



A report by a Panel of the National Academy of Public Administration for the Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security

A Call to Action

The Federal Government's Role in Building a Cybersecurity Workforce for the Nation

ISPAB Meeting

Thursday, March 10, 2022

Panel of Academy Fellows:

Dan Chenok (Co-chair)
Karen Evans (Co-chair)
Dr. Marilu Goodyear

Dr. Costis Toregas
Daniel Weitzner



Scope of Work

This study was requested by Congress as part of the FY 2021 Consolidated Appropriations Act.

Through interviews and documentary research, the report answers the following research questions:

1. What is the current state of CISA and other federal cybersecurity workforce programs, and what are their responsibilities and challenges?
2. What can the federal government do to create a sufficient workforce with the necessary knowledge and skills to meet the nation's short- and longer-term cybersecurity needs?
3. Within the larger context, where and how could—or should—CISA lead or participate in meeting the nation's cybersecurity workforce needs? How well are current initiatives working, and how effective and scalable are the partnership models CISA is currently using to meet its objectives?
4. What governance arrangements will result in clear leadership priorities being articulated and then implemented through transparent coordination across the federal government, other governments, educators, and the private sector to meet the nation's cybersecurity workforce needs most effectively and efficiently?

Methodology

- To answer this charge, the Academy convened an expert Panel with broad cybersecurity knowledge and backgrounds and established a highly qualified Study Team. Under the Panel's direction, the Study Team:
 - Analyzed CISA documents and information, and asked CISA to self-assess its workforce development programs against three criteria specified by Congress (scalability, diversity, and excellence)
 - Reviewed documents on cybersecurity workforce development, data on workforce needs, other federal agency workforce development programs, congressional hearings and legislation, reports, media coverage, and relevant presentations
 - Interviewed approximately 90 stakeholders, experts, current and former CISA officials, and experts and practitioners in academia, the private sector, and SLTT governments
- These data were used to assess CISA's workforce development programs, identify workforce development challenges and opportunities, and develop recommendations.

Panel of Academy Fellows and Study Team

Panel



Daniel Chenok

Panel Co-Chair

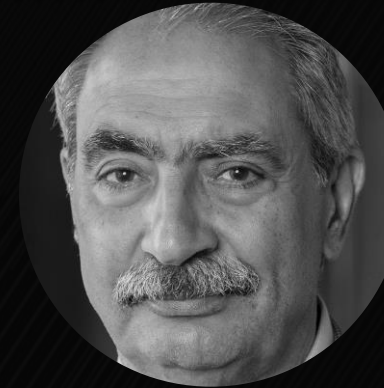


Karen Evans

Panel Co-Chair



Dr. Marilu Goodyear



Dr. Costis Toregas



Daniel Weitzner

Study Team

Brenna Isman, Director of Academy Studies
Sarah (Sally) Jaggart,* Project Director
Maria Rapuano, Senior Advisor
Jonathan Tucker, Senior Research Analyst
Adam Darr, Senior Research Analyst

Allen Harris, Senior Research Associate
Elise Johnson, Senior Research Associate
Sarah Jacobo, Intern

*Academy Fellow

Overview of Recommendations

The Panel's recommendations focus on:

- The need for a comprehensive government-wide cybersecurity workforce development strategy
- The leadership, strategy, and coordination of an effective governance structure that can enable existing programs operated by multiple agencies to build upon their progress and success
- ONCD's role in developing and implementing an operating model and governance structure to integrate actions by CISA, NSA, NIST, DoD, and other relevant federal agencies and organizations involved in cybersecurity workforce development
- Ensuring data relevant to cyber workforce challenges and needs are collected and available for use in developing strategy, creating educational programs, and assessing the impact and effectiveness of workforce development initiatives
- Routinely assessing the funding, staffing, resources, and authorities CISA needs to develop effective partnerships and drive progress with its workforce development programs

Government-Wide Strategy

This government-wide strategy should include the following four elements:



Element 1

Encouraging more people to choose a career in the cybersecurity field through outreach and education



Element 2

Enabling education and training to build needed competencies and alternative pathways to cybersecurity careers



Element 3

Overcoming barriers to recruiting talent and matching people to jobs



Element 4

Assessing performance and promoting innovation in workforce development practice

NICE Strategic Plan and Implementation Plan

To energize, promote, and coordinate a **robust community** working together to advance an **integrated ecosystem** of cybersecurity **education, training, and workforce development**.

NICE also has a framework for outreach and regularly holds events and community convenings.

Cyber Strategy can build off and advance NICE Plan



Promote the Discovery of Cybersecurity Careers and Multiple Pathways



Transform Learning to Build and Sustain a Diverse and Skilled Workforce



Modernize the Talent Management Process to Address Cybersecurity Skills Gaps



Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)



Drive Research on Effective Practices for Cybersecurity Workforce Development

Governance Framework

Purpose: A governance framework creates structure and processes for decision making and effective collaboration, including planning, priority setting, assigning roles and responsibilities, and accountability.

The three essential components for effective governance are:

- Leadership
- Strategy
- Coordination

The creation of the Office of the National Cyber Director—located within the Office of the President—presents a unique opportunity to establish such a framework to achieve the coordination and collaboration to address national cybersecurity workforce needs.

The ONCD can build upon existing programs and progress developed and operated by multiple agencies and departments – such as NICE -- to lead the development of a national cyber workforce strategy, monitor its implementation, and manage interagency coordination.

Contact

Brenna Isman

Director of Academy Studies

National Academy of Public Administration

Blisman@napawash.org

Connect with the Academy



About the Academy



The National Academy of Public Administration is an independent, nonprofit, and non-partisan organization established in 1967 and chartered by Congress in 1984. It provides expert advice to government leaders in building more effective, efficient, accountable, and transparent organizations. To carry out this mission, the Academy draws on the knowledge and experience of its over 950 Fellows—including former cabinet officers, Members of Congress, governors, mayors, and state legislators, as well as prominent scholars, career public administrators, and nonprofit and business executives. The Academy helps public institutions address their most critical governance and management challenges through in-depth studies and analyses, advisory services and technical assistance, congressional testimony, forums and conferences, and online stakeholder engagement. Learn more about the Academy and its work at www.NAPAwash.org.

The views expressed in this report are those of the Panel of Academy Fellows. They do not necessarily reflect the views of the Academy as an institution.