MITRE's Response to the ONCD RFI on a National Cyber Workforce Strategy

November 3, 2022

For additional information about this response, please contact:
Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

©2022 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited. Case Number 22-01891-09.

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple federally funded research and development centers (FFRDCs), participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's 9,000-plus employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

Introduction and Overarching Recommendations

America's cyber workforce plays a critical role in supporting the country's national aspirations. Cybersecurity affects many aspects of the country, from national security and economic competitiveness to healthcare and elections—yet the cybersecurity workforce has been addressed by multiple players within an often-disconnected ecosystem. As the Office of the National Cyber Director (ONCD) works to develop a comprehensive national strategy, it should recognize, align with, and leverage (as appropriate) the federal government's broader human capital initiatives led by the Office of Management and Budget (OMB) and the Office of Personnel Management (OPM).[1, 2] The federal government is the country's largest employer and has a variety of cyber workforce needs, enabling it to pilot and assess impacts of innovative concepts for potential broader applications. In this section, MITRE thus provides a high-level overview of key federal workforce initiatives and opportunities that could support the federal government's goal of creating a robust national cyber workforce.

Pre-Existing Human Capital Flexibilities for Cyber Workforce

The Federal Cybersecurity Workforce Assessment Act of 2015 requires the OPM to establish procedures to implement the National Initiative for Cybersecurity Education (NICE) coding structure and to identify all federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.[3] In 2017, OPM issued guidance to support the appropriate coding needed to catalog cyber-related functions,[4] and in 2018, a subsequent OPM memo set forth agency requirements to

[1] MITRE responded to a previous RFI regarding the President's Management Agenda (PMA; https://www.performance.gov/pma/) and workforce considerations. This "North Star" approach can be found in detail at https://www.mitre.org/sites/default/files/2022-04/pr-21-01760-13-response-mitre-corporation-gsa-rfi-federal-workforce.pdf.

[2] Ibid. Two key principles are (1) employee tenures that may begin at the early career/change of career, mid-career, and/or end-of career stages; and (2) employee tenures that include joining, leaving, and re-joining the federal government, as well as an anticipation of regular migration across agencies.

[3] Workforce Framework for Cybersecurity (NICE Framework). 2022. Cybersecurity & Infrastructure Security Agency, https://niccs.cisa.gov/workforce-development/nice-framework. Last accessed October 31, 2022.

[4] Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions. 2017. Office of Personnel Management, https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity. Last accessed October 31, 2022.

identify critical needs and create strategies to fill those needs.[5] (Notwithstanding these efforts, in 2019, the U.S. Government Accountability Office reported that agencies had not yet sufficiently identified the civilian positions that required cyber skills and capabilities, despite having a human capital infrastructure that could document and convey critical hire needs and a template to develop an action plan.[6])

The federal government also has pre-existing flexibilities to attract, recruit, hire and retain top cyber talent, which could be leveraged within future ONCD activities and programs, including:

- Hiring, pay, and leave flexibilities for cyber positions[7]
- Compensation flexibilities for cyber professionals[8]
- Pathways Programs (Intern Program, Recent Graduates Program, and Presidential Management Fellows Program)
- CyberCorps
- National Centers of Academic Excellence
- OPM's Cyber Pool Hiring Action
- DOL's Cyber Apprenticeship program[9]

Diversity, Equity, Inclusion and Access Pre-Existing Requirements, Government-Wide Initiatives, and Pilots

This RFI coincides with the Presidential Management Agenda, Executive Order 14085, on Diversity, Equity, Inclusion, and Accessibility (DEIA) in the Federal Workforce, and other initiatives led by the OMB and OPM to improve the experience and diversity of the federal workforce, and to enable the federal work environment to be more inclusive.[10] The issue of recruiting, hiring, and retaining a high-quality workforce that is representative of the diversity in this nation is an administration priority. Although the cyber workforce has its own unique challenges, there are many opportunities to learn from existing DEIA and workforce best practices.

Government-led initiatives designed to support DEIA are instrumental tools to meet cyber workforce needs. As highlighted in later sections, these initiatives are designed to increase the diversity of the cyber workforce while tapping top talent who may not have otherwise considered careers in this field. Earlier this year, OPM and NICE hosted a webinar discussing the data efforts needed to understand cyber

---

[5] Guidance for Identifying, Addressing and Reporting Cybersecurity Work Roles of Critical Need. 2018. Office of Personnel Management, https://chcoc.gov/content/guidance-identifying-addressing-and-reporting-cybersecurity-work-roles-critical-need. Last accessed October 31, 2022.

[6] Agencies Need to Fully Implement Key Workforce Planning Activities. 2019. Government Accountability Office, https://www.gao.gov/assets/gao-20-129.pdf.

[7] Cybersecurity Hiring, Pay, and Leave Flexibilities. 2015. Office of Personnel Management, https://www.chcoc.gov/content/cybersecurity-hiring-pay-and-leave-flexibilities. Last accessed October 31, 2022.

[8] Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals. 2016. Office of Personnel Management, https://www.opm.gov/policy-data-oversight/pay-leave/reference-materials/handbooks/compensation-flexibilities-to-recruit-and-retain-cybersecurity-professionals.pdf.

[9] Cybersecurity. 2022. ApprenticeshipUSA, https://www.apprenticeship.gov/apprenticeship-industries/cybersecurity. Last accessed October 31, 2022.

[10] The President's Management Agenda enumerates four key strategies: "(1) Attract and hire the most qualified employees, who reflect the diversity of our country, in the right roles across the Federal Government; (2) Make every Federal job a good job, where all employees are engaged, supported, heard, and empowered, with opportunities to learn, grow, join a union and have an effective voice in their workplaces through their union, and thrive throughout their careers; (3) Reimagine and build a roadmap to the future of Federal work informed by lessons from the pandemic and nationwide workforce and workplace trends; and (4) Build the personnel system and support required to sustain the Federal Government as a model employer able to effectively deliver on a broad range of agency missions."

workforce needs, the applicability of promoting professional development and advancement, and successful practices used by the Federal Bureau of Investigation to attract cyber talent.[11]

Presidential Management Agenda Priority Area #1 (Empowering and Strengthening the Federal Workforce) and Related Activities to Address Critical Job Occupation Needs across Federal Agencies

Government-wide efforts have highlighted the imperative to cultivate a system that engenders a high-performing and talented federal workforce, while recognizing that an employee's career path will likely involve multiple employers. The President's Management Agenda sets forth the goal to strengthen and empower the federal workforce, with the following key success metrics:

- Create a more equitable employee engagement experience across the Federal workforce, including across employee groups and organizational units within agencies;
- Improve the Federal hiring process to efficiently hire the best talent;
- Attract the right talent for the right roles; and
- Promote diversity, equity, inclusion, and accessibility (DEIA) strategies and practices across all human capital activities.[12]

Complementing this PMA effort has been a specific focus on agencies' abilities to fill mission-critical occupations, which include cyber professionals, based on new Congressional charges pursuant to the America's Rescue Plan and the Infrastructure Investment and Jobs Act. Together, these efforts have created an immediate, actionable, and measurable impact.

With this landscape as a backdrop, ONCD can, in collaboration with federal agencies and the leadership of the Federal CISO, provide a cohesive cyber workforce approach for federal agencies. This approach can be one that explicitly sets forth how agencies can take advantage of the existing human capital flexibilities, statutory requirements, cyber workforce-specific programs, and other resources that are available to federal agencies. Insights gleaned can also be leveraged while developing and implementing this national cyber workforce strategy.

Questions Posed in the RFI

1) Area: Cyber Workforce

a) Sub-Area: Recruitment and Hiring

i) Attract people from communities that are underrepresented in cybersecurity and provide them opportunities to join the cyber workforce

Leverage Individuals with Special Neurodiverse Capabilities

Neurodiverse individuals, which include those with autism, are a potential, untapped source of talent to fill cyber positions across a wide range of employers. For example, autistic traits are associated with an increased presence in computing, IT, engineering, and physics disciplines, more advanced digital skills, 40% faster problem-solving, and better hacking and systematizing skills, all of which are critical in some of the country's hardest-to-fill roles. Yet, autistic job candidates are less likely to be hired due to interviewers' lack of knowledge about autistic traits (such as increased concrete thinking, processing

[11] Federal Cybersecurity Workforce Webinar: Impactful Diversity, Equity, Inclusion, and Accessibility Initiatives for the Federal Cybersecurity Workforce. 2022. National Institute of Standards & Technology, https://www.nist.gov/news-events/events/2022/01/federal-cybersecurity-workforce-webinar-impactful-diversity-equity. Last accessed October 31, 2022.

[12] Strengthening and Empowering the Federal Workforce. 2022. Office of Management and Budget, https://www.performance.gov/pma/workforce/. Last accessed October 31, 2022.

time, and sensory sensitivities, as well as reduced facial expressions, rapport, and reciprocation to smiles and handshakes), which often negatively impacts interviewers' impressions of job candidates.

MITRE has implemented an internal program to hire and retain such individuals and has designed and supported implementation of federal agency pilots to help agencies increase the population of neurodiverse employees, who are frequently underemployed.[13] In 2020, the National Geospatial Agency (NGA) was the first U.S. agency to participate in the Neurodiverse Federal Workforce[14] pilot, which takes the principles from the Autism at Work Playbook and adapts them to agency culture and requirements. Lessons learned from that pilot are being integrated into NGA processes and systems to help the agency better recruit and retain neurodivergent talent.[15] Information from NGA's experiences and those of other agencies that will participate in the pilot will be integrated into a federal version of the Autism at Work Playbook, set to publish in the second quarter of fiscal year 2023 (FY23). With proper direction, more agencies could learn from the pilot and adapt their practices—perhaps even expanding to a more wholistic program to help meet the federal government's, or the nation's, cyber workforce needs and to increase the participation of underrepresented neurodiverse individuals.

Leverage DEIA Analyses to Support Human Capital Outcomes

MITRE has developed and implemented approaches to improve the diversity and inclusivity of the federal human capital approach (which supports attracting, hiring, and retaining top talent in all fields, including cybersecurity) and has partnered with federal agencies to conduct federal workforce DEIA analyses. Through this work, it is apparent that a root cause analysis of barriers to equal employment is critical to develop actionable changes to increase and maintain the diversity of a workforce. Through root cause analysis, adhering to the guidance offered by the Equal Employment Opportunity Commission (EEOC) on barrier analysis, it is possible to identify underrepresented populations and key pain points for those underrepresented groups.[16] These analyses produce data-driven and evidence-based approaches to increasing and sustaining a diverse and inclusive workforce.

There is an opportunity to develop an approach to consistently analyze barriers to equal employment opportunities in the areas of hiring, retention, and executive leadership for cyber-related positions. Because each federal agency (or private-sector employer) is responsible for their own cyber workforce, a repeatable and consistent barrier analysis tool or methodology can be developed and used by agencies across the federal cyber workforce. The benefit of this consistent approach is that the analysis can provide a holistic view of the entire federal cyber workforce and consistent analysis across agencies of the barriers specific to cyber workforce job series during the employment life cycle. A consistent approach and aggregated data from various agencies would enable appropriate comparisons that can lead to government-wide and agency-specific recommendations. A consistent framework or approach to the cyber workforce life cycle would also guide how agencies meet the goals of the PMA and how OPM and the EEOC asses the rigor or quality of the barrier analyses.

MITRE has also developed a Federal Inclusivity Index Tool (FIIT) that analyzes workforce inclusion data to identify organizational barriers to an inclusive work culture and provides concrete actions to remedy or

[13] Individuals with disabilities are underemployed in both the public and federal sectors.

[14] Neurodiverse Federal Workforce Pilot Program. 2020. MITRE, https://nfw.mitre.org/. Last accessed October 31, 2022.

[15] D. Schiavone. Leading the Charge to Increase Neurodiversity in the Federal Workforce. 2021. MITRE, https://www.mitre.org/news-insights/impact-story/leading-charge-increase-neurodiversity-federal-workforce. Last accessed October 31, 2022.

[16] Instructions to Federal Agencies for EEO MD-715. 2022. U.S. Equal Employment Opportunity Commission, https://www.eeoc.gov/federal-sector/management-directive/instructions-federal-agencies-eeo-md-715-1. Last accessed October 31, 2022.

remove those barriers.[17] These approaches are critical to understanding the barriers to equal employment opportunities for any workforce, including cyber. It is critical for entities with a cyber workforce to measure the diversity of their cyber workforce and understand their perceptions of inclusivity to uncover and remedy those pain points that may prevent individuals from joining, participating, and staying in the cyber workspace. The FIIT enables agencies to respond to White House guidance by developing data-driven, DEIA-targeted workforce and human capital management strategies that can support their specific goals, measure the progress of their initiatives, and foster a culture of inclusion, and could serve as a model for similar national-level analyses.

ii) Improve learning pathways to careers in cybersecurity, including internships, apprenticeships, co-ops, and other work-based learning opportunities

Maximizing growth within the cyber career path requires targeted and cohesive development throughout its pipeline while simultaneously recognizing that staff may onboard and leave at various stages. MITRE conceptually views this pipeline as depicted in Figure 1, which could easily be genericized for application at the national level and complement the suite of cyber workforce-related tools and approaches already offered by OPM and other federal agencies.[18] It could also serve as a model for the private sector, though some adaptation will be required for smaller, less-technical organizations.

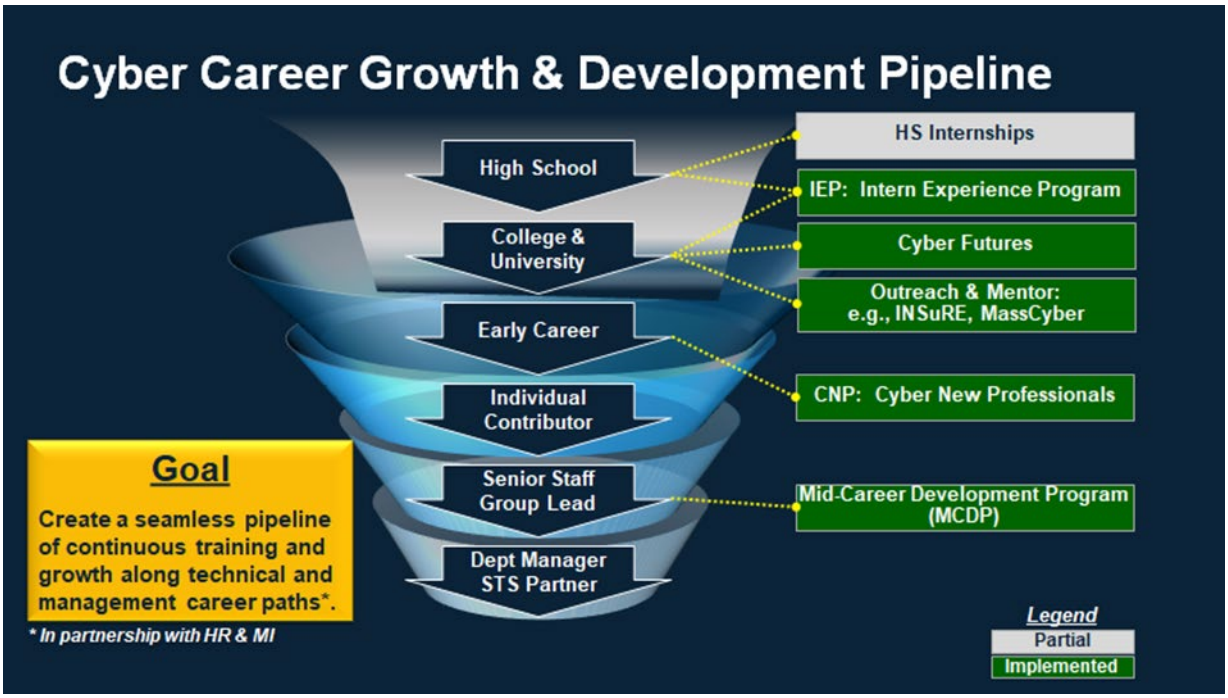


Figure 1 - Cyber Career Growth & Development Pipeline

We have developed learning programs at, and specific to, multiple stages within this pipeline. Brief descriptions and insights of the subset that could be of interest in a national context are provided below.

Intern Experience Program. MITRE designated cyber-oriented intern coordinators who work within their organizations to identify interesting projects for interns as well as opportunities for interns to meet

[17] The Federal Inclusivity Index Tool. 2021. MITRE, https://sjp.mitre.org/insights/610839d2139845001e9fe327. Last accessed October 31, 2022.

[18] For example, see Policy, Data, Oversight. 2022. Office of Personnel Management, https://www.opm.gov/policy-data-oversight/human-capital-management/cybersecurity/. Last accessed October 31, 2022.

one another and collaborate. Multiple interns return for multiple summers and then apply to MITRE for a full-time position upon graduation.

Cyber Futures. We launched a cybersecurity-specific internship program in FY21 to build a diverse cybersecurity workforce talent pipeline for national security. Participants are students from underrepresented populations who are early in their college careers—rising sophomores and juniors from participating historically black colleges and universities and minority-serving institutions—and represent multidisciplinary courses of study (e.g., computer science, engineering, business, policy).[19]

The Cyber Futures program has been operational for just two years, but early data suggests that exposing students early in their collegiate studies to the breath of career options/roles in cybersecurity will have meaningful influence over their decisions to follow cybersecurity career paths. Early data further suggests that students studying disciplines outside of "traditional" cyber-related fields (e.g., math, computer science) become increasingly interested and open to pursuing cyber careers once they understand the value to the field of disciplines outside of science, technology, engineering, and mathematics (STEM) as well as the opportunity to have significant impact through public service. Program data suggests that coupling hands-on technical training with federal mission-aligned capstone projects heightens students' awareness of cybersecurity career options and opportunities—specifically how to hone their cyber skills, and where and how to seek employment that supports national and economic security.

Outreach & Mentor. The Information Security Research and Education[20] (INSuRE) project is a collaboration between National Security Agency (NSA)-designated Centers of Academic Excellence institutions and government, FFRDCs, and national labs to connect students with cyber research projects. The vision for the program is to create a top-notch onboarding program with substantive hands-on learning and mentoring opportunities to build both knowledge and a personal professional network. It is successful in part because it offers what new graduates value: training and development, and mentorship.

Cyber New Professionals. MITRE established its Cyber New Professionals (CNP) program five years ago. It is a two-year rotational program for new professionals that concludes with the professionals "graduating" and transferring to organizations throughout the corporation. One key element of the program is the broad view we take of cyber, which contrasts with most students' relatively narrow initial view of cybersecurity. Through the program's Cyber Learning Path, students are introduced to the broad range of MITRE's cyber activities, from cyber strategy and policy, critical infrastructure security, and defensive cyber operations to privacy, cryptography, reverse engineering, adversary emulation, cloud security, and more. At completion, some students continue to focus on the aspect of cyber they discovered in college while others shift their focus to newly discovered aspects. But all students are able to leverage their newfound insights and broader perspectives in creative ways. We have seen a marked increase in hiring and retention of top talent early career cyber professionals because of this program.

[19] M. Manchenton. MITRE Prepares for a Second Wave of Cyber Futures Interns. 2022. MITRE, https://www.mitre.org/news-insights/impact-story/mitre-prepares-second-wave-cyber-futures-interns. Last accessed October 31, 2022.

[20] INSuRE. 2022. CAE in Cybersecurity Community, https://caecommunity.org/initiative/insure. Last accessed October 31, 2022.

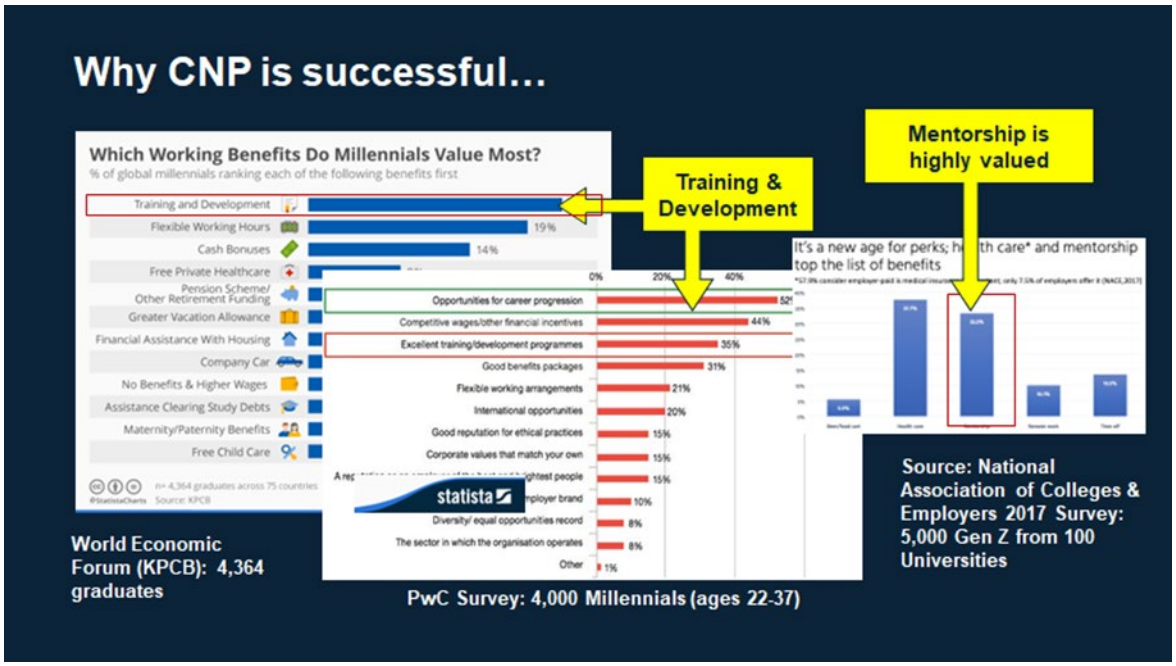


Figure 2 - Why CNP is successful

b) Sub-Area: Career Development and Retention

MITRE has developed a Cyber Workforce Development Framework to help developing nations build a cyber workforce strategy that leverages public-private partnerships. This framework is being applied on behalf of the U.S. State Department in several partner nations around the world, and by the Department of Homeland Security's Cyber Development, Education, and Training program in response to Solarium Commission recommendations.[21] Findings indicate that governments are usually best positioned to integrate the cyber ecosystem of industry, academia, cyber professionals, commercial training programs, and national security needs. They can convene leaders, develop standards, set long-range goals, incentivize progress and cooperation, and eliminate barriers. But government is not enough. The main finding of the framework survey is that public-private partnerships are key. Together, governments and private organizations can develop standards for training, job descriptions, and career pathways; develop policies that facilitate workforce development; and identify regional barriers for cyber career seekers. Specific findings and recommendations can be found in the Cyber Workforce Development Framework Excerpt presentation found in Appendix A of this document. Cases studies where this framework was applied are available in Appendix B.

c) Sub-Area: Data

ii) Measure the success efforts to advance diversity and inclusion in the cyber workforce

Cyber practitioners and national security officials often express alarm at the absence of diversity among cyber specialists in both the public and private sectors.[22] A more rigorous, coordinated approach to cyber workforce DEIA requires a baseline understanding of the current demographic composition of the cyber

[21] Construction of the framework began with a broad survey of tech workforce development approaches across nations of various sizes and economies, development non-governmental organizations (NGOs), and other subject matter experts. They identified commonalities, needs, and best practices in several categories and then synthesized the information into the Framework, focused on key areas and approaches.

[22] For example, see M. Miller. Biden Administration Establishes Program to Recruit Tech Professionals to Serve in Government. 2021. The Hill, https://thehill.com/policy/cybersecurity/570068-biden-administration-establishes-program-to-recruit-tech-professionals. Last accessed October 31, 2022.

field. Producing and sharing more comprehensive data on the makeup of the cyber workforce would support and accelerate operational changes to education, recruitment, training, and retention practices. Benefits include:

- Providing a baseline of cyber workforce DEIA for assessing the effectiveness of policies and programs. This can occur both at the enterprise level (e.g., evaluating whether a recruitment strategy increases the number of women who apply to security roles) and at a regional or national level (e.g., evaluating a K-12 program aiming to attract underrepresented groups to the cybersecurity field).
- Identifying priority areas for additional investment aimed at improving the diversity of the cyber workforce
- Enabling organizations and industry sectors to benchmark themselves in relation to similar entities. By leveraging the spirit of competition among rivals, this can help create marketing, branding, and recruitment incentives that drive organizations toward greater diversity without legal mandates.
- Highlighting the geographical roots of disparities within and across national and multinational organizations, which may be important in understanding the roles of different laws, policies, and cultures.
- Providing greater insight into issues like pay equity and promotion rates.
- Helping workers make informed decisions about potential employers by showing how seriously those employers take their public commitments to diversity and inclusion.

Supported by a grant from the Hewlett Foundation, MITRE examined the challenges associated with producing a demographic baseline of the nation's cyber workforce. MITRE partnered with Aspen Digital—a program of the Aspen Institute—to carry out the study based on a literature review, workshops, and interviews with cyber and workforce experts across industry, government, and academia. The results of this study were published in the report, "Diversity in the Cyber Workforce: Addressing the Data Gap."[23] The report discusses the benefits of having a diverse cyber workforce and describes the current state of knowledge regarding the diversity of that workforce. It identifies the most significant challenges associated with the collection, analysis, and distribution of cyber workforce diversity data and provides insights based on our research and inputs from key stakeholders. The report closes with a set of actionable recommendations that address the challenges described within.

The following insights from our study can be used by ONCD to develop well-informed policies for improving a demographic baseline of the nation's cyber workforce:

Types of data needed:

- Cyber workers are spread throughout an enterprise. While it is important to capture data on engineers and computer scientists, the community also need to identify managers, lawyers, policymakers, and non-technicians who are key players in the cyber arena.
- It is unclear which aspects of diversity can and should be collected. Biological characteristics like age, race, and birth sex are the easiest to capture. A full exploration of diversity would need to include ethnicity, sexual orientation and gender identity, neurodiversity, and perhaps other

[23] I. Lachow. Diversity in the Cyber Workforce: Addressing the Data Gap. 2022. MITRE, https://www.mitre.org/sites/default/files/2022-02/pr-21-01226-4-diversity-in-the-cyber-workforce-addressing-the-data-gap.pdf.

aspects as well. However, the collection of such data would be difficult and needs further exploration.[24]

Data collection process:

- Data collection should be voluntary.
- Data anonymization is critical.
- The security and privacy of the collected data must be paramount.
- Impacted communities need to be part of the data collection process and survey design. If they are not, data collection efforts might unintentionally perpetuate biases found in the field.
- A one-time snapshot of the cyber workforce is not helpful. To track progress and assess the utility of different policies and initiatives, it is imperative to gather longitudinal data based on consistent definitions and criteria.

Analysis and sharing:

- Data analysis is critical: Decision makers rely on analytical findings—raw data is not useful for their needs.
- Two sharing models deserve further exploration:
  1. Information Analysis and Sharing Organizations/Centers
  2. The Aviation Safety Information Analysis and Sharing model

Organization:

- The data collection, analysis, and dissemination functions must be run by a single organization. There are several requirements for that organization:
  1. It must be trusted by those providing the data. There cannot be any real or perceived conflicts of interest.
  2. It must be able to safeguard the data.
  3. It must employ or have access to a team of organizational psychologists, economists and/or statisticians, and cyber experts.
  4. It must be able to withstand ebbs and flows in political sentiment.
- Not-for-profit organizations provide the best option for taking on the role of collecting, storing, and analyzing cybersecurity diversity data. Several types of not-for-profit organizations appear to satisfy the criteria needed to do the job, including, but not limited to, industry associations, information sharing and analysis organizations/centers, think tanks, federally funded research and development organizations, and university-affiliated research centers.

Funding:

- Developing a useful demographic picture of the nation's cyber workforce will require information gathering, analysis, and dissemination over a period of years. This enterprise will require sustained funding that will likely cost several hundred thousand dollars per year.
- Industry is unlikely to fund such an activity initially and may not fund it at all. For this effort to succeed, it will require a consistent source of funds over several years. That type of funding is best provided by the federal government.

[24] MITRE discussed some of these considerations in a prior RFI response on LGBTQI+ Equity, which is available at https://www.mitre.org/sites/default/files/2022-10/pr-22-01891-04-mitres-response-ostp-rfi-help-inform-development-federal-evidence-agenda-lgbtqi%2B-equity.pdf.

Additional recommendations for action can be provided upon request.

3) Area: Training, Education, Awareness

Cybersecurity training, education, and awareness should be a community-wide endeavor, with important aspects being (1) to ensure input for analyses comes from a wide variety of sectors, and (2) to forge partnerships that include local government, local academic leadership,[25] and non-profit organizations. A good example is our work with the city of San Antonio, Texas.[26] The city's Chamber of Commerce and Cyber Industry Council have a close-knit relationship with the San Antonio government, which is consistently engaged on matters related to cybersecurity, including local and national legislative affairs, foreign visitors, and government speaking engagements at events. Related aspects include:

- The University of Texas at San Antonio (UTSA), which has attained Center of Academic Excellence status from NSA, Department Of Homeland Security (DHS), and Defense Intelligence Agency (DIA), houses the National Security Collaboration Center—a collaborative forum with participants from government, university, industry, national laboratories, and federally funded research and development centers. This collaboration is enhancing the San Antonio cyber security ecosystem.
- Protecting Local Communities in Cyberspace (Project Xander) is a public-private-academia collaboration where cyber professionals serve as mentors to teams of university students who perform cyber assessments and provide awareness of vulnerabilities and priority solutions to protect local nonprofits against cyber threats.[27, 28] Project Xander began as an initiative by San Antonio cyber leaders who were concerned with the rise of cybercrime in the form of ransomware attacks and identity theft impacting San Antonio and other local communities, and is being extended nationwide to other geographic areas and providing lessons learned for related efforts.
- The Texas Education Agency has included cyber curricula mandates at the high school level. An examination of educational curricula mandates throughout K-12 is required at the state and national levels to baseline current requirements. The Center for Infrastructure Assurance and Security (CIAS) at UTSA has partnered with MITRE to increase student engagement in the areas of technology and cybersecurity. The CIAS K-12 Cybersecurity Program has launched nationally to provide an innovative approach to creating a culture of cybersecurity for people of all ages. MITRE, in partnership with UTSA, the Cyber Texas Foundation, and San Antonio's Northside Independent School District, created after-school programs to introduce cybersecurity lexicon and concepts at the elementary school level.
- CyberTexas Foundation[29] organizes cyber workforce development initiatives supporting local, state, and national efforts. Example activities include CyberPatriot, a National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other STEM disciplines critical to the nation's future. San Antonio is a Center of Excellence for CyberPatriot.

---

[25] The Cyber Innovation and Research Consortium, powered by CyberTexas, comprises all San Antonio area universities and colleges. Specifically, the representatives are professors in the fields of cybersecurity, information technology, and computer science. Their goal is to integrate and amplify institutions' high-powered cybersecurity capacities into cohesive, academic superiority. More information is available at https://circsa.org/research/.

[26] MITRE @ San Antonio in Partnership with UTSA. 2020. MITRE, https://sites.mitre.org/san-antonio/wp-content/uploads/sites/24/2021/02/San_Antonio_Factsheet8-31-2020.pdf.

[27] Project Xander. 2022. MITRE, https://sites.mitre.org/san-antonio/wp-content/uploads/sites/24/2022/10/Project-Xander-Brochure.png. Last accessed October 31, 2022.

[28] Project Xander: Faith-Based and Non-Profits in Cyberspace. 2022. MITRE, https://sites.mitre.org/san-antonio/protecting-communities. Last accessed October 31, 2022.

[29] CyberTexas Foundation. 2022. CyberTexas Foundation, https://cybertexas.org/. Last accessed October 31, 2022.

Appendix A

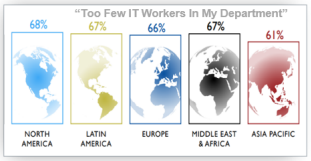
Cyber Workforce Development Framework Overview

August 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Background – Why Focus on Cyber Workforce?

- Virtually **every sector** of **every economy** is increasingly reliant on internet and communications technologies (ICT)—security of these systems and data is a key component of economic success
- In the early part of the 2010s, **ICT contributed more than 10% of total GDP growth** to countries like India
- In these countries, **companies with a robust internet presence grew twice as fast** as those relying on traditional brick and mortar establishments (McKinsey)
- By 2022, unfilled cybersecurity jobs are expected to top **3.5M vacancies worldwide**—a 350% increase over 2013

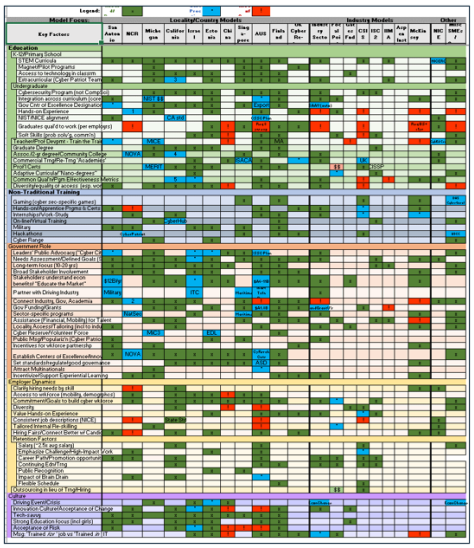


Frost & Sullivan, Executive Report, "2017 Global Information Security Workforce Study," (ISC)², Center for Cyber Safety & Education

- A recent year-long ISSA survey (2017) of security executives found 70% say **workforce shortages impact business**—45% have had at least one security event in the past year
- Current programs focused on **university degrees and certs are not aligned with employer needs**: according to the MIT Technology Review, fewer than 1 in 4 applicants for IT/cyber jobs are qualified

Organizations have invested in cybersecurity technologies, but not the people to use them

Our Workforce Development Framework Approach

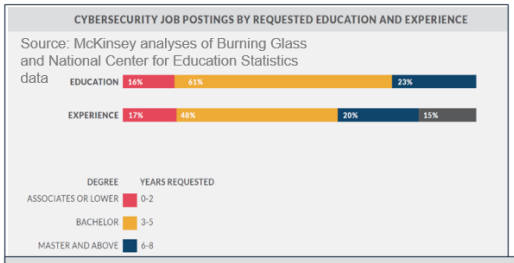


- **Broad survey of tech workforce development approaches**
  - Nations of various size, economy
  - US States with different economic bases
  - Development NGOs (World Bank, Gates Foundation)
  - Economic Experts (McKinsey, Aspen Institute)
  - Cybersecurity SMEs (ISC2, CSIS, NICE)
- **Identified commonalities, needs, and best practices in 5 categories:**
  - Traditional Education (K-12 and college/university)
  - Other Training/Education approaches
  - Employer Inputs
  - Government Role
  - Cultural Factors
- **Synthesized into Framework focused on key areas and approaches for building cyber workforce capacity**

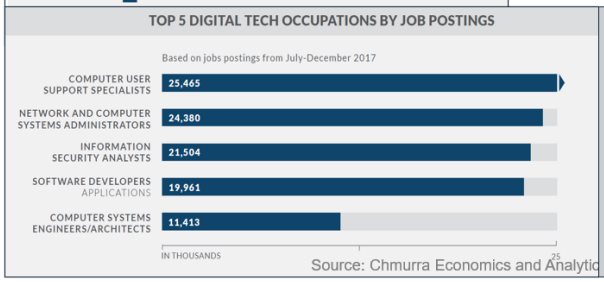
Who is this Framework For?

- **Developed from data representing various city, state, national, and sector economies around the world, as well as ideas from cybersecurity, education, and economics subject matter experts, it is intended to be applicable to a wide range of entities:**
  - **Nations** transitioning to a digital economy or adjusting incentives and pipelines to increase investment in and access to cyber professionals
  - **City, State, or Regional planning groups** focused on increasing high-tech employment and associated ecosystem
  - **Industry and academia** seeking to grow a local talent pool
  - **Government agencies** at all levels developing policy and/or legislation to incentivize cyber talent development and retention in key functional areas

Summary of Findings:
Misalignment in the Cyber Skills Markets and Training Paths



- Non-university educated job seekers are not aware of cyber/ICT job opportunities, and don't feel qualified
- Perceptions of tech as math-intensive, high qualification, and elite discourage potential applicants (esp. women)
- Employers do not have accurate assessments of their cyber-related needs, distorting training incentives
- Current paths focus on Universities and certs misses the vast need for practical "middle skills" training



Keys to developing a cyber workforce:

- Basic **K-12 education** that includes tech awareness
- **Public-private partnerships** to connect industry, government, and academia in developing programs
- Local, affordable, accessible **hands-on training** tailored to the needs of job seekers/employers
- **Common lexicon** (such as NICE) to identify, describe, and build to the specific Key Skill Areas (KSAs) actually needed in the workforce

Mis-alignment in Incentives

Demand Side:

- **The complexity of employer requirements means more than 50% of applicants are considered "unqualified," particularly in cyber-security (vs. IT) roles:**
  - **84%** of postings studied required a **bachelor's degree**
  - **83%** required at least **three years** of experience—more than **35% required certification**, with the top three desired certifications requiring a minimum of **five years** of experience
- **Cybersecurity practitioners represent a continuum of engineers, scientists, developers, operators, defenders, investigators, and analysts**
- **These roles do not require the same amount of education and training, but most employers post job qualifications as if they do**

Supply Side:

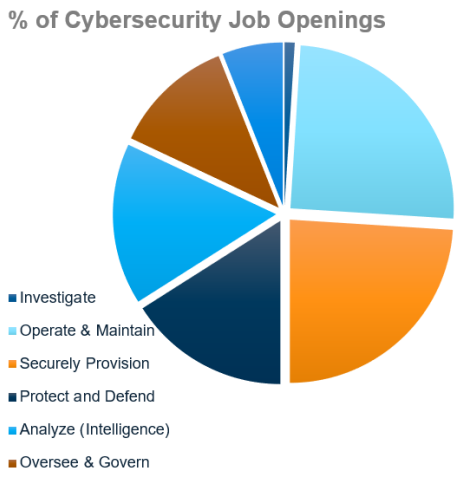
- **Lack of awareness: only 37% of students were advised about cybersecurity as a career**
- **Information about the cybersecurity career path is not easily discoverable or consumable**
- **Potential candidates don't understand the myriad cyber-related options or what could be possible for them with digital skills (particularly those who are focused on business rather than computers)**

Summary of Findings – Employers

- Employers feel current programs are not producing graduates with the right qualifications to meet their IT/cybersecurity needs
- At the same time, employers often specify experience (3-8 years) and education (BS in comp sci or network engineering) requirements that don't match actual job needs
- The skills needed by most employers are more easily and affordably attained through hands-on apprenticeships, internships, on-the-job-training, informal IT experience, and training programs focused on specific system administrator and help desk skills
- There are insufficient hands-on programs to produce the kind of experience desired by employers, despite growing need
- There is no common guideline to help employers—particularly those outside of ICT—identify skills-based needs, and what programs or experiences may meet those needs
- Providing these kinds of programs are ideal opportunities for public-private partnerships

Summary of Findings – Employers (Continued)

Open Jobs by NICE Category



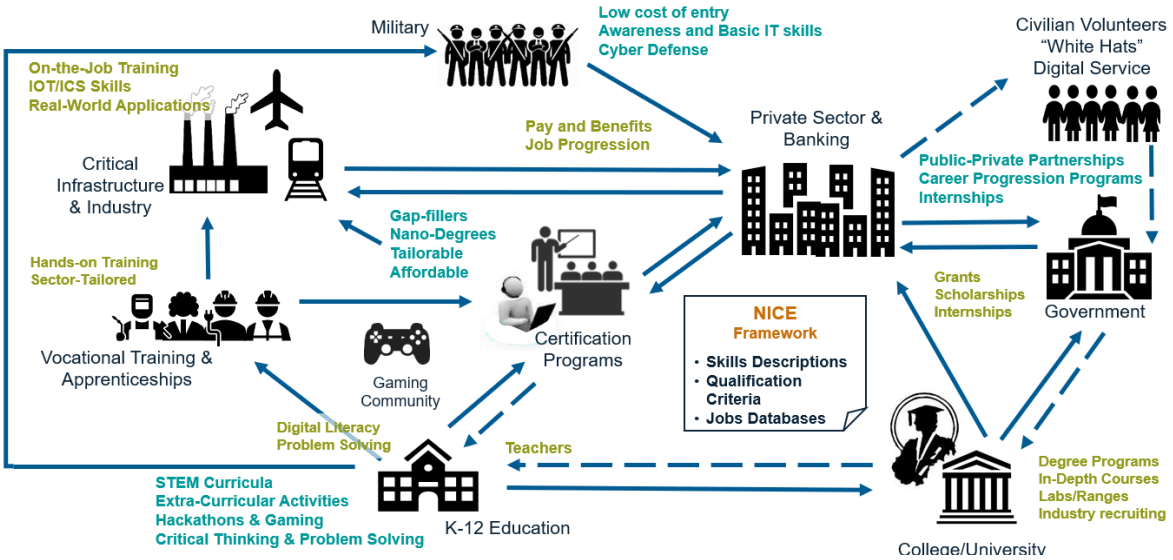
Source: The Aspen Institute, Aspen Cybersecurity Group

NICE Framework Categories	Role Description
Securely Provision	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system/network development
Operate & Maintain	Provides the support, administration, and maintenance necessary to ensure effective information technology (IT) system performance and security
Protect & Defend	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks
Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems and networks
Intelligence Analysis	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Oversee & Govern	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work
Collect Intelligence, Conduct Operations	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence

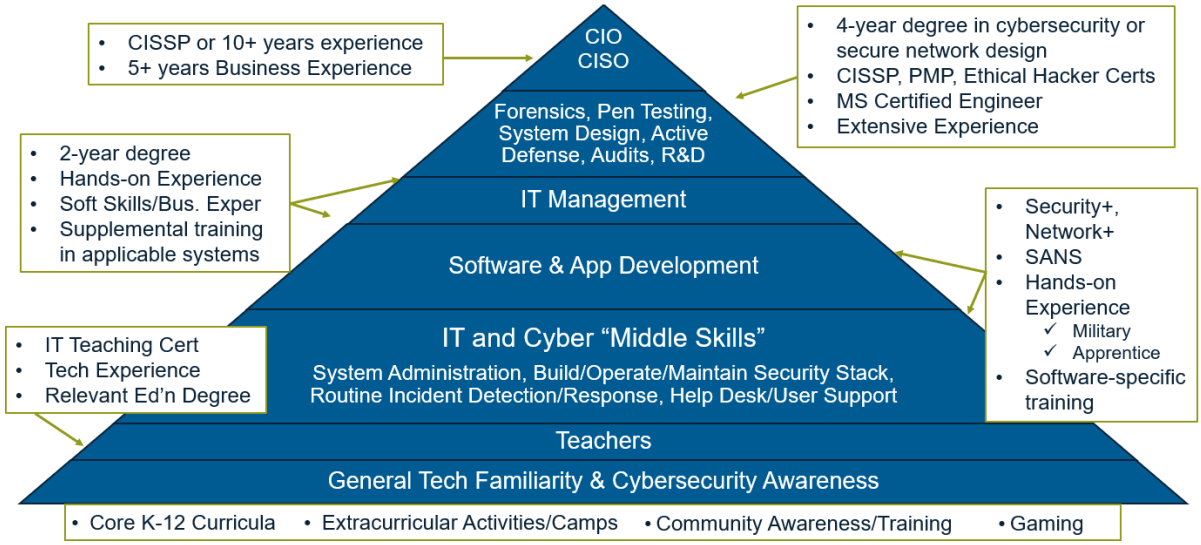
Most In-Demand Skills

Source: National Institute of Science and Technology (NIST) – NICE Framework

National Cyber Workforce Ecosystem

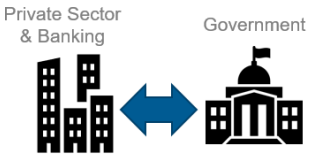


Notional Workforce Pyramid and Possible Qualifiers



Public-Private Partnerships are Key

- **Government is not enough**
  - Typically can't offer enough jobs, or enough pay, to drive training programs
  - Industry employers that exert major influence over a local economy are needed to create a strong enough jobs "demand signal"
- **Government and Industry can work together to:**
  - Create a National Needs Assessment - strategic workforce goals based on anticipated economic and security needs
  - Establish a common lexicon (such as NICE) to synchronize academia, employers, government, and job-seekers
  - Codify relevant standards for training program accreditation, tied to KSAs
  - Guide academia in producing qualified graduates for higher skill jobs



Government must work closely with technology innovators to "co-design governance frameworks."
- World Economic Forum

- **Government can provide:**
  - Improved access through grants, "Scholarships for Service," and accredited community college programs
  - Incentives for participation in worker exchange job progression programs (affordable talent for government)
  - Development of alternative experience paths, such as vocational programs, talent identification programs like hackathons and bug bounties, and nationally recognized apprenticeship accreditation programs
- **Employers can provide:**
  - Skills-based hiring requirements (rather than degree, cert, or years experience) that accurately reflect their needs
  - Good pay, on-the-job training and/or work-study experience, job progression, upskilling and reskilling opportunities

Summary of Findings – Government's Role

- **The government is usually best positioned to integrate the cyber ecosystem of industry, academia, cyber professionals, commercial training programs, and national security needs**
- **First step: Identify shortfalls and develop and publicize a long-range (10+ years) plan**
- **"Educate the Market" - Broaden understanding of the importance of cybersecurity skills to national security and economic growth across the national ecosystem**
- **Establish a common lexicon, such as NICE, that can help align jobs, candidates, and education/ training programs and facilitate skills-based training and hiring**
- **Convene academia, industry, and commercial training providers to develop standards that can guide training and education programs, help shape career paths, assure employers of qualifications**
- **Provide opportunity and incentive to cooperate across government and industry in career development and retention, including at the local level**
- **Eliminate barriers to cooperation and investment in training, and to competitive compensation for skilled employees**

Potential Public-Private Partnership Engagement Opportunities

- **Context Development**
  - Sector dependencies/Opportunities driving local cyber workforce needs
  - Employer/Government needs/goals and ongoing initiatives
  - Current Barriers and development path gaps
  - Regional issues (common industries, competing incentives, etc.)
- **Needs Assessment**
  - Gaps/Misalignments in current programs and incentives
  - Applying the NICE Framework to set standards, address gaps and align programs with needs
  - Educating the Market – getting industry and investors on board
- **Public-Private Partnership discussions**
  - Identify potential programs (K-12 through University, incl commercial/"academy" training) to meet employer needs
  - Establishing standards and appropriate certification pathways (with metrics)
  - Using NICE to standardize job descriptions across the ecosystem
  - Eliminating legislative and policy barriers and incentivizing change ("How Might We…?)
- **Implementation**
  - Developing Hands-on Training Programs
  - Developing government policy/legislation to facilitate workforce development
  - Best Practices in Public-Private Partnership execution

Appendix B

TAPPING THE K-16 EDUCATION PIPELINE TO GENERATE A TALENTED CYBER WORKFORCE

CHALLENGE

California's successful tech industry (exemplified by the famed Silicon Valley) has led to a voracious demand for cybersecurity jobs. While the state was proactive in developing opportunities for building a cyber workforce, by the middle of the past decade it found itself struggling to keep up with a growing gap of insufficiently trained labor.

To begin to reverse the trend, California needed to make a more concerted effort to narrow the cybersecurity workforce gap, implementing both short- and long-term solutions. State government, industry foundations and groups, and academic institutions needed to emphasize cyber in the K-16 education to train and build the skillsets of California's future labor force.

SOLUTION ELEMENTS

Support Partnerships
Academic institutions, government agencies, industry, and non-profits need to work together

Steward Talent
Encourage, support, and educate a wide range of students for cyber-careers throughout K-12, community and traditional college education

Industry Interest
Industry foundations and professional groups directly supported students and young professionals into cyber-careers

Maintain Oversight
Develop metrics and processes to measure progress and keep goals in sight

MITRE

CYBER WORKFORCE DEVELOPMENT **CASE STUDY: CALIFORNIA, USA**

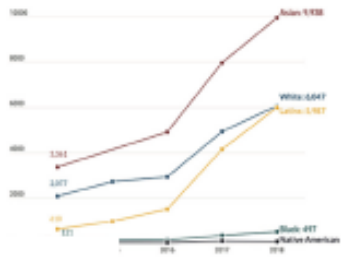
FINDINGS

Key Lessons from Califronia

- Identify leaders to support removing barriers for young adults and students.
- Find learning opportunities, even non-traditional ways, that spark interest with young students.
- Couple career path strategies with training programs for young adults.
- K-12 cybersecurity education should seamlessly transition into college- and then career-readiness.

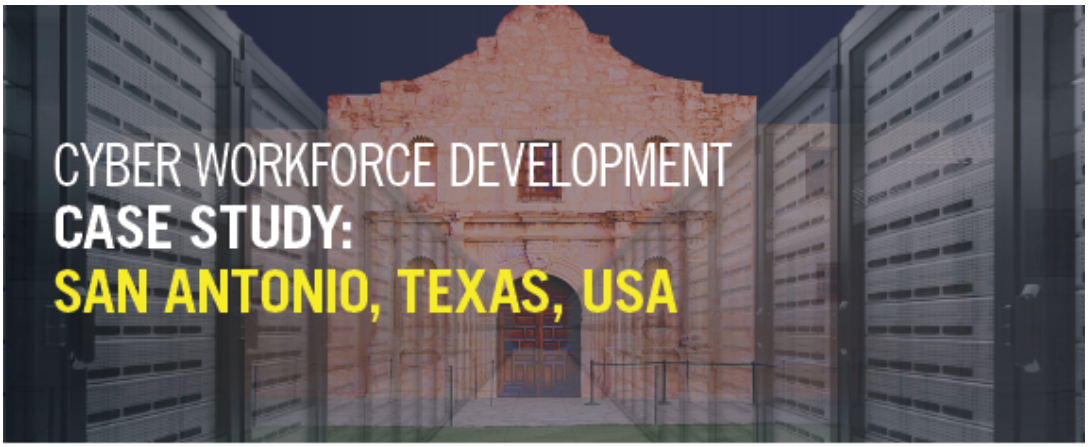
Information Security Degrees and Certifications Awarded
(State of California)

AP Computer Science Participation, by Race/Ethnicity
(2014-2018)



MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD



HOW A SERVICE-ORIENTED CITY BUILT A SUCCESSFUL CYBER WORKFORCE

CHALLENGE

During the 1990s, civil service employees at San Antonio area military bases worried about the changing labor market in an environment where current occupations were being offset by emerging technologies.

Then much of San Antonio's economy was based in service industries and regional government—offering wage rates well below national averages. Preserving their livelihood would require new industries with higher paying jobs–those supporting the growing cybersecurity focus of the remaining military bases.

With support from city and local leaders, this dedicated group sought to create "Cyber City, USA" by growing opportunities for cybersecurity employment and regional viability for cyber-related industry.

SOLUTION ELEMENTS

Lasting Partnerships

Lasting partnerships with regional academic institutions, government agencies (local, state, federal), local / national industry, non-profits, and trade associations.

Talent Pipeline

Working with primary, secondary, and higher education to put curriculum in place that can encourage, educate, and support interest in cyber-related careers.

Devoted Facilities

Dedicated facilities were built to support cyber workforce growth. This led to the formation of an emerging San Antonio tech corridor featuring a university-public-private collaboration facility.

Constant Messaging

Consistency in messaging reinforcing the purpose of San Antonio's efforts has been a key to the city's success.

MITRE

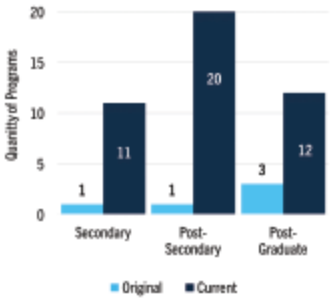
CYBER WORKFORCE DEVELOPMENT **CASE STUDY: SAN ANTONIO, TEXAS, USA**

FINDINGS

Key activities from San Antonio

- Determine a prominent industry focus as the rallying point.
- Identify leadership to ensure collaboration from leaders across industry, academia, and government.
- Identify sources for short-term and long-term investments.
- Incorporate a market strategy with consistent messaging and strong community engagement.

Growth in Academia Cyber Programs (2012 - 2020)



Cyber Workforce Increase (2012 - 2017) **and Growth Projection** (2017 - 2022)

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD