NATIONAL ACADEMY OF PUBLIC ADMINISTRATION®

A Call to Action

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

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

January 2022

Contents

Scope of Work

- This study was requested by Congress as part of the FY 2021 Consolidated Appropriations Act.
- Research questions pursued are:
  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.

Background and Landscape

- Developing a professional cybersecurity workforce is critical to an effective national response to cybersecurity challenges, a responsibility of the federal government.
- Estimates of the significant and increasing national cybersecurity workforce "gap" range in the hundreds of thousands across the US and in the millions worldwide.
- Military and civilian agencies have been preparing for and responding to growing cybersecurity threats for several decades. A range of public and private sector agencies and actors are increasingly involved in multiple aspects of workforce development to meet cyber-related needs—including curriculum development, training, certification, apprenticeships, and research.
- Federal agencies with key roles and activities include CISA, DoD, NSA, ED, NIST/NICE, NSF, OMB, OPM, and others that execute a variety of long-standing and, in some cases, relatively new programs and initiatives with a range of purposes.
- Academia (from K-12, experiential learning programs, and university levels) and private sector technology companies of many types are performing multiple, important roles in workforce development. This is far from just a government-sponsored initiative or need.
- However, these activities and approaches are neither strategic, coherent, integrated, prioritized, nor evaluated for impact and effectiveness.

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.

Background and Landscape (cont.)

- For more than a decade, NIST's National Initiative on Cybersecurity Education (NICE) has worked via a collaborative process to define cybersecurity work roles and related knowledge and skills, chiefly in the federal government
- In recent years, NIST has sought to better adapt the NICE framework to reflect the work roles in private industry and facilitate the use of its framework in company human capital processes.
- In keeping with a 2014 Congressional mandate, the NICE Strategic Plan (developed every five years) is intended to advance an "integrated ecosystem" of cybersecurity education, training, and workforce development.
- Thus, the NICE program provides a fundamental framework to build on.

Government-Wide Strategy for Developing the National Cybersecurity Workforce

Government-Wide Strategy

Finding 1: The federal government lacks a comprehensive, integrated government-wide strategy for developing a national cybersecurity workforce.

Recommendation 1: The National Cyber Director, in consultation with the CISA Director and other relevant leaders, should lead the creation of a government-wide strategy to develop the national cybersecurity workforce. The strategy should reflect the following guiding principles and priorities:

- Addressing both federal government and national workforce development needs
- Partnering with industry, academia, and nonprofits to achieve goals and priorities
- Reaching out to and engaging underrepresented populations and communities
- Considering the needs of SLTT governments and leveraging and supporting their workforce development initiatives
- Identifying areas where the federal government can serve as the model for implementing innovative and cost-effective approaches.

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

Enabling Alternative Pathways to Cybersecurity Careers

- The Panel sees apprenticeships as an important part of a strategy for enabling alternative pathways to cybersecurity careers.
- The cybersecurity workforce gap cannot be addressed by putting more people through four-year degree programs. Alternative modes of preparation are needed.
- However, to be successful, alternatives will need to earn employer confidence.
- One approach to boosting employer confidence in alternatives (as well as in traditional four-year degree programs) is the development of relevant scenario-based exercises for experiential learning and testing to verify certain competencies.
- Another approach is provided by apprenticeships, in particular Labor's Registered Apprenticeship Program, that provide
  - A structured approach to actual, on-the-job experience through mentoring, together with systematic classroom instruction tailored to the needs of employers
  - An opportunity to assess the fit of potential employees

Governance Framework for Cybersecurity Workforce Development

Governance Framework

Purpose: A governance framework creates structure and processes for decision making, 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 needed to address national cybersecurity workforce needs.

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

Governance Framework

Finding 1: Although active collaboration between leaders of the Office of the National Cyber Director (ONCD) and CISA has led to great strides in coordinating initiatives and resources for meeting the nation's larger cybersecurity challenges, federal agencies are not clear about their developmental, implementation, and operational responsibilities for workforce development and how these fit together to accomplish the larger workforce development objectives of the nation.

Recommendation 1: The ONCD should develop and implement an appropriate operating model and governance structure to integrate actions by CISA, NSA, NIST, DoD, and other relevant federal agencies and organizations involved in building the cybersecurity workforce for the nation. This includes coordinating with and specifying roles and responsibilities between and among agencies.

Recommendation 2: Congress should ensure the ONCD has budget and performance assessment authority to lead and coordinate the programs that will develop the needed workforce, including authorities to drive agency implementation of these programs.

Governance Framework

Recommendation 3: The ONCD should establish and run a leadership working group or council for cybersecurity workforce development with responsibility for both government-wide and external cybersecurity workforce development programs.

- The ONCD should also charge a designated senior official as leader of this working group.
- The ONCD should specify the authorities and responsibilities of the group and its leader and identify the major federal member organizations. Private sector, SLTT governments, and academic representatives could also be included as working group members, as appropriate, based on objectives.

Recommendation 4: The ONCD should ensure 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.

- One way of accomplishing this would be to establish a Bureau of Cybersecurity Statistics or a similar organization.

A Review of CISA's Workforce Development Programs and Strategies

CISA's Workforce Development Programs

Congress asked the Academy to review how and how well CISA's Cybersecurity Defense Education and Training (CDET) group carries out its workforce development programs.

CISA's major workforce development programs include:

1. **Cybersecurity Education and Training Assistance Program (CETAP)**
   Develops K-12 cybersecurity curricula, professional development for teachers, and technology to classrooms.
2. **Non-Traditional Training Provider Grant (NTTP)**
   Expands cybersecurity talent pipeline by building pathways in underserved communities that include certifications and apprenticeships.
3. **Public Infrastructure Security Cyber Education System (PISCES)**
   Pairs post-secondary cybersecurity students with small local governments that have no cybersecurity expertise.
4. **Industrial Control Systems (ICS) Training**
   Highly technical training targeting the critical infrastructure community.
5. **President's Cup Cybersecurity Competition**
   Annual cybersecurity competition for federal employees and uniformed services personnel.

CISA's Workforce Development Programs

Congress identified three workforce development objectives, and the Panel defined the objectives as follows:

1. **Diversity**
   Expanding participation in the cybersecurity workforce by underrepresented groups, such as people of color, women, people with disabilities, people who are neurodivergent, and rural communities.

2. **Excellence**
   Enabling education/training that provides the competencies (mix of knowledge and skills) required to meet the needs of employers and to allow employees to advance in their careers.

3. **Scalability**
   Enabling rapid and cost-effective expansion; encompasses economies of scale such as developing education and training that meets multiple goals (e.g., training covering numerous areas of knowledge, skills, and abilities).

CISA's Workforce Development Programs

Finding 1: The planning and design of most of CISA's cybersecurity workforce development programs—as implemented by CDET—meet diversity, excellence, and scalability objectives identified by Congress.

Finding 2: CISA's workforce development programs succeed because of CDET's ability to identify and partner with organizations with a proven track record in cybersecurity and workforce development.

	Diversity	Excellence	Scalability
CETAP	• Underserved communities • Blind and visual impairments	• CYBER.ORG over 10 years experience in curriculum development • Stakeholder input	• Professional development and curriculum online • "Train the trainer" approach • Large-scale virtual competition next year
ICS Training	• Currently not applicable • Virtual training can now reach broader audience (domestic + international)	• Idaho National Laboratory. • Recognized globally for its relevance	• Advanced courses must be attended in person • Now has virtual courses with no attendee limit • Created virtual physical critical infrastructure range
NTTP	• Designed to reach underserved communities • Covers 8 of 10 CISA regions	• Grantees have experience creating training programs • Hands-on learning and apprenticeships	• Three-year pilot • Scalability factored into design of grant solicitation • Not possible to predict scalability at this time
PISCES	• Targets HCBUs and Minority Serving Institutions	• Pacific Northwest National Laboratory. • Hands-on experience examining cyber meta data for local government (<100 employees)	• Demonstrated potential scale • Funding constrains and varying state data laws currently prevent more partnerships • CDET intends to gradually scale the program
President's Cup	• Currently not applicable • Need authority and funding to target non-federal and underrepresented	• Software Executive Institute (SEI) • SEI leads in cyber and scenario-based training • Venue for highly skilled federal employees	• Potential to scale up • Future plans to share challenges and source code

CISA's Workforce Development Programs

Finding 3: Although CISA is not considered an education agency, CISA has the authority and responsibility under law to create programs focused on elementary and secondary education. There are several benefits of the Cybersecurity Education and Training Assistance Program's (CETAP) placement in CISA, as currently administered by CDET.

- Some question CISA's role in K-12 cybersecurity education and training.
- The law establishing CISA includes "increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education."

- CETAP is CISA's grant program focused on K-12 cyber education.
  - CYBER.ORG has been the only grantee since 2012.
  - CETAP is highlighted as a foundational cyber education program by the Solarium Commission.
  - CETAP's location in CISA provides access to cyber experts that lend credibility to the standards and helps in working with state boards of education to implement the curriculum.
- CETAP is not included in the president's budget request.

Recommendation 1: As a key approach to workforce pipeline building, the OMB, DHS, and CISA should sustain funding for CETAP in the President's budget request to better integrate and update the grant in accordance with future planned K-12 workforce activities.

CISA's Workforce Development Programs

Recommendation 2: Congress should provide CISA with additional grant-making authority to effectively partner with colleges, universities, and community colleges. The additional authority should allow CISA to issue grants that can last up to five years in duration. CDET is the entity responsible for these initiatives within CISA.

- CISA relies on grantees to implement and scale programs
- CISA is exploring hub-and-spoke model to scale cost effectively **(see visual in appendix)**
- Hub-and-spoke model successful with PISCES program
- Contract studying the model with DHS Cybersecurity Infrastructure Resilience Institute
- Expanding to additional hub schools will require grant-making authority to incentivize schools

Recommendation 3: Congress should periodically review and adjust CISA's staffing, resources, and authorities as CISA's cybersecurity workforce development program changes.

- Scalability is an essential feature of CISA's five workforce development programs
- As scale increases, additional staff capacity will likely be necessary
- CISA's workload is expanding. For example, the K-12 Cybersecurity Act of 2021 requires CISA to develop an online training toolkit for school officials.

Appendix

Element 1:

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

Recommended Focus Areas:

- Conducting outreach to underrepresented populations and communities
- Enabling K-12 educators to take advantage of cybersecurity curricula
- Ensuring that schools, particularly in underserved communities, have the necessary technology infrastructure in place to support teacher development and student participation in cybersecurity education and training, including competitions
- Exploring options for targeting the existing noncybersecurity workforce and adult learners for recruitment into the cybersecurity field and helping them acquire the necessary credentials

Element 2:

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

Recommended Focus Areas:

- Promoting the development of educational and training programs at institutions willing and able to provide high-quality, experience-based curricula and activities
- Helping to ensure relevant scenario-based exercises and low-cost, adaptable platforms for experiential learning are accessible to education and training institutions
- Supporting the adoption of apprenticeship programs by the public and private sectors

Element 3:

Overcoming barriers to recruiting talent and matching people to jobs

Recommended Focus Areas:

- Expanding the authorities of the Cyber Talent Management System (CTMS) program to provide flexibilities that will help the federal government compete with the private sector and attract and retain top talent
- Making the most of hiring flexibilities within the federal personnel system in the near term
- Making it easier for federal agencies to tap top private sector cybersecurity talent to meet immediate cybersecurity needs
- Increasing employer confidence in certifications and encouraging a more flexible approach to cybersecurity position qualifications

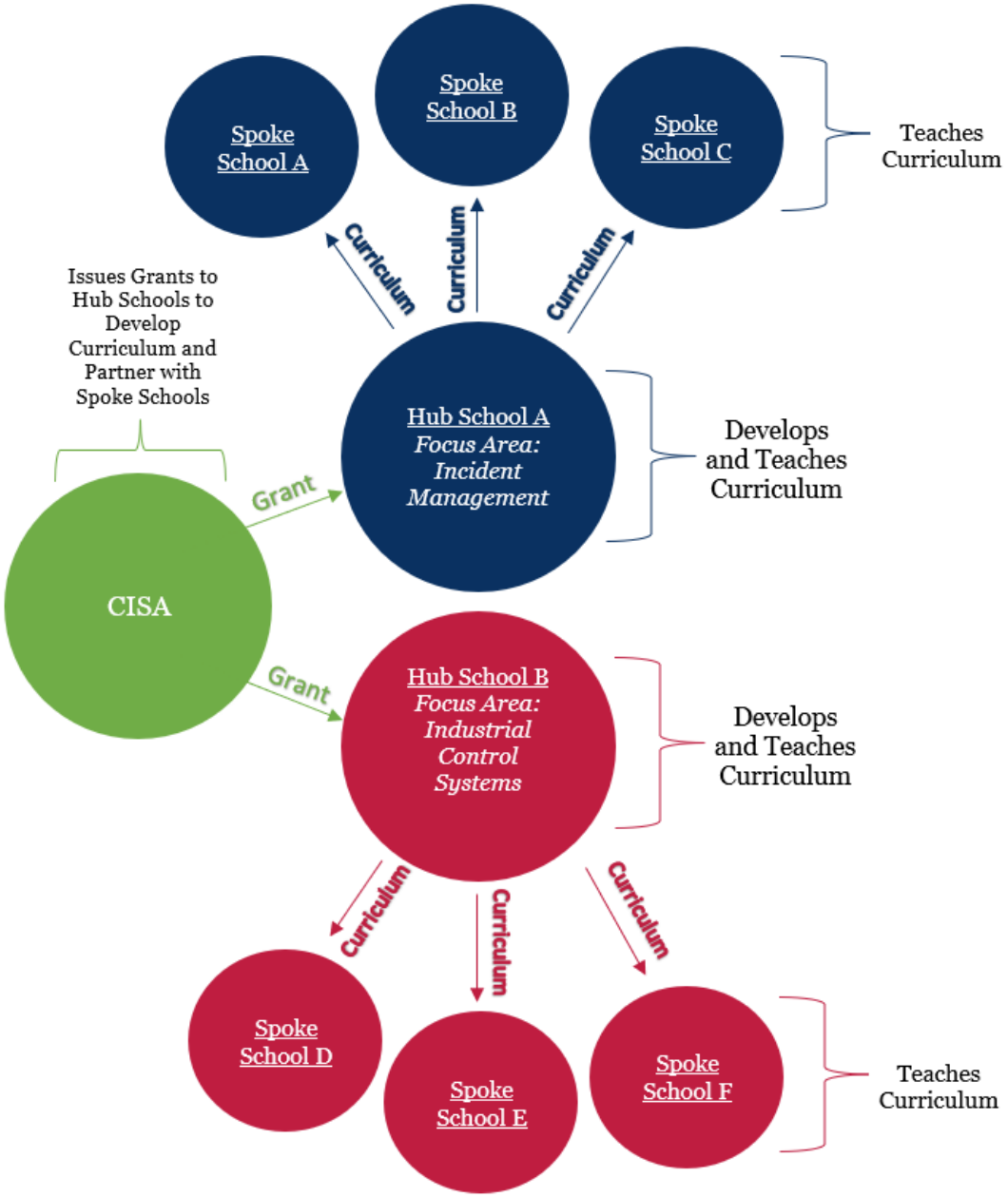
Element 4:

Assessing performance and promoting innovation in workforce development practice

Recommended Focus Areas:

- Evaluating the performance of federal programs and private sector approaches to workforce development
- Cultivating innovative approaches to workforce development

Visual Representation of Hub-and-Spoke Model



- CISA would issue a grant to a four-year university to serve as a "hub" for several "spoke" schools.
- Spoke schools would be a mix of geographically dispersed four- and two-year schools, including HBCUs and minority-serving institutions.
- Hub schools develop cybersecurity curriculum in specific concentration areas that spoke schools could implement, and the other spoke schools teach cybersecurity curriculum.

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) Jaggar,* 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

Contact

Brenna Isman
Director of Academy Studies
National Academy of Public Administration
BIsman@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.