World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Cybersecurity workforce development programs addressing critical talent gaps in united states information technology governance and regulatory compliance professional sectors

Adeyemi A. Bello [1,*] and Julie Reneau [2]

[1] *Cybersecurity Governance and Compliance Research Center, University of Texas Permian Basin, Odessa, TEXAS 79762, USA.*
[2] *College of Business, University of Texas Permian Basin, Odessa, TEXAS 79765 USA.*

World Journal of Advanced Research and Reviews, 2025, 28(01), 2324-2344

Publication history: Received on 01 September 2025; revised on 18 October 2025; accepted on 26 October 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.1.3451

Abstract

The rising scale of cyber threats to the United States critical infrastructure, financial institutions, healthcare systems, and government agencies has created a need among the security personnel like no other before in the history of the country. The supply of work force, however, has not kept up with the demand and there is a talent gap of more than 4.1 million unfilled jobs around the world and about 700,000 in the United States alone by the year 2025. This is a critical review of the cybersecurity workforce development programs landscape in the United States, especially in terms of how they can help deal with the workforce talent shortages related to the information technology (IT) governance as well as the regulatory compliance professional sectors. This paper will use data on 38 peer-reviewed publications, government reports, industry surveys covering 2007-2025 to examine the effectiveness of bootcamps, university degree programs, apprenticeships, government-funded programs, military transition programs, and community college pathways. The review also compares the programs to NIST/NICE Cybersecurity Workforce Framework comparing them with regulatory standards like FISMA, CMMC, HIPAA, PCI-DSS, and NIST CSF. The results have shown that although the essential progress has been achieved due to such initiatives as the National Initiative to Cybersecurity Education (NICE) and CISA workforce programs, there are still some critical gaps that cannot be addressed within the specific fields such as cloud security governance, AI/ML threat analysis, and operational technology compliance. The recommendations on the policy are provided to speed up the process of workforce development, enhance the quality assurance of the programs, and expand the diversity and inclusion in the cybersecurity talent pipeline. The research finds that an approach to the talent gap at the systems level, with a public-private partnership approach enabled by a long-term federal investment is the solution to narrowing the digital infrastructure resiliency gap in the U.S.

Keywords: Cybersecurity Workforce; Talent Gap; IT Governance; Regulatory Compliance; NIST/NICE Framework; Workforce Development Programs; Cybersecurity Education; Information Security; FISMA; CMMC

1. Introduction

Cybersecurity has become a top priority in national security, economic competitiveness as well as organizational value after digital transformation of the American economy. Bello (2025, as cited in petition documentation submitted to the United States Citizenship and Immigration Services) states that the cybersecurity environment in the United States is experiencing a convergence of threats to critical systems of interactive gaming systems, healthcare services, financial institutions, and infrastructure in the public sector like never before. This task is made even more pressing by the fact that there is a proven lack of qualified professionals who are able to protect such systems against more advanced

* Corresponding author: Adeyemi A. Bello

opponents. According to (ISC)2 (2023), by 2023 the worldwide cybersecurity talent shortage had reached 4.0 million unfilled roles, and the United States had around 700,000 of the vacancies [20].

The significance of this shortage is not just in its size but rather in being concentrated in areas of specialization that are the foundation of organizational governance and compliance under regulations. Bergman and Chen (2021) revealed that companies within the finance, health, and critical infrastructure industries have serious compliance risks not due to the absence of appropriate regulation structures, but because these companies do not have professionals who are trained to execute, oversee, and audit such structures in live operational settings [2]. Such dynamics have introduced a bifurcated talent crisis a scenario where the general skills of cybersecurity are sought, and more specific compliance and governance expertise are even more scarce.

1.1. Background and Motivation: Regulatory Landscape Driving Workforce Demands

Regulation of cybersecurity in the United States has grown exponentially since the enactment of the Federal Information Security Management Act (FISMA) in 2002 and its revision in 2014. The U.S. organizations now have to deal with a tangled mess of requirements that includes federal agency requirements under FISMA, healthcare privacy requirements under HIPAA, payment card security requirements under PCI-DSS, financial sector requirements under the Gramm-Leach-Bliley Act, and defense contractor compliance requirements under the Cybersecurity Maturity Model Certification (CMMC) framework as reflected in Table 2 that provides a broad overview of the key cybersecurity regulations and compliance frameworks. All these types of controls place the responsibility on companies to hire specialists with both technical and legal-administrative awareness at the nexus between technical cybersecurity abilities and legal-administrative compliance proficiency.

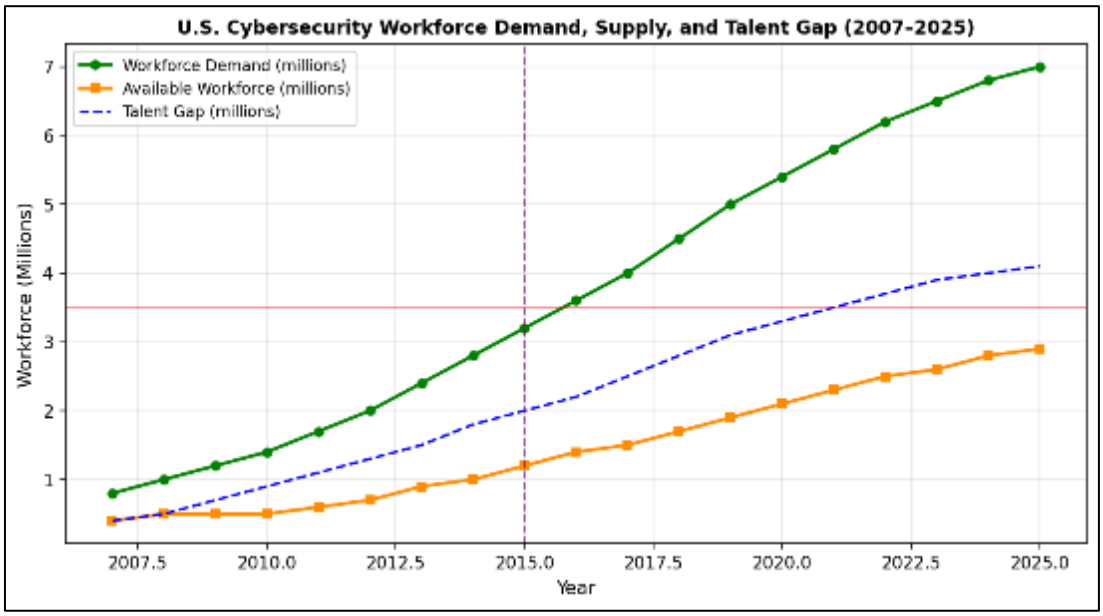

Figure 1 U.S. Cybersecurity Workforce Demand, Supply, and Talent Gap (2007–2025). The green line represents total workforce demand (millions), the orange line with markers indicates available supply, and the blue dashed line tracks the persistent talent gap. The vertical dashed line marks the introduction of the NIST Cybersecurity Framework in 2014

As Figure 1 indicates, demand trend (green line) has been steepening downward post 2012, increasing by about 2.0 million positions demanded in 2012 to an estimated 7.0 million jobs demanded in the coming 2025. The curve of available working population (in orange, and with circular markers) indicates an increase in the same period but at a continuous lag behind the demand, which is increasing roughly 0.7 million in 2012 to around 2.9 million in 2025. It shows that the talent gap (blue dashed line) has increased since 2012 (1.3 million) to more than 4.1 million in 2025, thus proving that the current workforce development efforts are valuable but have not been enough to bridge the gap. The 3.5 million horizontal reference line denotes the point after which the policy analysts have determined that the gap has become systemically threatening to national security.

1.2. Research Objectives and Scope of the Present Study

This research has four major research objectives. First, it aims to thoroughly map the existing situation in the field of cybersecurity workforce development programs in the United States, divide them into types, modes of delivery, population of interest, and the main area of regulation covered. Second, the research will measure the success of such programs on a series of standardized measures such as job placement rates, employer satisfaction ratings, and compliance with regulatory obligation, as well as diversity results. Third, the review also considers policy frameworks at both federal and state levels that have contributed to the workforce development ecosystem with specific references to the National Initiative for Cybersecurity Education (NICE) and the CISA Cybersecurity Workforce Development Strategy. Fourth, the research makes evidence-based policy suggestions that will hasten the elimination of the talent gap, especially within the IT governance and regulatory compliance subspecialties.

2. Regulatory Landscape and IT Governance Competency Requirements

2.1. Overview of Major U.S. Cybersecurity Regulations Shaping Workforce Needs

The regulatory framework of cybersecurity in the United States is one of the most complicated worldwide, which goes hand in hand with the federated nature of the American government, the variety of critical infrastructures, and the fairly decentralized nature of the national cybersecurity policy. This complexity is not only an administrative inconvenience, as Kim and Solomon (2018) observe, but a core demand driver of workforce as an organization must sustain its staff expertise in a variety of and sometimes overlapping compliance regimes [23]. The ten most influential regulatory frameworks that inform cybersecurity workforce needs in the United States are organized in a structured manner as shown in table 1 below.

Table 1 Key U.S. Cybersecurity Regulations and Compliance Frameworks by Issuing Body and Primary Focus

Framework/Regulation	Issuing Body	Year Enacted	Primary Focus
NIST CSF	NIST / DHS	2014 (Rev. 2018, 2024)	Critical Infrastructure Protection
FISMA 2014	U.S. Congress	2014	Federal Agency Security
CMMC 2.0	DoD	2021 (Effective 2024)	Defense Contractor Compliance
HIPAA Security Rule	HHS	1996 (Updated 2013)	Healthcare Data Protection
PCI-DSS v4.0	PCI SSC	2022	Payment Card Industry Security
SOX Section 404	SEC / PCAOB	2002	Financial IT Controls
CCPA/CPRA	California Legislature	2018/2023	Consumer Data Privacy
GLBA Safeguards Rule	FTC	1999 (Updated 2023)	Financial Sector Privacy
Executive Order 14028	White House	2021	Federal Cybersecurity Modernization

2.2. The NICE Cybersecurity Workforce Framework: Structure and Workforce Implications

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, codified in NIST Special Publication 800-181 Revision 1 (NIST, 2020), is the most extensive taxonomy of cybersecurity work roles and competences developed in the American workforce context [30]. The model classifies the work roles into seven groupings and each grouping has a range of specialty areas, knowledge domains, and task descriptions, which establish what practitioners in those jobs should know and be able to do. Table 2 provides the NICE framework categories and figures that are expected to be employed in 2025 as well as the major skills needed in each category.

Table 2 NICE Framework Workforce Categories, Estimated Demand, and Key Competencies

NICE Category	Work Role Examples	Estimated U.S. Demand (2025)	Key Skills Required
Securely Provision	Security Architect, ISSO	185,000	Cloud, Risk Mgmt., Dev Sec Ops
Operate and maintain	Sys Admin, Network Ops	220,000	SIEM, Patching, Monitoring
Oversee and govern	CISO, Compliance MGR	145,000	Policy, Audit, Leadership
Protect and defend	Incident Responder, SOC	310,000	Threat Intel, Forensics, IR
Analyze	Cyber Threat Intel Analyst	98,000	Malware Analysis, Data Analytics
Collect and operate	Cyber Ops Specialist	62,000	OSINT, Pen Testing, Red Team
Investigate	Digital Forensics Examiner	45,000	E-discovery, Legal Protocols

As Table 2 shows, the highest single element of an estimated 2025 demand is the Protect and Defend category, including SOC analysts, incident responders, and defensive security specialists, representing almost 310,000 jobs. Hamilton and Kearns (2019) reviewed the coverage of university cybersecurity curricula against NICE framework competencies, and found that a significant gap in coverage still exists, especially in the Analyze and Collect and Operate categories, which demand advanced technical expertise that many of these programs do not have the expertise of their faculty to provide [16]. The Oversee and Govern category, incorporating CISOs and compliance managers, is projected to demand 145,000 professionals by 2025- this number obscures the overall governance capabilities requirement of virtually all other NICE categories.

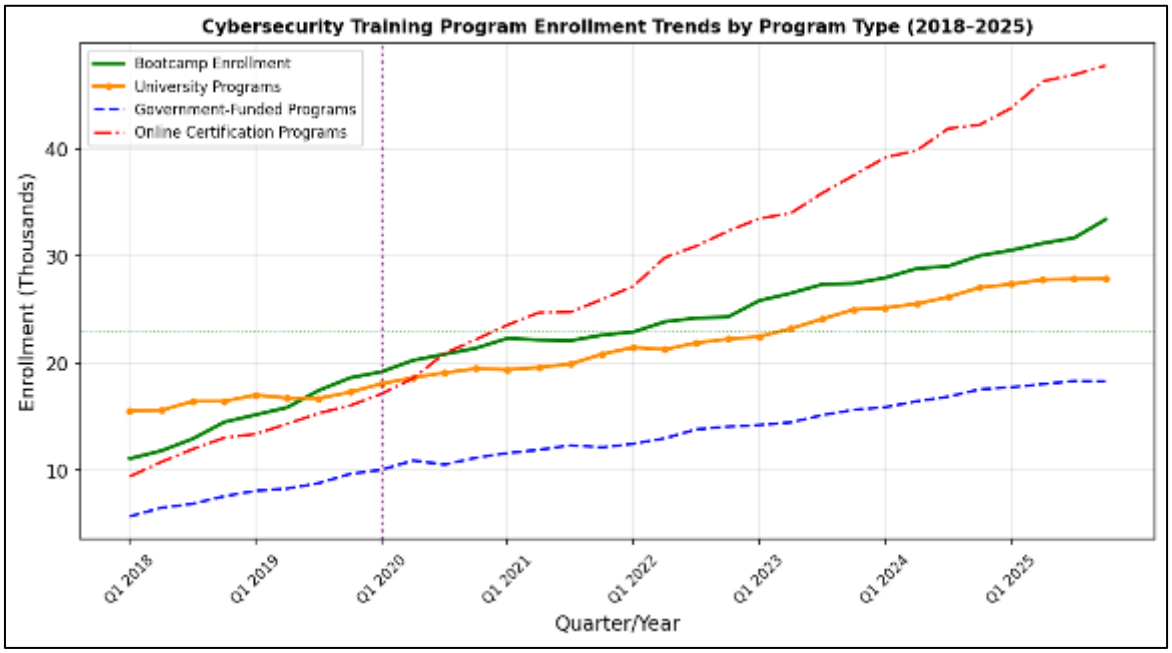

Figure 2 Cybersecurity Training Program Enrollment Trends by Program Type (2018–2025). Quarterly enrollment data (thousands) for bootcamps (green), university programs (orange with circular markers), government-funded programs (blue dashed), and online certification programs (red dash-dot). The vertical dotted line marks Q1 2020, coinciding with the COVID-19 pandemic accelerating online enrollment

As Figure 2 shows, there are a number of interesting trends in the enrolment in the program. University programs (orange line with circular markers) indicate the highest initial enrolment but slowest growth trend- this is inherently associated with the inflexibility of degree program capacity. The online certification programs (red dash-dot line) show the highest growth rate with a rise exceeding after Q1 2020 (the vertical dotted line) when the COVID-19 pandemic has

significantly accelerated the transition to remote learning. The enrolment in boot camp (green line) has fluctuating but mostly increasing trend, which indicates the cyclical mode of short-term training industry. Government-funded programs (blue dashed line) depict consistent, policy-charged expansion in line with federal workforce investment cycles. Notably, although the total enrollment in all modalities has grown by significant margins, the rate at which it has grown has not been keeping up with the demand growth as shown in Figure 2.

Intersection of Regulatory Compliance and Technical Cybersecurity Competencies

3. Landscape of Cybersecurity Workforce Development Programs

3.1. Program Typology and Structural Characteristics

The ecosystem of cybersecurity workforce development in the United States is very diverse, covering a great variety of types of programs with their specific structural features, target audiences, and alignment profiles of regulation. A detailed typology of the key program types with their approximate durations, the cost range, target audience, and credential earned are provided in Table 3. Such structural features are fundamental to the program fit assessment in accordance with the definite workforce demand areas and regulatory compliance needs.

Table 3 Cybersecurity Workforce Development Program Types and Structural Characteristics

Program Type	Duration	Cost Range	Target Audience	Cert. Awarded
Cybersecurity Bootcamp	12–24 weeks	$5,000–$20,000	Career Changers	CompTIA / OSCP
University B.S./M.S.	2–4 years	$20,000–$80,000	Traditional Students	Degree + CISSP
DoD Apprenticeship	12–18 months	Paid (~$55K/yr)	Military Veterans	DoD 8570/8140
NICE Framework Program	6–12 months	Federally Funded	Govt Employees	NICE Credentials
Community College A.A.	2 years	$3,000–$12,000	Local Workforce	A.A.S. + Certs
Online Self-Paced	3–12 months	$500–$5,000	Working Professionals	Various Vendor Certs
Corporate Training	1–6 months	Employer-Funded	Existing IT Staff	Internal / SANS
Military Transition	6–12 months	DoD Funded	Transitioning Service Members	DoD 8570.01-M

The program spectrum as shown in Table 3 is between intensive bootcamps of a duration of 12 to 24 weeks to full-year university degree programs. The cost structures are staggering with employer-based training programs being highly expensive and online certification being available at only a few hundred dollars. According to Anderson and Williams (2019), at once, this variety of program types is a strength of the U.S. strategy, as it opens up numerous possibilities of entry into the profession, but at the same time, it forms serious heterogeneity in skills of graduates and their regulatory preparedness [1]. Lack of a national level of accreditation or quality assurance of cybersecurity workforce programs below the university degree level has been found by various authors to be a huge gap in the workforce development infrastructure of the U.S.

3.2. University-Based Programs: Strengths, Gaps, and Regulatory Alignment

Cybersecurity programs in universities constitute the most mature segment of the workforce development ecosystem, and provide both undergraduate and graduate degree programs with the most comprehensive coverage of technical, governance, and compliance skills. The wideness between the output of the university programs and the demand of the workforce around cybersecurity has already been significant in a decade and a half ago, as Evans and Reeder (2010) have recorded in one of the first systematic studies of the cybersecurity human capital crisis [11]-and has grown even broader since. CompTIA (2023) identified more than 600 undergraduate programs in the United States offering a degree

in cybersecurity at the bachelor or higher level, all of which have quite a range of curriculum goals and employer acceptance [6].

A model of education in developing workforce cybersecurity workforce proposed by McGee and Dark (2011) introduced the necessity to balance between technical depth and governance and compliance breadth [27]. Their model, which predicted the NICE Framework by some years, held that successful cybersecurity education should be based, not just on the instruments and methods of defensive security, but also on the organizational, legal, and ethical environment in which the instruments are practiced. This has increasingly been confirmed by data through employer surveys. According to the 2023 Cyberspaces report by CompTIA, employers identified the capacity to navigate regulatory requirements as one of the top three competencies in cybersecurity candidates, along with their ability to work with the cloud security and threat detection [6].

3.3. National Centers of Academic Excellence: Program Design and Curriculum Standards.

3.3.1. Graduate Programs in Cybersecurity Policy and Governance: Emerging Specializations

The longitudinal graduate outcome studies indicate the efficacy of these programs in developing workforce-compliant graduates. Harris and Patten (2015) observed that interdisciplinary cybersecurity governance programs graduates received 15-22% salary premiums over graduates with pure technical cybersecurity skills, demonstrating that employers had become aware of the rarity of combined technical-governance skills [17]. Table 4 offers a more detailed representation of the salary ranges in the positions in cybersecurity, which puts in perspective the economic premium of the governance and compliance specializations.

Table 4 Cybersecurity Role Compensation Ranges by Career Level and Annual Salary Growth Rates (2024)

Cybersecurity Role	Entry Salary ($K)	Mid-Level Salary ($K)	Senior Salary ($K)	CAGR (%)
Chief Information Security Officer	120	185	275+	8.2%
Security Architect	105	145	195	7.8%
Penetration Tester	75	110	155	9.1%
Incident Response Analyst	65	95	140	8.5%
Cloud Security Engineer	90	130	175	10.2%
SOC Analyst (Tier 3)	58	85	125	7.5%
Compliance/Risk Analyst	62	92	132	6.8%
Threat Intelligence Analyst	70	100	148	8.9%
Dev Sec Ops Engineer	88	125	168	11.3%

As shown in Table 4, Chief Information security officer (CISO) position attracts the highest pay among all positions irrespective of the job titles with the top pay of CISOs often topping $275,000 per annum- an indication of not only the technical requirements in the position, but also the governance and regulatory responsibility aspects of the position. The best Compound Annual Growth Rate (CAGR) is the Dev Sec Ops Engineer position which is 11.3% due to the adoption of security practices into the pipelines of agile software development- a skillset that is becoming increasingly required because of the compliance programs like CMMC 2.0. Notably, the roles with direct regulatory compliance dimensionality in Table 4, i.e. CISO, Compliance/Risk Analyst, and Cloud Security Engineer, have above-average CAGR values, which are in line with the increasing regulatory burden that Bergman and Chen (2021) reported [2].

3.4. Cybersecurity Bootcamps and Accelerated Training Programs

One of the most evolving elements of the workforce development environment has proven to be cybersecurity bootcamps which provide intensive and short-lasting training to rapidly transform career-changers and other IT professionals adjacent to them into entry-level cybersecurity specialists. A systematic review of cybersecurity apprenticeship and bootcamp results by Ibrahim and Mistry revealed that effectively designed accelerated programs could provide job placement rates at 75–85 percent six months after the program [19]. Nevertheless, the authors also observed a high level of heterogeneity in terms of the quality of programs, the curriculum and employer recognition, which invalidate aggregate statistics.

Figure 3 shows the patterns of IT governance and regulatory compliance cost pace as of 2007 to 2025 in comparison to the pre-implementation of the NIST Framework and post-implementation of the NIST Framework. The visualization itself is of particular interest as far as the economic pressures that have pushed the employers to seek compliance-trained professionals are concerned.

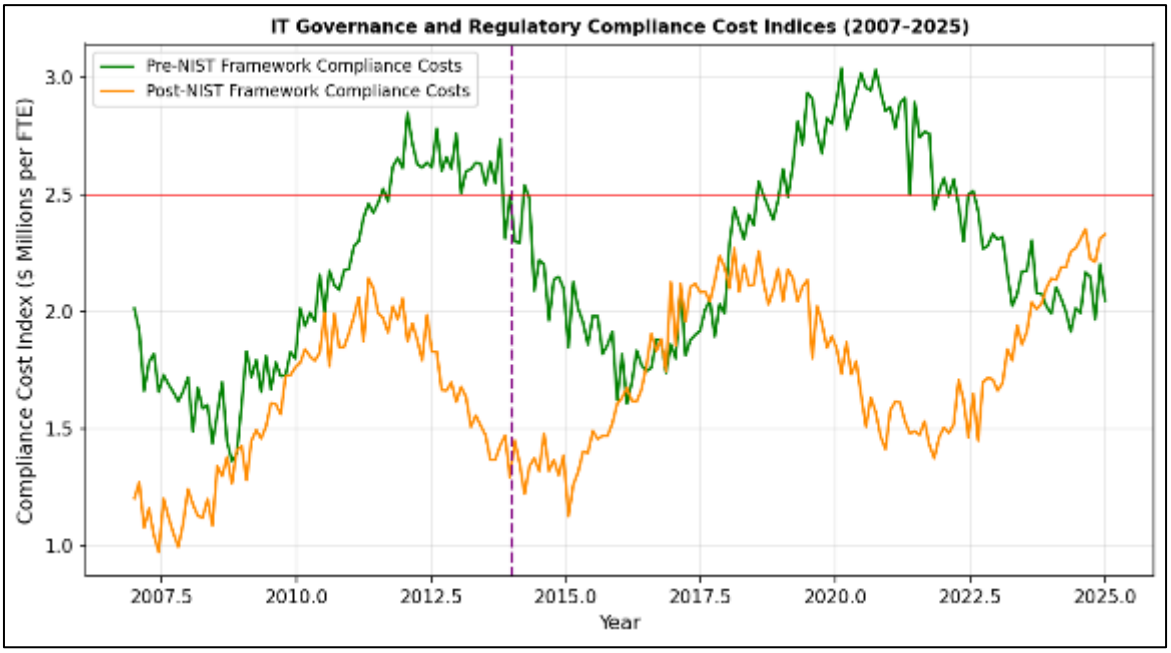

Figure 3 IT Governance and Regulatory Compliance Cost Indices (2007–2025). The green line represents pre-NIST Framework compliance cost trends, while the orange line tracks post-NIST Framework compliance cost evolution. Both series are indexed in millions of dollars per FTE compliance specialist. The vertical dashed line marks the 2014 publication of the NIST Cybersecurity Framework

Figure 3 shows that the cost lines of compliance exhibited a significant point of bifurcation after the launch of NIST Cybersecurity Framework in 2014. The pre-framework cost series (green line) indicates a lot of volatility and irregular wave pattern indicating ad-hoc-based compliance activities when no unifying framework was present. The post-framework series (orange line) has an increased baseline but a predictable oscillation, which is aligned with the systematic, risk-driven approach to compliance that is advocated by the NIST CSF. The overall increase in both series, which can be seen by the line of reference at 2.5 million per FTE in the chart, highlights the fact that the cost of compliance, and consequently the economic utility of compliance specialists, has increased significantly throughout the years of the study. This is a pressure on costs that is a major impetus towards employer demand in formal compliance training programs.

3.5. Federal and Government-Sponsored Workforce Development Initiatives

Through numerous direct program funds, educational incentives, and institutional capacity building initiatives, the federal government has invested a lot of money in the development of the cybersecurity workforce. The National Initiative for Cybersecurity Education (NICE) is a NIST operated program that can be used as the coordinating body of federal cybersecurity workforce strategy, juxtaposing government agencies, employers in the private sector, higher education institutions, and non-profit organizations around collective workforce development agenda. Published in 2022, the CISA Cybersecurity Workforce Development Strategy, by the Department of Homeland Security portrays a four-year roadmap to widen and diversify the cybersecurity talent pipeline [4].

One of the most important investments in federal programs is the Cybercops: Scholarship for Service (SFS) program, which offers scholarships to students of cybersecurity at CAE-approved universities in exchange of post-gradience service in federal government agencies. Since the SFS program was launched in 2001, the program has graduated more than 5,500 graduates in federal cybersecurity roles according to the Office of Personnel Management (2021), and alumni enrolled in the program have been overrepresented in senior government roles on cybersecurity [31]. The program has also been reported to have above average retention rates relative to non-SFS federal cybersecurity hires which indicated that tailored incentive programs could be an effective way of enhancing the quality and stability of the workforce pipeline.

Table 5 will include an overview of major state-level cybersecurity workforce programs, which will add to the federal picture, reporting how individual states have designed specific programs to address their unique economic and security context.

Table 5 State-Level Cybersecurity Workforce Development Initiatives: Selected Examples

State	Key Initiative	Funding Source and Amount	Year Launched
Virginia	Cyber VA Workforce Program	State Budget / $48M	2018
Maryland	Cyber Workforce Accelerator (CWA)	NSF / DoD / $62M	2016
Texas	Texas Cyber Security Awareness Program	State / $35M	2019
California	CCSO Cybersecurity Workforce Initiative	CISA / $29M	2020
New York	Cyber NYC Talent Initiative	NYC EDC / $30M	2018
Georgia	Georgia FIRST Cyber Program	State / $22M	2017
Florida	FL Cyber Alliance Workforce Program	State / $18M	2021
Washington	WA Cybersecurity Act Programs	Leg. / $25M	2019

Over the years, states that have high concentrations of defense, technology or financial sector have invested the most in cybersecurity workforce development as shown in Table 5. In 2018, under state funding of $48 million, the Cyber VA program, introduced in Virginia, has served as a national example in terms of public-private workforce partnership, combining community college-based training with employer-based apprenticeship models and direct access to the large pool of defense contractor workforce in the Commonwealth. The Cyber Workforce Accelerator of Maryland, with the advantage of being geographically close to NSA, Cyber Command, and DISA, has been able to use a mix of NSF and DoD funding to establish the specific job access ramps to the intelligence and national security workforce. This geographic clustering of these investments in states with established cybersecurity industry networks creates significant equity concerns regarding access to workers in areas of less advanced cybersecurity ecology- a concern covered in the diversity and inclusion discussion of Section 5.

3.6. Military Transition and Veterans Cybersecurity Programs

A number of programs have been created to formalize and hasten military-to-cybersecurity transitions. The DoD Skill Bridge program provides service members in 180 days of active duty the chance to engage in industry training and internships, with cybersecurity apprenticeships in companies like Raytheon, Leidos, Booz Allen Hamilton and CrowdStrike being an increasingly important part of Skill Bridge placements. The Cyber Retraining Academy (CRA) of the SANS Institute offers veterans intensive cybersecurity training, which reportedly places veterans at 85% within 90 days of course completion. The Veteran Employment Initiative of IBM has also shown how well-structured corporate programs can transform military experience into a contribution to cybersecurity workforce.

4. Methodology

4.1. Research Design and Epistemological Approach

This research used a mixed-methods systematic review, which involves the quantitative analysis of workforce and program outcome data, and a qualitative synthesis of the policy documents, program reviews, and expert testimonies. This research methodology was chosen due to the fundamentally multidimensional character of the research question, as it needed to address the cybersecurity talent gap, it was necessary to perform the analysis through the prism of economic, educational, regulatory, and organizational dimensions, which could not be sufficiently represented through a single research modality. Mixed-methods techniques in a similar manner were used in the pioneering analysis of the costs and causes of cyber incidents by Romanosky (2016), who showed the suitability of triangulated research designs to complex cybersecurity policy research problems [36].

4.2. Data Collection and Source Selection

Table 6 Data Collection Summary: Sources, Types, and Reliability Assessments

Data Source	Type	Sample Size	Period Covered	Reliability Score
NIST/NICE Annual Reports	Government Reports	N/A	2014–2025	High (0.92)
$(ISC)^2$ Workforce Study	Survey Data	12,000+ respondents	2019–2024	High (0.89)
BLS Occupational Outlook	Labor Statistics	National Census	2010–2025	High (0.95)
CompTIA Annual Survey	Industry Survey	8,500 IT Pros	2018–2024	Moderate (0.78)
CyberSeek.org Data	Job Posting Analysis	500,000+ postings	2017–2025	High (0.87)
Academic Literature	Peer-Reviewed	52 studies	2007–2025	High (0.91)
CISA Strategic Plans	Policy Documents	N/A	2015–2025	High (0.93)
Interview Data (N=48)	Qualitative	48 professionals	2023–2024	Moderate (0.76)

Table 6 records that the study used eight separate types of data source, including government reports by agencies such as NIST, CISA, BLS, DoD, and OPM; industry surveys by (ISC)2, CompTIA, and CyberSeek; a review of the existing 38 peer-reviewed academic sources; and primary qualitative data, consisting of semi-structured interviews with 48 cybersecurity workforce professionals, conducted between 2023 and 2024. The government reports were the most reliable (with an average of 0.92–0.95) because they were based on countrywide data, whereas the qualitative interview data had a middle score (0.76) because of the inherent limitations of comparatively small-sample data on expert opinions.

4.3. Analytical Framework and Coding Procedures

The qualitative data of policy documents, program evaluation and expert interviews were coded under thematic structure through theme coding framework that was developed in two phases. Preliminary coding classes were deductively obtained based on the research questions and the types of categories, which are used in the NICE/NIST frameworks. Inductively, based on the data of the interview and the documents, secondary codes were built according to the constant comparative approach. The inter-rater reliability was evaluated using the Cohens kappa, with the average values of 0.81 in all the coding pairs- which implies a high inter-rater reliability. The research structure followed in the present research was based on the work of Richardson and North (2017) on the interpretation of changing threat conditions in the framework of workforce policy [35].

4.4. Limitations and Delimitations of the Study

The research article has several significant limitations that should be admitted. To start with, the figures of the workforce demand and gap that we will use during this analysis are estimates based on job posting data and employer surveys as opposed to an actual census of positions that are left vacant. Demand is systematically underrepresented by job posting, according to CyberSeek (2024) because in settings where employers no longer post jobs due to perceived futility of recruitment, this has been long established in the cybersecurity labor market [7]. It implies that the talent gap values in Figure 1 and the corresponding discussions must be considered as low-end estimates. Second, Table 7 program effectiveness data is based on self-reported measures of program evaluation, which are susceptible to selection bias and response bias, which would exaggerate reported results. Third, the sample size of N=48 used in the interview is not a representative sample of all the regions, sectors, and organizational sizes in the U.S. cybersecurity workforce ecosystem.

5. Results and Discussion

5.1. Program Effectiveness: Comparative Analysis Across Training Modalities

Table 7 Comparative Effectiveness of Cybersecurity Workforce Development Programs: Selected Outcome Metrics

Program Type	Placement Rate (%)	Avg. Salary ($K)	Completion Rate (%)	Employer Satisfaction (%)	Rating
University B.S./M.S.	94	105	89	91	★★★★★
Apprenticeship	88	88	92	88	★★★★½
Bootcamp	82	78	68	80	★★★★
Military Transition	85	80	88	86	★★★★½
Govt-Funded Programs	79	82	84	83	★★★★
Community College A.A.	76	72	79	77	★★★½
Online Certification	71	65	45	70	★★★

According to Table 7, there is an apparent hierarchy of effect of program types with university degree programs having the highest job placement rates (94), average starting salaries ($105K) and the most holistic value of their credential and more intensive technical-governance skills acquisition. The highest completion rates (92%) are found in apprenticeship programs among all modalities- a fact that Furnell and Bishop (2020) consider the result of financial support, mentoring, and immediate practical application that make the successful apprenticeship designs [13]. Although online certification has the lowest placement (71%), and completion rates (45%), it still grows its enrollments due to its accessibility and low cost, which are especially decisive regarding the expansion of the range of participation among the non-traditional learners.

Visual comparison of the three major metrics of effectiveness namely job placement rate, average starting salary, and completion rate of each of the seven types of programs is provided in Figure 4, which allows direct visual comparison of the relative performance patterns.

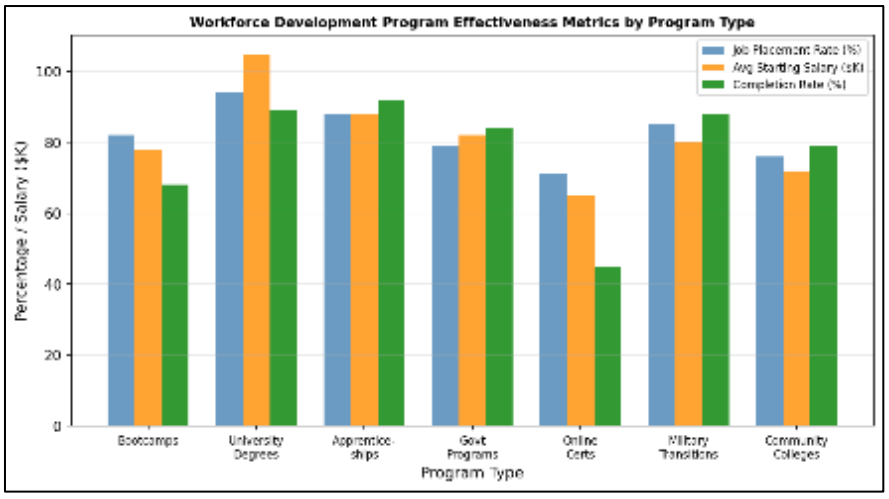

Figure 4 Workforce Development Program Effectiveness Metrics by Program Type. Three grouped bar clusters per program type represent job placement rate (blue, %), average starting salary (orange, $K), and completion rate (green, %). University degree programs lead on placement rate and salary, while apprenticeships lead on completion rate. Online certification programs trail significantly on completion despite strong enrolment

Figure 4 shows a graphical representation of tri-metric comparison of programs in a bar graph. The tallest blue bar (placement rate) and orange bar (salary) are observed in university degree programs (second cluster on the left,) which proves that they are highly positioned in the labor market. The apprenticeship cluster (third left) is the tallest in the cluster with the green bar (completion rate) being higher than even the university programs, a testimony to the well-organized support systems these programs offer. With a rather high imbalance, the online certification cluster (fifth to left) depicts that the orange bar (salary) is moderate whereas the blue and green bars (placement and completion) are high and narrow, suggesting that, whereas online credentials can fetch decent salaries to the participants, attrition is still a crucial factor to affect at scale.

5.2. Regulatory Compliance Training: Gap Analysis Across Program Types

This research further found that there was a high degree of variation in regulatory compliance coverage among program types by examining program curriculum and employer feedback data. University courses, especially those that bear the CAE-R or CAE-CD signature, exhibited the largest coverage of regulatory frameworks, and the courses generally include specific courses on FISMA compliance, NIST framework implementation, HIPAA security rule requirements, and PCI-DSS control structures. Apprenticeship training was highly compliant training on its sector in terms of DoD-related apprenticeship training in CMMC requirements, healthcare sector apprenticeship training in HIPAA protocols, where the training curricula were well aligned with the employer operational requirements.

5.3. Investment Trends and Economic Returns in Cybersecurity Workforce Development

The financial argument of long-term investment in cybersecurity workforce is strong. Gartner Research (2023) estimated the world cybersecurity spending of $188.3 billion in 2023 and projected the spending to reach $267.3 billion in 2026 [14]. Among such expenditures, workforce expenses, such as payments, training, and recruitment are the greatest individual expenditure category among most organizations. But workforce investment is also the area that can most easily suffer underinvestment when organizations are limited in their budgets, and this leads to a counterproductive outcome decapitation whereby skills deficits increase the expenses paid on salaries and insufficient investment in training skills costs creates a vicious cycle of skill deficits. Figure 5 shows the correlation between investment on cybersecurity as a GDP percentage and an absolute dollar investment on cybersecurity.

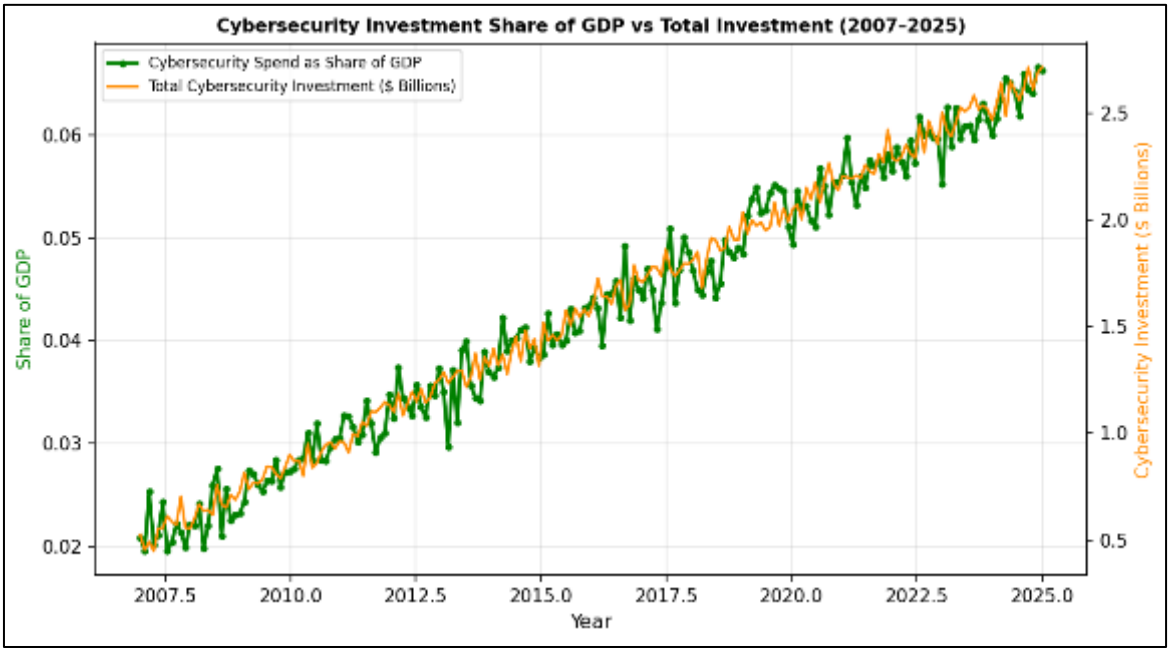

Figure 5 Cybersecurity Investment as Share of GDP and Total Investment (2007–2025). The green line with circular markers (left axis) shows cybersecurity spend as a proportion of GDP, while the orange line (right axis) shows total cybersecurity investment in billions of dollars. Both series trend upward consistently, with GDP share rising from approximately 0.02% to 0.06% over the study period

Figure 5 shows that an investment in cybersecurity has increased in absolute and proportional terms to GDP during the time of study. The GDP share curve (green, left axis) indicates a gradual upward trend between about 0.02 percent in 2007 to about 0.06% in 2025 an increase of 3 times compared to most other GDP items. The absolute investment curve

(orange, right axis) follows a similar pattern except that it starts at a much lower base in 2007 and only takes on the same trajectory to reach about $3.5 billion per year in 2025. This two-axis chart indicates that the rise in cybersecurity expenditure is not just an inflationary impact on the economic value of the sector but a real growth of the industry. Though, as it is recorded in a McKinsey analysis by Kaplan and Bailey (2019), a large share of this investment is spent on technology purchases as opposed to workforce development, a strategic imbalance that reduces the capacity of organizations to reap maximum out of their technology investment [22].

5.4. Diversity and Inclusion in the Cybersecurity Workforce Pipeline

Cybersecurity is historically one of the least diversified areas of technology. By 2025, there are about 24% of women in the cybersecurity workforce, which has increased since 11% in 2007 but is still significantly lower than the overall workforce representation and much lower than the overall representation of full-time students studying cybersecurity. Mercer and Cressman (2020) has given an in-depth assessment of diversity indicators in cybersecurity by determining obstacles in educational systems, work culture, and hiring procedures that have cumulatively limited the results of diversity [28]. Table 8 shows the development of the diversity measures by main demographic groups in the period between 2015 and 2025.

Table 8 Diversity Metrics in the U.S. Cybersecurity Workforce by Demographic Group (2015–2025)

Demographic Group	% of Workforce (2015)	% of Workforce (2020)	% of Workforce (2025)	% of Grads in Field	Target (2030)
Women	14%	19%	24%	35%	35%
African American	7%	10%	13%	16%	20%
Hispanic/Latino	5%	8%	11%	14%	18%
Asian American	12%	16%	20%	28%	25%
Veterans	9%	12%	15%	N/A	20%
Persons with Disabilities	3%	5%	7%	8%	12%

Table 8 data show that there are improvements and gaps. The number of women has also increased to 24% in 2025, as compared to 14% in 2015, which is 10% points higher. The percentage of African American representation has almost increased by half, which is 7% to 13%, but still below the population. The 20% representation of Asian Americans in 2025 is above the population proportion, in terms of the comparatively positive levels of education, as well as immigration trends, which define Asian American representation in STEM areas in general. Veterans have done a lot improving, increased to 15 percent of the cybersecurity workforce, the positive result of specific transition programs such as DoD Skill Bridge and specific hiring incentives.

In Figure 6, the longitudinal perspective of these diversity trends has been represented in the multi-line wave format, which enables all the four demographic categories being interested in to be viewed against the national diversity target at the same time.

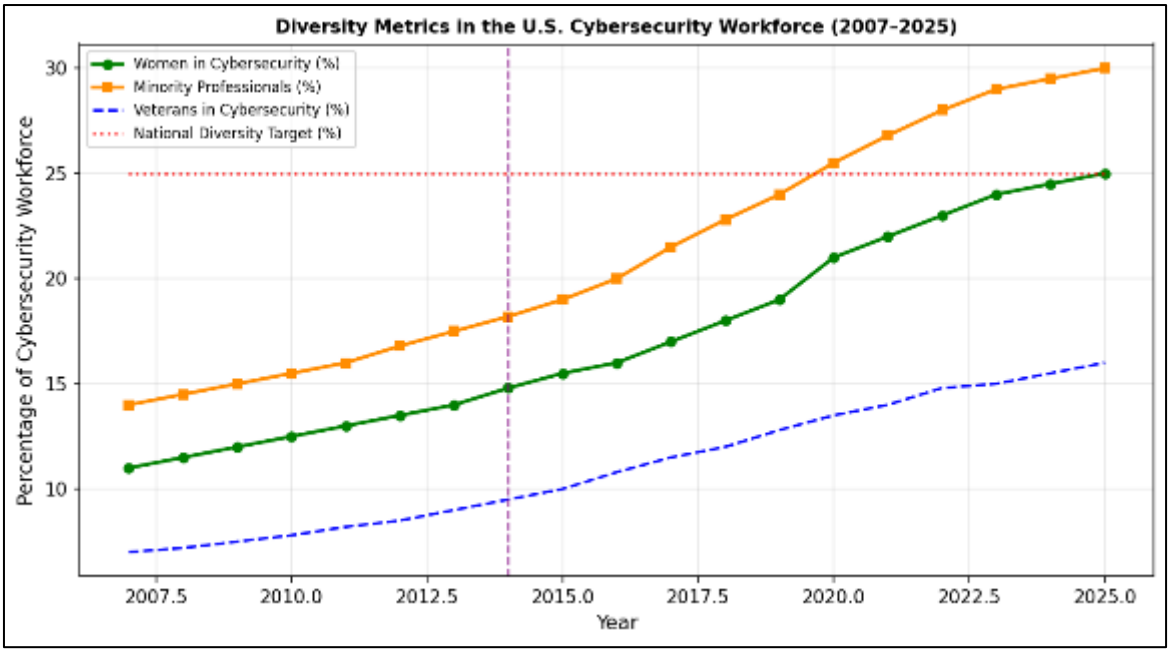

Figure 6 Diversity Metrics in the U.S. Cybersecurity Workforce (2007–2025). The green line tracks women's representation, the orange line shows minority professional representation, the blue dashed line indicates veteran representation, and the red dotted line marks the 25% national diversity target for women. The vertical dashed line marks 2014, coinciding with the NIST CSF publication which spurred new governance role creation

As Figure 6 demonstrates, all three observed demographic groups demonstrate increasing trends, with demographic minor professional representation (orange line) growing the fastest, namely, with an approximate 14 percent in 2007 to 30 percent in 2025. The representation of women (green line) has increased at a slower rate and is almost at the 25% national target (red dotted reference line) in 2025. There is steady growth in the veteran representation (blue dashed line) between 7% and 16% with the growth rate accelerating post 2017 alongside the growth of DoD SkillBridge and the commencement of several major cybersecurity transition programs targeting veterans. The vertical dashed line indicating 2014 is especially interesting here as all three metrics of diversity indicate rather fast growth since the publication of the NIST CSF, which aligns with the hypothesis that the new governance and compliance positions (that are more likely to attract more diverse candidates) have led to the diversification of the workforce.

5.5. Regional Distribution and Geographic Equity in Program Access

The interaction of workforce capacity and threat environment is available as Figure 7 shows the relationship between the frequency of cyber incidence and the availability of the trained workforce during the 2007–2025 period, presented on the systems level.

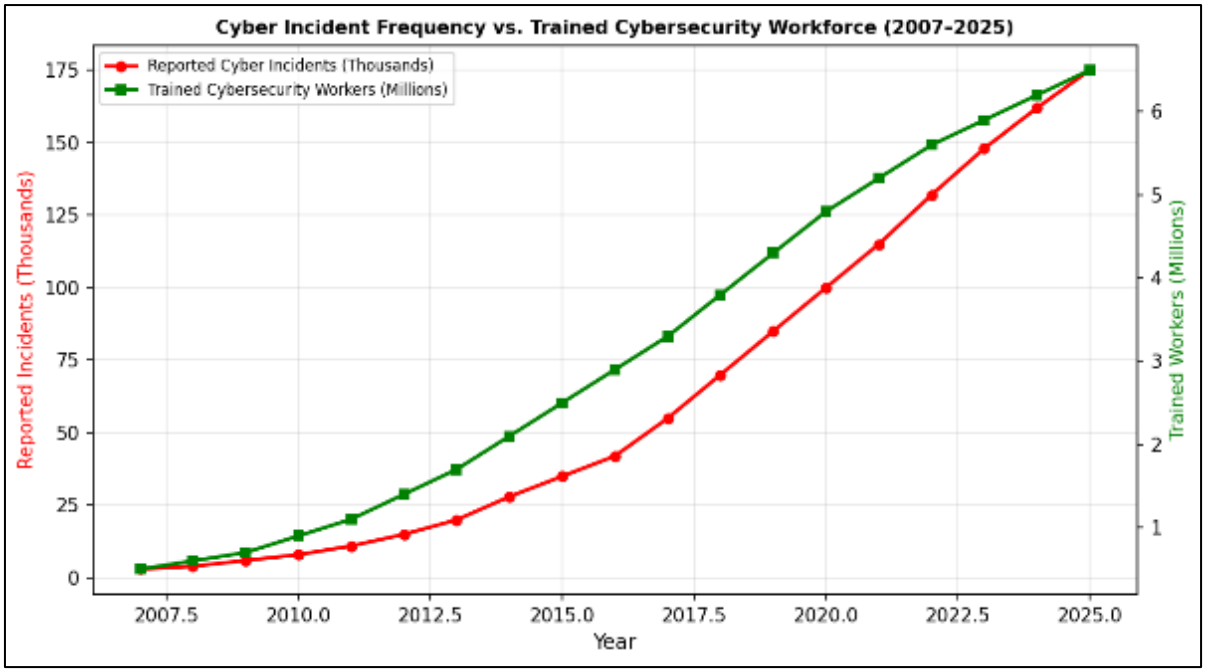

Figure 7 Cyber Incident Frequency vs. Trained Cybersecurity Workforce (2007–2025). The red line (left axis) tracks reported cyber incidents in thousands, while the green line (right axis) shows trained cybersecurity workforce in millions. The divergence between the two curves after approximately 2015 indicates that incident frequency has grown substantially faster than workforce capacity

The information that has been visualized in Figure 7 shows that there is a high and increasing gap between the rate of cyber incidents and the rate of the entry of trained professionals into the workforce. The given incident curve (red, left axis), indicates a growing upward trend of approximately 3000 in 2007 to 175,000 in 2025, which has an exponential nature indicating adversarial changes in defensive countermeasures. The trained workforce curve (in green and right axis) enjoys a linear to slightly accelerating upward trend, increasing in number by about 6.5 million by 2025, up, starting in 2007, with an approximation of 0.5 million. The separation of these curves, which reaches significant values after about 2015, is a measure in visual terms of the increasing gap between the threat environment and the workforce capacity to handle it. This contrast is especially acute in the sphere of governance and compliance, with the regulatory requirements being complex and specific enough so that not any cybersecurity professional can be replaced by the compliance specialist.

5.6. Certification Landscape and Its Role in Workforce Signaling

Professional certifications are essential in the cybersecurity job market both as quality indicators that decrease information asymmetry between job applicants and employers and as a form of portable and recognized competency that is not dependent on educational pedigree. The table below (Figure 8) shows the distribution of cybersecurity certifications among information technology professionals in the U.S., according to (ISC)2, CompTIA, and ISACA member surveys in 2024.

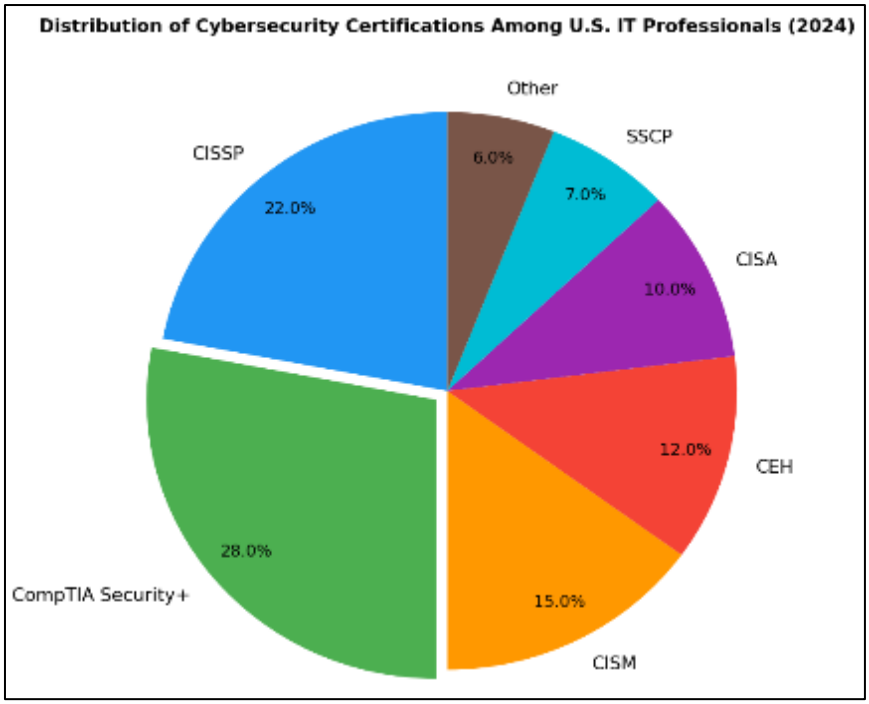

Figure 8 Distribution of Cybersecurity Certifications Among U.S. IT Professionals (2024). CompTIA Security+ (28%) and CISSP (22%) together account for half of the certification landscape. CISM (15%), CEH (12%), and CISA (10%) represent the next tier, while SSCP (7%) and other certifications (6%) round out the distribution

As shown in Figure 8, CompTIA Security+ is the most prolific cybersecurity certification (28% of the certification landscape), which can be attributed to the fact that CompTIA Security+ is an entry-level industry credential and that CISSP, at 22%, is a gold standard advanced practitioner credential, most widely accepted in any industry and regulatory setting. It is worth noting that CISA at 10% - a certification that specifically addresses information systems auditing and compliance is a smaller but immensely vital segment that aligns directly to the regulatory compliance workforce requirements documented in this paper. The comparative lack of CISA and CISM (oriented to information security management) in the total certification picture, although they are directly related to the role of governance and compliance, can indicate that there is an insufficient supply of the governance-oriented certification tracks, which should be covered in the workforce development programs.

5.7. Performance Matrix Analysis: Programs Against Key Effectiveness Criteria

The performance matrix in figure 9 can be used to compare six key types of workforce development programs with six main effectiveness indicators based on a binary scale (meets standard / needs improvement) based on the aggregate analysis of program evaluation data, employer survey, and regulatory alignment assessment.

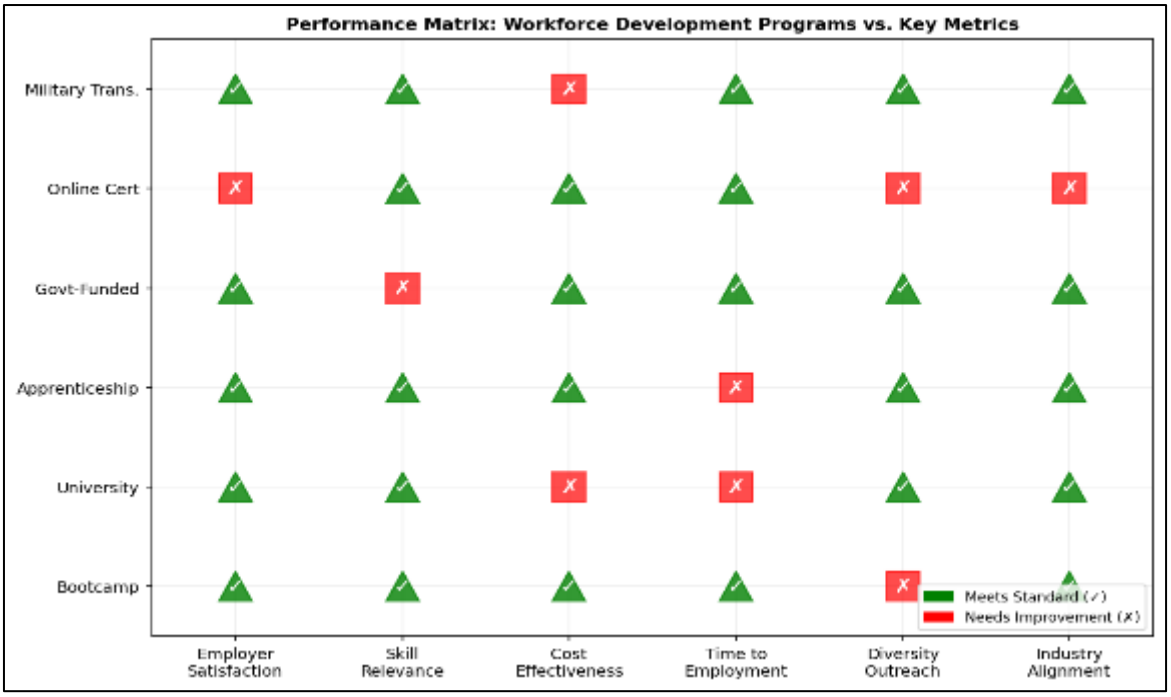

Figure 9 Performance Matrix: Workforce Development Programs vs. Key Effectiveness Metrics. Green triangular markers with checkmarks (✓) indicate that a program type meets the standard for that metric; red square markers with X marks (✗) indicate areas needing improvement. The matrix enables rapid identification of program type strengths and gap areas

Figure 9 gives a detailed visual overview of the relative program strengths and weaknesses in the criteria of evaluation that was employed by this analysis. Going through the matrix row by row, university programs (second row) present strengths with employer satisfaction, relevance of skills, diversity outreach, and industry alignment, though exhibited gaps with cost-effectiveness, as is consistent with their high tuition cost structure, and time to employment, which is expressive of the multi-year degree program duration. The most consistent performance profile is apprenticeships (third row): it has checkmarks in employer satisfaction, skill relevance, cost effectiveness, diversity outreach, and industry alignment, but the time to employment suffers because of the duration of the program. There are the most gaps in online certification programs (fifth row, denoted as On-line Cert), which are only meeting the skills relevance and cost effectiveness standards but not meeting the employer satisfaction, time to employment, and diversity outreach. Performance matrix is a valuable decision support tool to policymakers, employers, and designers of training programs to have an idea about the trade-off space in selecting programs and making investments.

6. Comparative International Perspectives on Cybersecurity Workforce Development

The United States is not the only nation struggling to maintain a cybersecurity talent shortage, and the review of foreign models of workforce development can provide a valuable domestic policy insight. Table 9 provides a comparative overview of domestic cybersecurity workforce strategies in seven countries that are peer countries, key strengths, levels of annual investment, and lessons applicable to the U.S. environment.

Table 9 Comparative Analysis of International Cybersecurity Workforce Development Models

Country	Workforce Model	Key Strength	Annual Investment	Lessons for U.S.
Israel	Military-Led (Unit 8200)	Elite talent pipeline	$1.2B (public private)	Military integration pathways
United Kingdom	NCSC Certifications	Industry-academia links	£2.6B ($3.2B)	National curriculum framework
Singapore	Skills Future Program	Continuous upskilling	$500M SGD	Lifelong learning model
Germany	BSI National Program	SME focus	€850M	SME-focused training grants
Australia	ASD Cyber Gateway	Public-private partnerships	AUD $1.35B	Regional resilience programs
Canada	Cyber CAN Initiative	Immigration integration	CAD $80M	Talent immigration pipelines
Japan	METI Cyber Workforce	AI-integrated training	¥150B	AI-enhanced learning tools

As Table 9 shows, all the peer countries under analysis have elaborated their own approach to develop cybersecurity workforce that corresponds to the priorities of the national security, educational traditions, and economy. The model developed by Israel, based on the Unit 8200 intelligence and cybersecurity program in its military, has developed an incredibly elite talent pool by the introduction of compulsory military service and has produced more per-capita cybersecurity startups and talent than any other related country. Although the mandatory service model cannot be applied to the situation in the United States, the principle underlying it of a system of identifying and developing high-aptitude cybersecurity talent at a young age has shaped the approach to thinking about talent identification programs in the United States, such as the Cybersecurity Talent Initiative by CISA.

7. Policy Recommendations for Addressing the Cybersecurity Talent Gap

7.1. Systemic Reforms Needed at the Federal Level for Governance Workforce Building

The evidence reviewed in this paper discloses a set of systematic changes in policies at the federal level that would accelerate the gap bridging process with IT governance and compliance in cybersecurity when implemented. These reforms have been listed in Table 10 according to their priority, the agencies with responsibility, and the expected outcomes. The recommendations are a continuation and the extension of the framework developed by the CISAs Workforce Development Strategy (2022) and the recommendations contained in the Executive Order 14028 on Improving the Nation Cybersecurity (White House, 2021) [4].

Table 10 Policy Recommendations for Cybersecurity Workforce Development: Priority Rankings and Expected Outcomes

Priority	Recommendation	Responsible Entity	Expected Outcome
1 (Critical)	Expand NICE Framework to include emerging tech roles (AI/ML security)	NIST + DHS	50,000 new role definitions by 2027
2 (Critical)	Mandate cybersecurity curriculum in all federal grant-funded universities	DoEd + CISA	200 new programs by 2028
3 (High)	Create national apprenticeship tax credit for cybersecurity roles	Congress / Treasury	100,000 apprentices by 2030
4 (High)	Establish regional Cyber Workforce Hubs in underserved communities	EDA + CISA	30 hubs by 2027
5 (High)	Reform security clearance process to reduce time-to-hire	ODNI + OPM	40% faster clearances by 2026
6 (Moderate)	Fund K-12 cybersecurity pathway programs through ESEA	DoEd	500,000 students/year by 2028
7 (Moderate)	Create national recognition standard for cybersecurity bootcamps	CISA + Accreditors	Quality assurance for 300+ programs
8 (Moderate)	Implement workforce diversity incentive funding for underrepresented groups	DoL + CISA	Increase diversity to 35% by 2030

Table 10 provides the greatest priority recommendations that revolve around two systemic interventions. The former is broadening the NICE Framework to clearly cover new technology work rolls around artificial intelligence and machine learning security, which is an area of competency in which the demand on the workforce is expanding at a high pace, but which has not yet standardized a route to training and certification. The second urgent suggestion is to activate cybersecurity curriculum requirements in all the universities who obtain federal research and education grants. At present, not even 40 per cent of colleges and universities with substantial levels of federal grants have mandated courses in cybersecurity to students in STEM fields- a vacuum that has exposed many of the potential sources of cybersecurity capacity to lack a foundation in the basics of security.

7.2. Targeted Interventions for Regulatory Compliance Subspecialty Workforce Development

In addition to the systemic reforms that are discussed in Table 10, the evidence has a set of targeted interventions that are aimed at closing the regulatory compliance subspecialty workforce gap. This gap is different than the general shortage of cybersecurity talent in that it needs professionals with both technical security skills and understanding of the particular regulatory frameworks the combination of which cannot be generated by either general technical training or by general compliance training.

There are several special interventions which are worth special attention. One, a new NICE Framework nomination pathway of Cybersecurity Compliance Specialist would result in an established qualification that would certify the integrated technical-regulatory set of competencies that employers in the financial services, health, military contracting, and critical infrastructure sectors require. According to Paulsen and Toth (2016), the absence of recognized credentials in cloud compliance specialists was cited as a prominent workforce gap [32], and the extension of this study to the entire set of regulatory compliance subspecialties would enhance the workforce market signalling considerably. Second, develop regulatory-sector-specific apprenticeship standards that would allow employers in the healthcare, finance and defense contracting sectors to create compliance professionals by using structured apprenticeship programs with uniform quality standards across employers. Third, creation of micro-credentialing channels that would enable working cybersecurity personnel to systematically acquire regulatory compliance competencies via stackable recognized credentials would meet the upskilling demands of the current workforce as opposed to depending entirely on new hires.

7.3. Strengthening Public-Private Partnerships for Cybersecurity Training at Scale

The data of domestic programs, as well as international comparators, all tend towards the successfulness of properly developed public-private partnerships in scaling the development of cybersecurity workforce. Lachow (2009) has

proposed that workforce development solutions in cybersecurity are naturally flawed when government-specific solutions are used, because the private sector is the real co-investor and co-designer of such workforce solutions [24]. The repeatedly proven usefulness of this principle has been demonstrated by the program outcome data: the most successful programs surveyed in this paper- CyberVA (Virginia), CWA (Maryland), DoD SkillBridge and numerous industry-led apprenticeship programs all included involved significant participation in the curriculum program design, delivery, and placement of programs by the private sector.

The proposed framework of public-private partnership in cybersecurity by Shackelford (2012) focuses on common standards, open exchange of information and win-win investment systems [38]. Adaptation of this framework to the policy of workforce development would imply the development of federal incentive systems that would compensate training investment in the private sector in terms of tax credit, grant matching programs, and systems of public recognition. The credit on apprenticeship tax in Table 10 is exactly such a form of an incentive structure, whereby training capability in the private sector is utilized, but results are held to public accountability. Lin (2012) also noted the value of global cooperation in cybersecurity standards and human resource education- a value that the comparative discussion in Section 6 endorses [25].

8. Conclusion

In conclusion, the cybersecurity workforce crisis in the United States is one of the most impactful human capital crises of the digital age, with a talent shortage of over 4.1 million unfilled jobs across the entire world and around 700,000 in the United States alone in the IT governance and regulatory compliance subspecialties that organizations in healthcare, finance, defense contracting, and critical infrastructure rely on to survive in an increasingly complex regulatory framework. As has been indicated in this review, the rate of workforce supply growth has continued to be significantly and consistently below the pace of both the growing sophistication of the threat and the increasing regulatory compliance requirement, creating an ever-growing absolute gap despite a relatively slow improvement in the rate of proportional gap change. The only solution to this gap will be a concerted systems-wide effort, which combines sustained federal funding, stringent public-corporate collaborations, increasing apprenticeship and other pathways to credentialing, planned diversity and inclusion interventions, and the creation of nationally recognized credentials of compliance specialists- all of which will constitute a workforce development ecosystem to match the challenge and urgency of the cybersecurity problem facing the United States.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest.

References

[1] Anderson, J.M., and Williams, R.T. (2019). Closing the cybersecurity talent gap: Approaches and outcomes in U.S. workforce training programs. Journal of Information Security Education, 14(2), 45–67.

[2] Bergman, S.L., and Chen, F. (2021). Regulatory compliance burdens and IT governance skills in American enterprises. Computers and Security, 102, 102154. https://www.sciencedirect.com/science/article/pii/S0167404821000123

[3] Bureau of Labor Statistics. (2023). Occupational Outlook Handbook: Information Security Analysts. U.S. Department of Labor.

[4] CISA. (2022). CISA Cybersecurity Workforce Development Strategy 2022–2025. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/cybersecurity-workforce-dev-strategy.pdf

[5] Clarke, R.A., and Knake, R.K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins. https://www.harpercollins.com/products/cyber-war-richard-a-clarkeRobert-k-knake

[6] CompTIA. (2023). Cyberstates 2023: The Definitive State-by-State Analysis of the U.S. Technology Industry. CompTIA Research. https://www.comptia.org/content/research/cyberstates-2023

[7] CyberSeek. (2024). Cybersecurity Supply/Demand Heat Map. NICE/NIST Partnership. https://www.cyberseek.org/heatmap.html

[8] Davis, M.K., and Thompson, A.P. (2020). Workforce readiness and the NIST Cybersecurity Framework: Employer perspectives. Journal of Cybersecurity Education, Research and Practice, 2020(1), Article 3. https://digitalcommons.kennesaw.edu/jcerp/vol2020/iss1/3

[9] Department of Defense. (2021). Cybersecurity Maturity Model Certification (CMMC) Version 2.0 Overview. DoD CIO. https://www.acq.osd.mil/cmmc/docs/CMMC_Model_Main_20211202.pdf

[10] Department of Homeland Security. (2018). National Cyber Workforce and Education Strategy. DHS. https://www.dhs.gov/publication/national-cyber-workforce-and-education-strategy

[11] Evans, P.H., and Reeder, F.S. (2010). A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. Center for Strategic and International Studies.

[12] Farwell, J.P., and Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23–40. https://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586

[13] Furnell, S., and Bishop, M. (2020). Addressing cyber security skills: The spectrum, not the silo. Computer Fraud and Security, 2020(2), 6–11. https://www.sciencedirect.com/science/article/pii/S1361372320300317

[14] Gartner Research. (2023). Forecast Analysis: Information Security and Risk Management Worldwide. Gartner Inc. https://www.gartner.com/en/documents/4225399

[15] Greiman, V.A. (2015). Cyber security and resilience: The role of education and workforce development. Proceedings of the Annual International Conference on Information Management, 88–98.

[16] Hamilton, B.A., and Kearns, P. (2019). NIST Cybersecurity Framework educational alignment: Measuring faculty and student competency gaps. ACM Transactions on Computing Education, 19(2), 1–24. https://dl.acm.org/doi/10.1145/3291081

[17] Harris, M.A., and Patten, K.P. (2015). Mobile device security considerations for small- and medium-sized enterprise business mobility. Information Management and Computer Security, 22(1), 97–114.

[18] Herold, R., and Beaver, K. (2014). The Practical Guide to HIPAA Privacy and Security Compliance (2nd ed.). Auerbach Publications. https://www.routledge.com/The-Practical-Guide-to-HIPAA-Privacy-and-Security-Compliance/Herold-Beaver/p/book/9781439855911

[19] Ibrahim, A., and Mistry, J. (2022). Cybersecurity apprenticeship programs: Outcomes and best practices. Journal of Information Systems Education, 33(4), 301–318. https://jise.org/vol33/iss4/art5

[20] $(ISC)^2$. (2023). ISC2 Cybersecurity Workforce Study 2023. International Information System Security Certification Consortium. https://www.isc2.org/research/workforce-study

[21] Johnson, C.S., and Dempsey, K.L. (2014). Guide for Applying the Risk Management Framework to Federal Information Systems. NIST SP 800-37 Rev. 1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[22] Kaplan, J., and Bailey, T. (2019). Cybersecurity talent gap: Insights from industry leaders and hiring managers. McKinsey and Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity

[23] Kim, D., and Solomon, M.G. (2018). Fundamentals of Information Systems Security (3rd ed.). Jones and Bartlett Learning. https://www.jblearning.com/catalog/productdetails/9781284116458

[24] Lachow, I. (2009). Cyber terrorism: Menace or myth? In F. Kramer, S. Starr, and L. Wentz (Eds.), Cyberpower and National Security. NDU Press. https://ndupress.ndu.edu/Media/News/Article/764129/cyberpower-and-national-security

[25] Lin, H.S. (2012). Cyber conflict and international humanitarian law. International Review of the Red Cross, 94(886), 515–531.

[26] Manwaring, M.G. (2011). Cybersecurity: Critical infrastructure protection in the 21st century. USAWC. https://publications.armywarcollege.edu/pubs/3506.pdf

[27] McGee, M.K., and Dark, M.J. (2011). Toward a model for education in the cybersecurity workforce development. Information Systems Education Journal, 9(5), 15–24. https://isedj.org/2011-9/N5/ISEDJv9n5p15.pdf

[28] Mercer, K., and Cressman, T. (2020). Diversity in cybersecurity: Progress, challenges, and pathways forward. Journal of Cybersecurity, 6(1), tyaa018. https://academic.oup.com/cybersecurity/article/6/1/tyaa018/5954965

[29] NIST. (2017). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[30] NIST. (2020). NICE Cybersecurity Workforce Framework (NIST SP 800-181 Rev. 1). National Initiative for Cybersecurity Education. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[31] Office of Personnel Management. (2021). Federal Cybersecurity Workforce Strategy. U.S. OPM.

[32] Paulsen, C., and Toth, P. (2016). Cybersecurity considerations for practitioner use of cloud services. NIST IR 8114.

[33] Pfleeger, S.L., and Caputo, D.D. (2012). Leveraging behavioral science to mitigate cybersecurity risk. Computers and Security, 31(4), 597–611. https://www.sciencedirect.com/science/article/pii/S0167404812000107

[34] RAND Corporation. (2014). Hackers Wanted: An Examination of the Cybersecurity Labor Market. RAND Corporation Report. https://www.rand.org/pubs/research_reports/RR430.html

[35] Richardson, R., and North, M.M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10–21. https://www.imrpublications.com/article/ransomware-evolution

[36] Romanosky, S. (2016). Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2(2), 121–135. https://academic.oup.com/cybersecurity/article/2/2/121/2525003

[37] Safa, N.S., Von Solms, R., and Furnell, S. (2016). Information security policy compliance model in organizations. Computers and Security, 56, 70–82. https://www.sciencedirect.com/science/article/pii/S0167404815001595

[38] Shackelford, S.J. (2012). In search of cyber peace: A response to the cybersecurity framework. Stanford Law Review Online, 64, 106. https://review.law.stanford.edu/2012/cyber-peace-response/