NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

To promote and energize a robust ecosystem of cybersecurity education, training, and workforce development.

Cybersecurity Enhancement Act of 2014

Title IV: Cybersecurity Awareness and Preparedness

- Section 401: National Cybersecurity Awareness and Education Program (NIST with public-private sectors)
  - . . . continue to coordinate a national cybersecurity awareness and education program, that includes activities such as . . .
    - (5) **supporting formal cybersecurity education programs at all education levels to prepare and improve a skilled cybersecurity and computer science workforce for the private sector and Federal, State, local, and tribal government**; and
    - (6) promoting **initiatives to evaluate and forecast future cybersecurity workforce needs of the Federal Government and develop strategies for recruitment, training, and retention.**
  - (c) Strategic Plan.--The Director, in cooperation with relevant Federal agencies and other stakeholders, shall **build upon programs and plans in effect** as of the date of enactment of this Act **to develop and implement a strategic plan to guide Federal programs and activities in support of the national cybersecurity awareness and education program** under subsection (a).
  - (d) Report.--Not later than 1 year after the date of enactment of this Act, and **every 5 years** thereafter, the Director shall transmit the strategic plan under subsection (c) to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives.

NICE Strategic Plan – January 2016

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

Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures – May 2017

- Stated, among other things, that it is the policy of the United States "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."
- The **Secretary of Commerce** and Secretary of Homeland Security were directed to:

  1) "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"; and,

  2) "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."

Executive Order Expanding Apprenticeships in America – June 2017

- Purpose. America's education systems and workforce development programs are in need of reform.
- It shall be the policy of the Federal Government to provide more affordable pathways to secure, high paying jobs by promoting apprenticeships and effective workforce development programs.
- The Secretary of Labor (Secretary), in consultation with the Secretaries of Education and **Commerce**, shall consider proposing regulations . . . that **promote the development of apprenticeship programs by third parties**.
- The Secretary [of Labor] shall establish in the Department of Labor a **Task Force on Apprenticeship Expansion**. The mission of the Task Force shall be to identify strategies and proposals to **promote apprenticeships, especially in sectors where apprenticeship programs are insufficient.**

Executive Order Establishing the President's National Council for the American Worker – July 2018

Established the President's National Council for the American Worker, co-chaired by the **Secretary of Commerce**, the Secretary of Labor, the Assistant to the President for Domestic Policy, and the Advisor to the President overseeing the Office of Economic Initiatives.

- Develop recommendations for a **national strategy** for empowering American workers, which shall include recommendations on how the Federal Government can work with private employers, educational institutions, labor unions, other non-profit organizations, and State, territorial, tribal, and local governments to create and promote workforce development strategies that provide evidence-based, affordable education and skills-based training for youth and adults to prepare them for the jobs of today and of the future;
- Establish a Workforce Policy Advisory Board to recommend steps to encourage the private sector and educational institutions to combat the skills crisis by investing in and increasing demand-driven education, training, and re-training, including through apprenticeships and work-based learning opportunities

National Cyber Strategy – September 2018

Pillar II: Promote American Prosperity

Objective: Develop a Superior Cybersecurity Workforce

Priority Actions:

- Build and Sustain the Talent Pipeline
- Expand Reskilling and Educational Opportunities for America's Workers
- Enhance the Federal Cybersecurity Workforce
- Use Executive Authority to Highlight and Reward Talent

America's Cybersecurity Workforce Executive Order – May 2019

- Policy Statements:
  - America's cybersecurity workforce is a **strategic asset** that protects the American people, the homeland, and the American way of life.
  - The United States Government must **enhance the workforce mobility** of America's cybersecurity practitioners to improve America's national cybersecurity. During their careers, America's cybersecurity practitioners will serve in various roles for multiple and diverse entities. United States Government policy must **facilitate the seamless movement of cybersecurity practitioners between the public and private sectors**, maximizing the contributions made by their diverse skills, experiences, and talents to our Nation.
  - The United States Government must **support the development of cybersecurity skills** and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. The United States Government must also **recognize and reward the country's highest-performing cybersecurity practitioners and teams.**
  - The Nation is experiencing a shortage of cybersecurity talent and capability, and **innovative approaches are required to improve access to training that maximizes individuals' cybersecurity knowledge, skills, and abilities.** Training opportunities, such as **work-based learning**, **apprenticeships**, and **blended learning** approaches, must be enhanced for both new workforce entrants and those who are advanced in their careers.

Overview of Provisions of Executive Order

- Section 2: Strengthening the Federal Cybersecurity Workforce
  - Cybersecurity Rotational Assignment Program (DHS)
  - Contracts for IT and Cybersecurity Services use NICE Framework (GSA)
  - List of Cybersecurity Aptitude Assessments (OPM)
  - Existing Awards and Decorations Recognize Performance and Achievements in Cybersecurity (All)
  - President's Cup Annual Cybersecurity Competition (DHS)
  - Exemptions Under Federal Labor-Relations Management Program (OMB)
- Section 3: Strengthening the Nation's Cybersecurity Workforce
  - Execute Recommendations in Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce (Commerce and DHS)
  - Identify and Evaluate Skills Gaps in Cyber Physical Systems, Especially Critical Infrastructure and Defense Systems (DOD, DOT, DOE, DHS)
  - Annual Presidential Cybersecurity Education Award (ED)
  - Encourage Voluntary Integration of NICE Framework Into Existing Education, Training, and Workforce Development Efforts (Commerce, DOL, ED, DHS)

References to NICE Cybersecurity Workforce Framework

- Cybersecurity Rotational Assignment Program
  - The use of the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework (NICE Framework) as the basis for cybersecurity skill requirements for program participants;
- Federal Contracts for Information Technology and Cybersecurity Services
  - Incorporate the NICE Framework lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services;
- President's Cup Annual Cybersecurity Competition
  - The parameters for the competition, including the development of multiple individual and team events that test cybersecurity skills related to the NICE Framework and other relevant skills, as appropriate.
- Voluntary integration of the NICE Framework into existing education, training, and workforce development efforts
  - 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.

Contracts for IT and Cybersecurity Services use NICE Framework

The Administrator of General Services, in consultation with the Director of OMB and the **Secretary of Commerce**, shall:

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

(ii) Ensure that contracts for information technology and cybersecurity services include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the **NICE Framework**; and

(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** in improving services provided to the United States Government, and makes **recommendations to increase the effective use of the NICE Framework** by United States Government contractors.

List of Cybersecurity Aptitude Assessments

The Director of OPM, in consultation with the **Secretary of Commerce**, the Secretary of Homeland Security, and the heads of other agencies as appropriate, shall within 180 days . . .

- 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.
- Agencies shall incorporate one or more of these assessments into their personnel development programs.

Execute Recommendations in Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce

The **Secretary of Commerce** and the Secretary of Homeland Security (Secretaries), in coordination with others, shall . . .

- execute . . . **to the greatest extent practicable** the recommendations from the report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce
- 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

Priority consideration will be given to the following imperatives:

(i) To launch a national Call to Action to draw attention to and mobilize public- and private-sector resources to address cybersecurity workforce needs;

(ii) To transform, elevate, and sustain the cybersecurity learning environment to grow a dynamic and diverse cybersecurity workforce;

(iii) To align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for lifelong careers; and

(iv) To establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

Encourage Voluntary Integration of NICE Framework Into Existing Education, Training, and Workforce Development Efforts

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**
- 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

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

To promote and energize a robust ecosystem of cybersecurity education, training, and workforce development.