator per year

Federal Cybersecurity Workforce

- Cybersecurity Rotational Program
- Federal Contracts for Information Technology and Cybersecurity Services
- Aptitude Assessments to Reskill Current Employees
- Awards and Decorations for Uniformed Services and Civilian Personnel
- President's Cup Cybersecurity Competition
- List of Federal Government Cybersecurity Agencies and Subdivisions

Nation's Cybersecurity Workforce

- EO 13800 Report to the President Imperatives – and Recommendations
- Cyber-Physical Systems Personnel and Training Gaps
- Presidential Cybersecurity Education Award
- Voluntary Integration of NICE Framework into existing education, training, and workforce development efforts

Q & A

Daniel Stein

Branch Chief

Cybersecurity Education and Awareness

U.S. Department of Homeland Security

CISA
CYBER+INFRASTRUCTURE

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cybersecurity Rotational Assignment Program

- Purpose:
  - To grow the cybersecurity capability of the United States Government,
  - To increase integration of the Federal cybersecurity workforce, and
  - To strengthen the skills of Federal information technology and cybersecurity practitioners
- Within 90 days . . . the Secretary of Homeland Security . . . shall provide a report to the President that . . .
  - describes the proposed program,
  - identifies its resource implications, and
  - recommends actions required for its implementation.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

President's Cup Cybersecurity Competition

- Goal: To identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines.
- A plan must be submitted to the President within 90 days for an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees.
- The first competition shall be held no later than December 31, 2019, and annually thereafter.

Cyber-Physical Systems Personnel and Training

- Purpose: To strengthen the ability of the Nation to identify and mitigate cybersecurity vulnerabilities in critical infrastructure and defense systems, particularly cyber-physical systems for which safety and reliability depend on secure control systems
- Provide a report to the President . . . within 180 days that:
  - Identifies and evaluates **skills gaps** in Federal and non-Federal cybersecurity personnel and **training gaps** for specific critical infrastructure sectors, defense critical infrastructure, and the Department of Defense's platform information technologies; and
  - Recommends **curricula** for closing the identified skills gaps for Federal personnel and steps the United States Government can take to close such gaps for non-Federal personnel by, for example, supporting the development of similar curricula by education or training providers.

Q & A

Danielle Santos

Program Manager

National Initiative for
Cybersecurity Education (NICE)

NIST

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

NICE Strategic Plan (January 2016)

Vision: A digital economy enabled by a knowledgeable and skilled cybersecurity workforce.

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

Goals:

Section 3: Strengthening the Nation's Cybersecurity Workforce

- The Secretaries of Commerce and Homeland Security, in coordination with the Secretary of Education and other agencies as appropriate, shall execute the recommendations from the report to the President on **Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce** (Workforce Report) developed pursuant to Executive Order 13800.

- Priority imperatives include
  - **Launching a national Call to Action** to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;
  - **Transforming, elevating, and sustaining the cybersecurity learning environment** to grow a dynamic and diverse cybersecurity workforce;
  - **Aligning education and training with employers' cybersecurity workforce needs**, improve coordination, and prepare individuals for lifelong careers; and
  - **Establishing and using measures that demonstrate the effectiveness and impact** of cybersecurity workforce investments.

Workforce Report: 20 Recommendations, 47 Actions

Examples include:

- Encouraging educators, training providers, and employers to use the taxonomy and lexicon of the NICE Cybersecurity Workforce Framework.

- Developing model career paths for cybersecurity-related positions.

- Establishing a clearinghouse of information on cybersecurity workforce development education, training, and workforce development programs and initiatives.

- Establishing at least one regional alliance or partnership for cybersecurity education and workforce in each state.

Section 3: Strengthening the Nation's Cybersecurity Workforce

The Secretaries shall develop **a consultative process** that includes Federal, State, territorial, local, and tribal governments, academia, private-sector stakeholders, and other relevant partners **to assess and make recommendations to address national cybersecurity workforce needs** and to ensure greater mobility in the American cybersecurity workforce.

NICE Interagency Coordinating Council

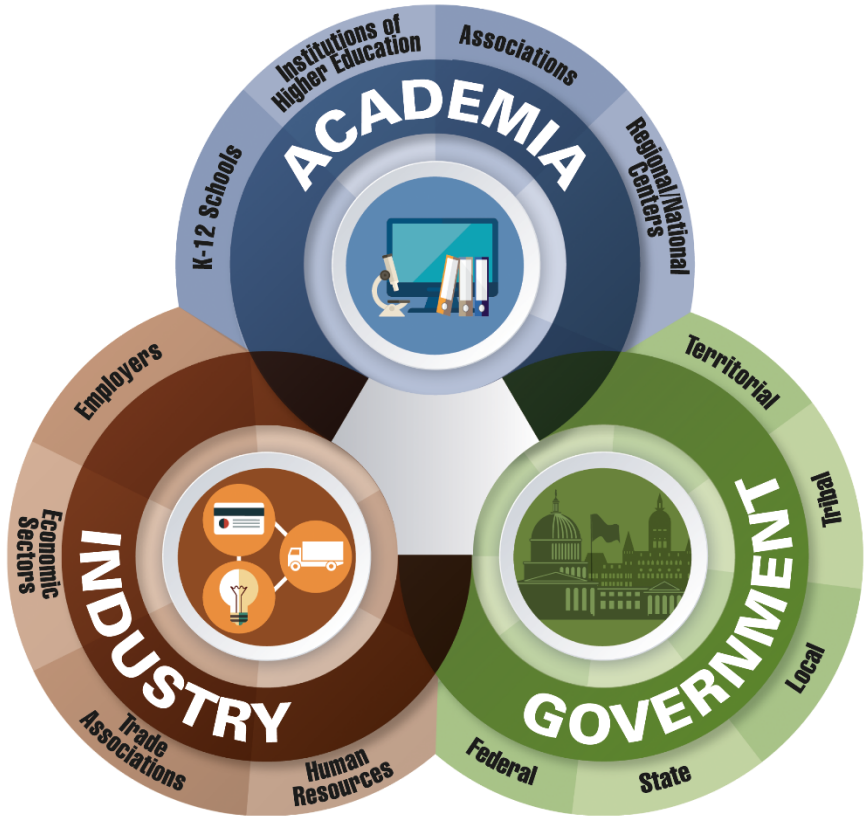
Convenes ***federal government*** partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development.

nist.gov/itl/applied-cybersecurity/nice/about/interagency-coordinating-council

NICE Working Group

Established to provide a mechanism in which ***public*** and ***private*** sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.

- K12
- Collegiate
- Training and Certifications
- Competitions
- Apprenticeship
- Workforce Management



nist.gov/nice/nicewg

Section 3: Strengthening the Nation's Cybersecurity Workforce

The Secretary of Commerce, the Secretary of Labor, the Secretary of Education, the Secretary of Homeland Security, and the heads of other appropriate agencies shall **encourage the voluntary integration of the NICE Framework into existing education, training, and workforce development efforts undertaken by State, territorial, local, tribal, academic, non-profit, and private-sector entities, consistent with applicable law.**

(iii) The use of the National Initiative for Cybersecurity Educa
Workforce Framework (NICE Framework) as the basis for cyb
requirements for program participants;

(ii) Ensure that contracts for information technology and cyber
include reporting requirements that will enable agencies to ev
personnel have the necessary knowledge and skills to perfor
in the contract, consistent with the NICE Framework; and

(iii) The parameters for the com
individual and team events that
Framework and other relevant
include competition categorie
reverse engineering and expl
analysis, cyber analysis, cyb
obfuscated coding, cyber-p

(i) Incorporate the NICE Framework lexicon and taxonomy into workforce
knowledge and skill requirements used in contracts for information technology
services;

(iii) Provide a report to the President, within 1 year of the date of this order, that
describes how the NICE Framework has been incorporated into contracts for
information technology and cybersecurity services, evaluates the effectiveness of
this approach
development of multiple services provided to the United States Government,
related to the NICE ns to increase the effective use of the NICE Framework

(d) The Secretary of Commerce, the Secretary of Labor, the Secretary of
Education, the Secretary of Homeland Security, and the heads of other
appropriate agencies shall encourage the voluntary integration of the NICE
Framework into existing education, training, and workforce development efforts
undertaken by State, territorial, local, tribal, academic, non-profit, and private-
sector entities, consistent with applicable law. The Secretary of Commerce shall
provide annual updates to the President regarding effective uses of the NICE
Framework by non-Federal entities and make recommendations for improving the
application of the NICE Framework in cybersecurity education, training, and
workforce development.

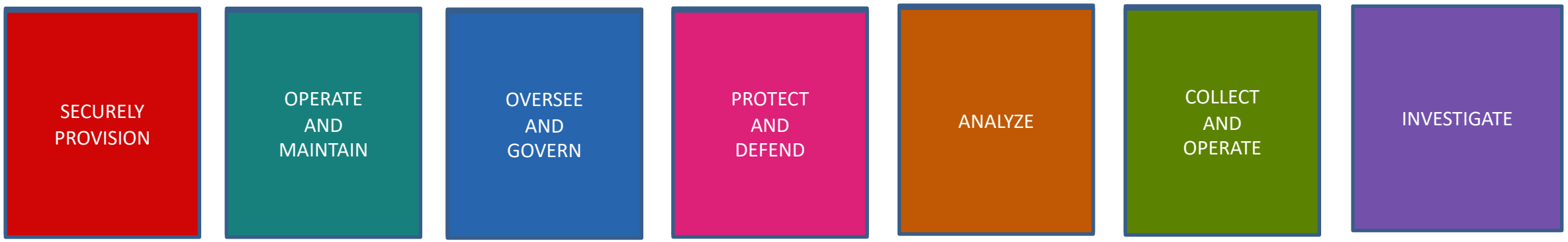
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181)

Audiences

- Public and Private Sector Employers
- Education Providers
- Technology Developers
- Current and Future Cybersecurity Workers
- Training and Certification Providers
- Policymakers

Cybersecurity Workforce Categories (7)

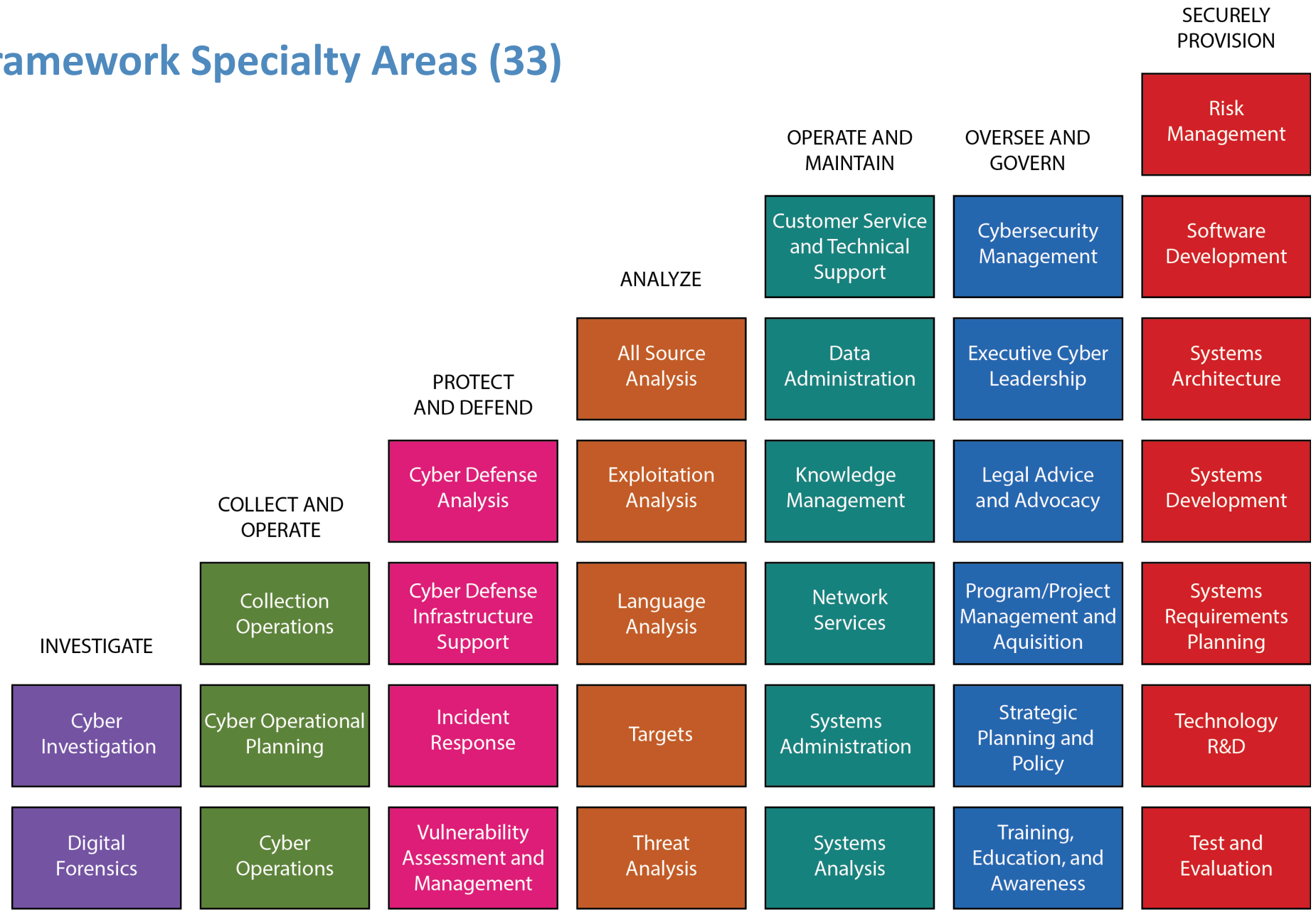


- **Specialty Areas** (33) – Distinct areas of cybersecurity work

- **Work Roles** (52) – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific *Knowledge, Skills, and Abilities (KSA's)* required to perform a set of *Tasks*.

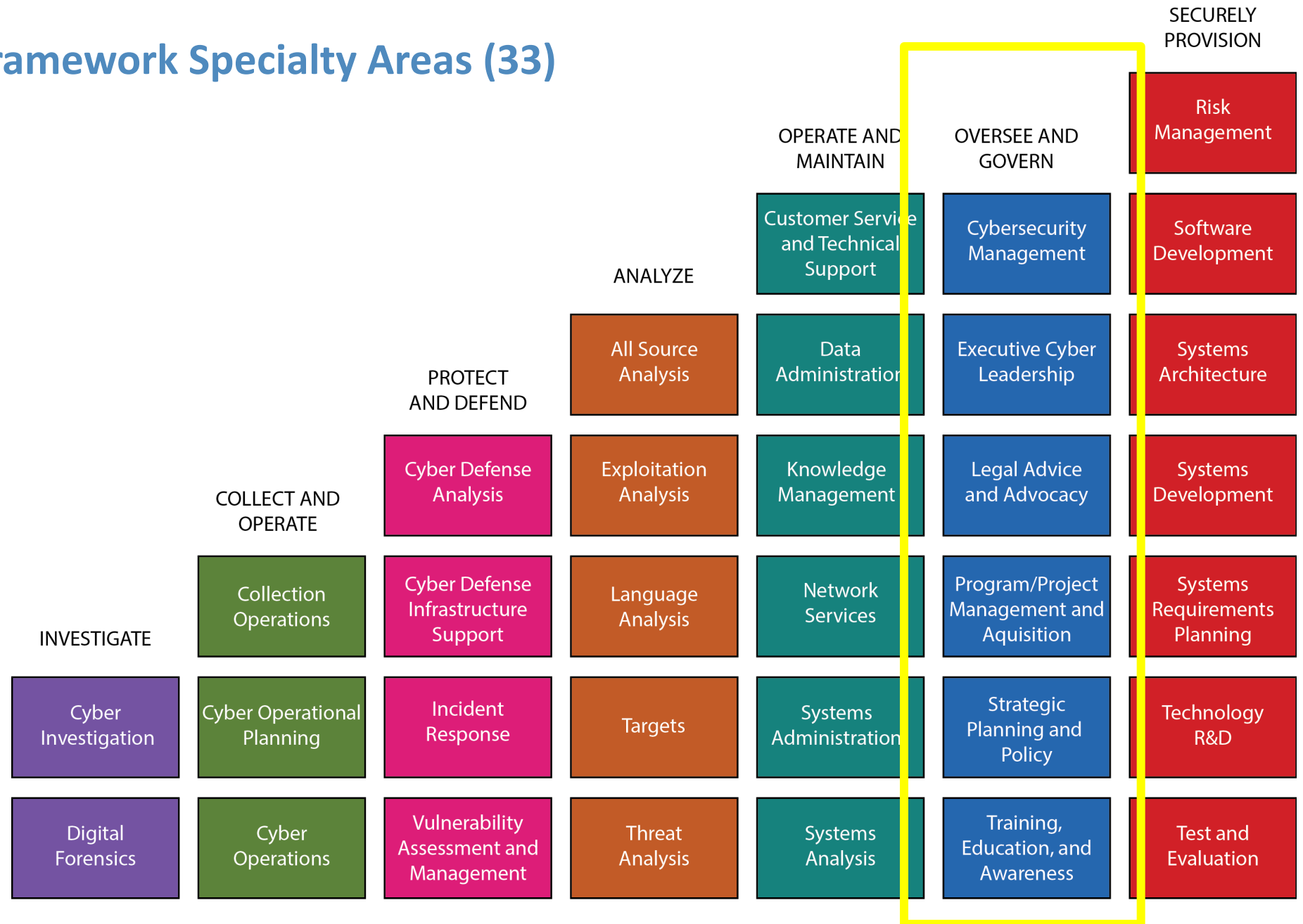
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Specialty Areas (33)



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Specialty Areas (33)



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

Federal Cybersecurity Workforce Assessment Act of 2015

- Assessment of the existing workforce
- Revision of coding structure to align with the NICE Cybersecurity Workforce Framework
- Coding of civilian positions and vacancies
- Identification areas of critical need

Application and Effective Uses of the NICE Framework

The Secretary of Commerce shall provide annual updates to the President regarding **effective uses of the NICE Framework** by non-Federal entities and make recommendations for improving the **application of the NICE Framework** in cybersecurity education, training, and workforce development.

Q & A

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Thank You for Joining Us!

Upcoming Webinar: "Tools in the Federal Cybersecurity Workforce Toolbox"

When: Wednesday, June 19, 2019 at 2:00pm EDT

Register: https://nist-nice.adobeconnect.com/webinar-may2019/event/registration.html

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION