NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Growing and Sustaining the Nation's Cybersecurity Workforce

Rodney Petersen, Director of NICE

Executive Order 13800: Cybersecurity Policy

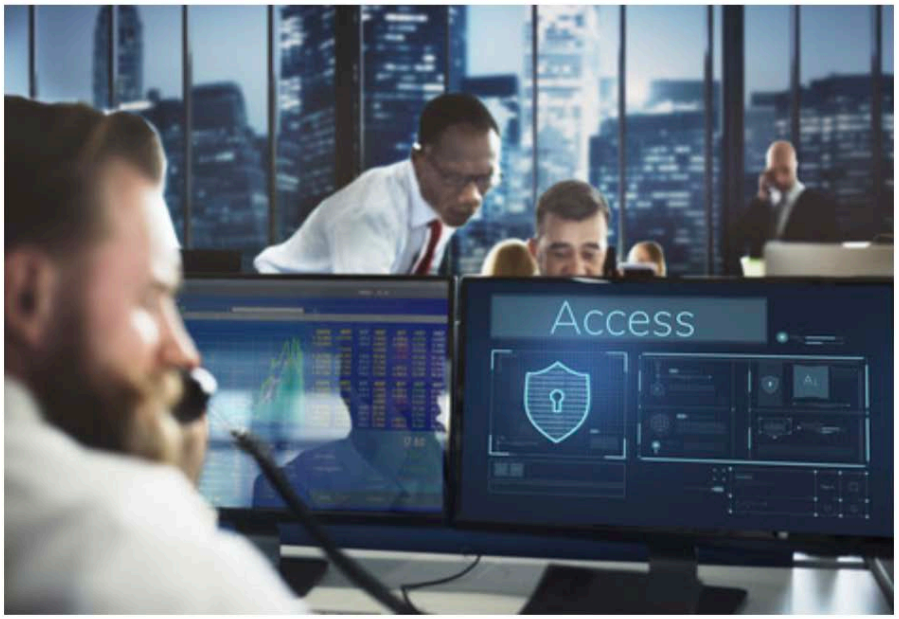
To ensure that the internet remains valuable for future generations, it is the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft. Further, **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.**

Public and Private Sector Workforce

- **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.

NIST

Report: U.S. needs immediate and sustained improvements in its cybersecurity workforce



WASHINGTON—In a report released by the White House today, the U.S. Departments of Commerce and Homeland Security urge immediate and sustained improvements in the country's cybersecurity workforce. The report, which was called for by the 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, includes findings and recommendations that address both public- and private-sector needs.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Website: nist.gov/nice/cybersecurityworkforce

Executive Order 13800: Growing and Sustaining the Cybersecurity Workforce

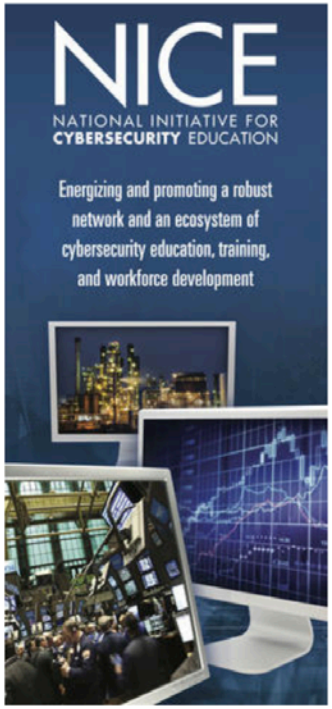
- Report
- Environmental Scan
- Findings and Recommendations
- Reference List
- Request for Information +
- Workshop on Cybersecurity Workforce Development
- Webinar: The President's Executive Order on Cybersecurity Workforce - Next Steps and How to Engage

Executive Order 13800: Growing and Sustaining the Cybersecurity Workforce

On May 11, 2017, the President of the United States issued the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. In part, the order states 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." Consequently, the Secretary of Commerce and Secretary of Homeland Security are 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."



With the active involvement of more than a dozen federal departments agencies, and with public input, the Commerce and Homeland Security Secretaries submitted a report to the President, Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce . A full list of federal contributors and details about private sector input is included in the report.

Key findings and recommendations from that report are available here.

Key Messages from the Report

- A strong and vibrant cybersecurity workforce is critical to our current and future national and economic security.
- The U.S. needs immediate and sustained improvements in its cybersecurity workforce.
- Collectively, the public and private sectors must do a better job of identifying, recruiting, developing, and retaining cybersecurity talent.
- This report provides practical and achievable recommendations that will require commitment and resources from both the public and private sectors.

Report Structure

- Executive Summary
- Vision for the Cybersecurity Workforce for the Future
- Imperatives, Recommendations, Actions
  - 4 Imperatives
  - 20 Recommendations
  - 47 Actions
- Appendixes (8)

  The Charge and Approach, State of the Cybersecurity Workforce, Executive Order 13800, Consolidated List of Recommendations and Actions, Request for Information, Webinar and Workshop, NICE Strategic Plan, Abbreviations and Acronyms

Vision for the Future

Prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity

Imperatives

- Launch a national Call to Action to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.
- Transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.
- Align education and training with the cybersecurity workforce needs of employers and prepare individuals for lifelong careers.
- Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

Key Recommendations

- The federal government should lead in launching a high-profile national *Call to Action* to draw attention to and mobilize public and private sector resources to address cybersecurity workforce needs.
- The Administration should focus on and recommend long-term authorization and sufficient appropriations for high-quality, effective cybersecurity education and workforce development programs in its budget proposals in order to grow and sustain the cybersecurity workforce.

Key Recommendations (continued)

- Federal agencies must quickly address major needs relating to recruiting, developing, and retaining cybersecurity employees and continue to implement the Federal Cybersecurity Workforce Strategy and the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA).
  - Agencies are carrying out their responsibilities, but they need to move even more aggressively.

Key Recommendations (continued)

- *Emphasize and expand opportunities for retraining* so that current and displaced workers and veterans can reskill to take on cybersecurity roles.
- *Build on and strengthen hands-on, experiential and work-based learning approaches*—including apprenticeships, research experiences, co-op programs, and internships.
- *Use virtual training and assessment environments* to augment the limited cadre of teachers and other educators and trainers and to improve assessment tools that match candidates with the skills and knowledge needed to succeed in the workforce and as life-long learners.

Key Recommendations (continued)

- *Expand the availability and expertise of teachers and faculty* through incentives and policy changes.
- *Provide greater financial assistance and other incentives* to reduce student debt or subsidize cybersecurity education and training costs.
  - Align education and training with employers' cybersecurity workforce needs, improve coordination, and prepare individuals for life-long careers.
  - Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

Actions

- *A variety of the recommendations are being pursued by **federal agencies** under existing authorities as resources allow*. These include:
  - Making greater use of the NICE Cybersecurity Workforce Framework to strengthen approaches to guide career development and workforce planning. SIJO8G
  - Other steps to address needs relating to recruiting, developing, and retaining cybersecurity employees.
  - Implementing the Federal Cybersecurity Workforce Strategy and the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA).
- Likewise, recognizing the urgency of the situation, **private sector organizations** are continuing to advance their cybersecurity workforce programs.

Nurture A Diverse Learning Community

Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

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

Guide Career Development & Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

NICE Cybersecurity Workforce Framework

NIST Special Publication 800-181

Reference Resource for Cybersecurity Workforce Development

- **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*.

CyberSeek™

About | Interactive map | Career pathway | Who this tool is for | Project partners

Cybersecurity Supply/Demand Heat Map

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

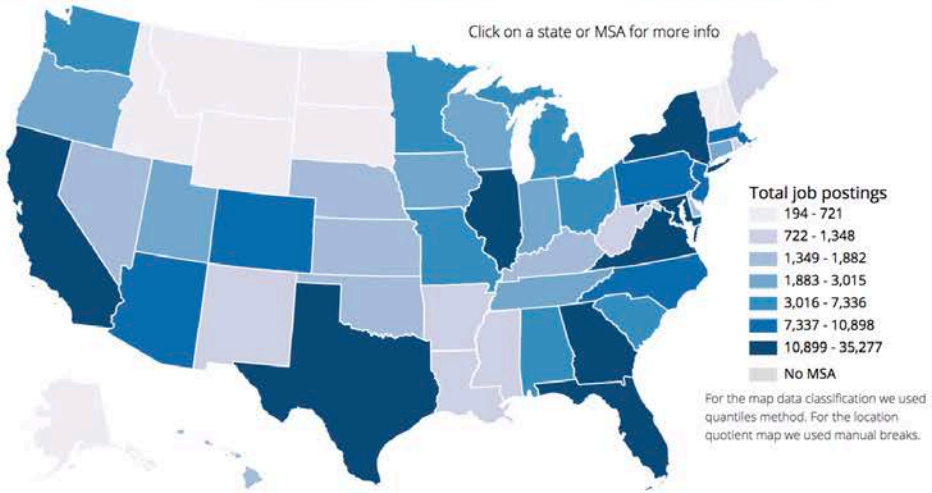
Share | Embed

States | Metro Areas

All Data | Public Sector Data | Private Sector Data

Total job openings

Search State



National level

TOTAL CYBERSECURITY JOB OPENINGS
301,873

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
768,096

SUPPLY OF CYBERSECURITY WORKERS
Very Low
CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

National average
2.5

GEOGRAPHIC CONCENTRATION
Average
LOCATION QUOTIENT

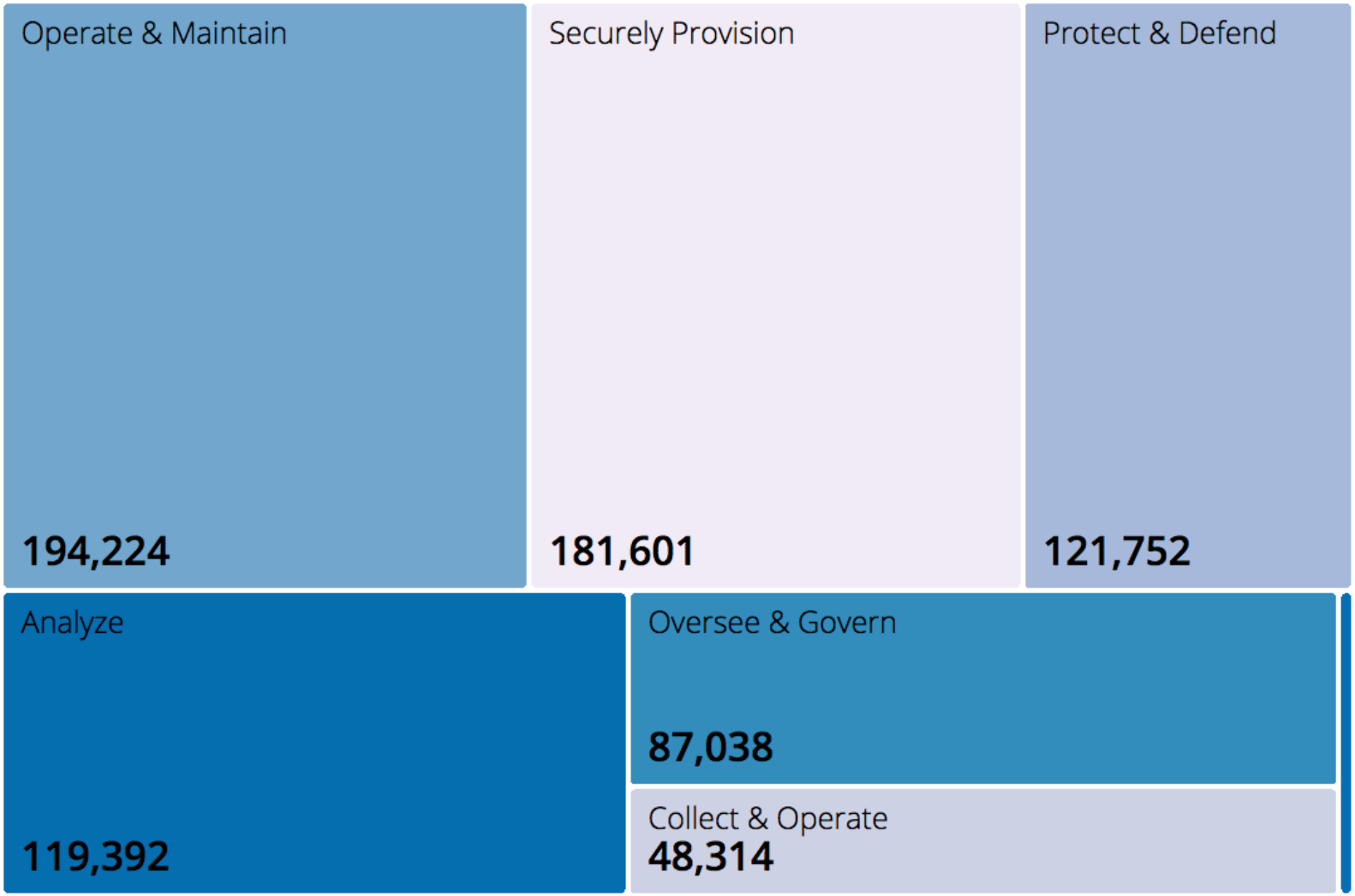
National average
1.0

TOP CYBERSECURITY JOB TITLES

- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Vulnerability Analyst / Penetration Tester
- Systems Administrator
- IT Auditor

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Engagement Process

- NICE Working Group

  Subgroups: K-12, Collegiate, Competitions, Training and Certifications, Apprenticeships, and Workforce Management
- NICE Interagency Coordinating Council
- NICE Webinars (Monthly)
- NICE eNewsletter (Quarterly)
- NICE Email Updates (Periodic)
- NICE Events

  NICE Conference & Expo: November 6-7, Miami, FL

  NICE K12 Cybersecurity Education Conference: Dec 3-4, San Antonio, TX
- National Cybersecurity Career Awareness Week: November 12-17

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

For more information, visit

nist.gov/nice/cybersecurityworkforce