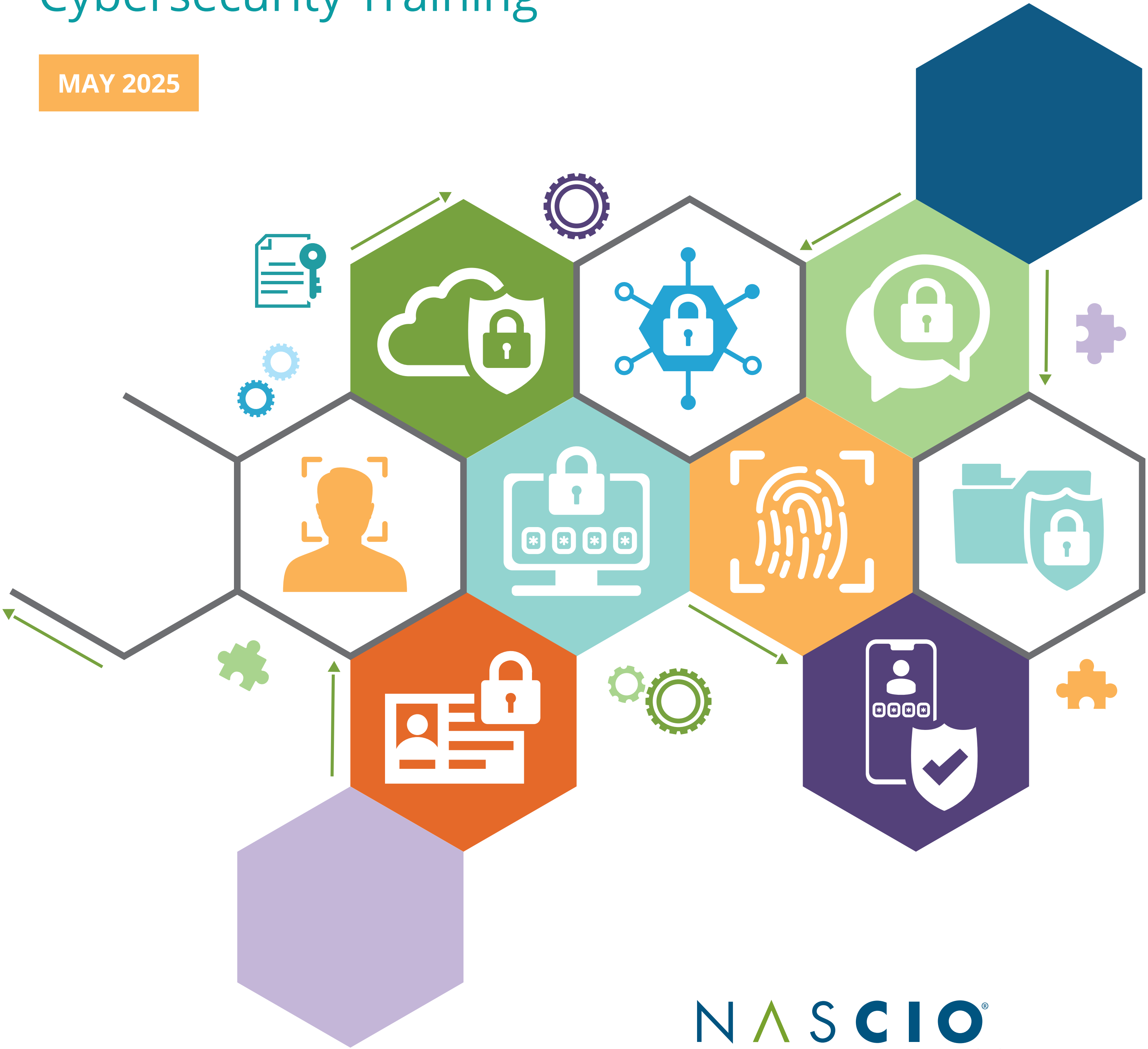
Unlocking Potential:

Empowering Reentry through Cybersecurity Training

MAY 2025



NASCIO
Representing Chief Information
Officers of the States

The Cybersecurity Talent Crisis

The cybersecurity sector in the United States is facing a critical shortage of skilled professionals, with nearly 265,000 job openings and only enough workers to fill 83 percent of available positions. This shortage is projected to be responsible for more than 50 percent of significant cybersecurity incidents by 2025, posing increased risks to two-thirds of organizations. NASCIO has studied the cyber workforce shortage in numerous publications; recently, the 2024 Deloitte-NASCIO Cybersecurity study revealed 49 percent of state CISOs cite cybersecurity staffing as top five challenge, even with demand for specialists rising. While state and local data on cybersecurity openings is sparse, the Pentagon reported having a vacancy for 28,000 civilian and military cyber roles in 2024 for the Department of Defense alone. Additionally, diversity remains a challenge, with women comprising only 24 percent of the cybersecurity workforce despite holding 36 percent of all technology industry jobs. The experience gap further exacerbates the issue, as jobs requiring more than two years of experience have only 77 percent of the supply needed to meet employer demand. By 2030, the global talent shortage across industries could lead to an estimated $8.5 trillion in unrealized annual revenue.

Considering these challenges, vocational cybersecurity training programs for non-violent offenders in correctional institutions present a unique opportunity to address multiple societal issues simultaneously. Individuals from low-income and technologically underserved communities, who are disproportionately represented in correctional institutions, can benefit from targeted training that equips them with valuable cybersecurity skills. Upon re-entering society, these individuals can fill critical gaps in the cybersecurity workforce, thereby reducing recidivism through gainful employment. Moreover, they can serve their communities by building rapport and trust, as they are often familiar faces to the locals. This approach not only addresses the cyber workforce shortage but also fosters a sense of community and trust in government institutions.

Implementing vocational cybersecurity training programs in prisons has the potential to significantly reduce recidivism rates among formerly incarcerated individuals, fill critical gaps in the cybersecurity workforce and enhance the cybersecurity resilience of low-income, technologically underserved communities.

Barriers for the Currently and Formerly Incarcerated

On average, over 600,000 people are released from state and federal prisons and over nine million from municipal or county jails per year. By the third year of release, at least 50 percent of released citizens are re-incarcerated. From a 30,000-foot view, scholars have proven for decades that low living wages and poverty are the primary indicators of crime and recidivism. The US Department of Justice Office of Policy and Programs found that being impoverished increases re-arrest likelihood by a factor of 4.6 and parole/probation violations by a factor of 12.7 for incarcerated women alone. Education intersects this issue, as many prisoners have low educational attainment which further complicates finding a decent job and keeping it. Around 40 percent of people going into prison do not have a high school diploma or GED equivalent, which is three times higher than the general US population. While approximately 40 percent of prisoners receive a GED while incarcerated, only 33 percent of all re-entering citizens use these skills in post-release employment, indicating that base-level education programs may not be enough.

Aside from poverty and limited educational attainment, gainful post-release employment is also negatively impacted by the most common type of work experience gained in prisons – prison labor. According to a study by the American Civil Liberties Union (ACLU) on the impact of prison labor nationwide, prison labor systems do not provide tangible workforce readiness, thus reducing job outcomes upon release. Prison labor roles, such as manufacturing, janitorial services, kitchen work and more, rarely provide certifications or other means that can be used to obtain post-release employment in the modern job market (e.g. technical skills, soft skills, industry exposure). In fact, the US Chamber of Commerce reported that more than half of states (27) restrict those with criminal records from gaining occupational licenses for marketable skills learned in prison. These jobs pay pennies per hour – ranging from $0.13 - $0.52 – which makes saving for post-release necessities virtually impossible, can create disdain towards work from being mistreated as an employee and deprives people of gaining real-world professional development experience (such as resume prep, interview prep, reviewing and accepting job offers.)

The Impact that Workforce Training has on Reentering Citizens

Research shows that having stable employment and income prevents crime. Obtaining employment within 600 days of reentering society is associated with a 20 percent lower likelihood of being re-incarcerated. The prospect of being re-arrested for non-employed formerly incarcerated people is 42 percent compared to 24 percent for those employed.

Prison education programs have been vital in increasing education and employment viability to reduce recidivism. A meta-analysis of 78 high-quality papers detailing prison education programs conducted by Mackinac Center for Public Policy found that generally, prison education programs have resulted in a nearly 15 percent decrease in recidivism. Breaking this down further, different program education levels also have varying effects on reentering citizens:

6.3%

reduction in recidivism through adult basic education/GED programs

7.2%

reduction in recidivism through secondary education

9.4%

reduction in recidivism through vocational education

27.8%

reduction in recidivism through college education

This meta-analysis also found that prison education programs contributed to a seven percent increase in the likelihood of being employed after prison, while more recent studies estimate the increase to be nearly eight percent, reflecting that for every 1,000 students that complete a prison education program, 30 more will obtain employment post-prison than those without program completion. Prison education programs also increased post-incarceration wages for participants by an average of $131 per quarter. While this may not seem like a significant increase, it is important to remember that most work experience obtained while incarcerated is prison labor, which can lead to lower-paying jobs once released. Prison education programs serve as a suitable alternative to prison labor, as formerly incarcerated people are better able to find fulfilling, better paying work on the outside.

Table 1: Effects of Prison Education Programs at Each Level of Education

Education Type	Cost (per participant)	Effect on Recidivism (% points)	Effect on Employment	Benefit: Employment Wages	Return on Investment
ABE	$1,400-$1,972	-2.9	+0.66	+$951	104%
Secondary	$1,987	-3.3	+0.54	+$883	122%
Vocational*	**$1,960-$2,126**	**-4.31**	**+2.48**	**+$1,978**	**205%**
College	$10,467	-12.7	+4.68	+$3,220	61%

Note: This table is an analysis of multiple sources. All statistics are in comparison to individuals who did not participate in any form of prison education program.

As shown in Table 1, prison education programs demonstrate consistent success across all levels, with varying cost-benefit outcomes. Adult Basic Education (ABE) offers high ROI (104 percent) by reducing recidivism by 2.9 percentage points, while secondary programs like GED yield modest employment gains and 122 percent ROI. College programs, though costlier, deliver the largest recidivism reduction (12.7 percentage points) and wage gains ($3,220), despite a lower ROI (61 percent). Based on this analysis, vocational training has the most value for money spent, making an excellent case for cybersecurity-focused education programs in prisons. Investing $1,960–$2,126 in one student can generate a $13.21 return per $1 spent (713 percent ROI) while reducing recidivism by 4.31 percentage points (e.g., from 46 percent to 41.69 percent) and increasing employment likelihood by 2.48 percentage points.

With that said, we can infer that prison education does provide a positive ROI at all levels. However, unmeasured benefits will also have a significant impact on communities. Through vocational cybersecurity training, reentering citizens will be qualified to work, especially in underserved communities, to fill gaps in the cyber workforce. Further, members of these communities can build trust in the government by interacting with public officials who understand community needs through lived experience and boost representation at higher state government levels.

Cybersecurity-Specific Training Model: NCSTA

The National Cyber Security Training Academy (NCSTA, formerly National Cyber Security University) offers the ***"Second Chances"*** Program to provide formerly incarcerated people with marketable cybersecurity skills that can help them secure a job and avoid reoffending. NCSTA partners with world-renowned cybersecurity organizations like CompTIA+, the Cybersecurity and Infrastructure Agency (CISA) and the International Law Enforcement Educators and Trainers Association to administer and design program courses. This creates a domino effect when people obtain jobs in their own communities, often underserved, and return to work in the place they call home. Citizens are better served by people who are aware of their communities' unique needs and cybersecurity workforce needs are met.

Enrollment in the NCSTA Second Chances Program is open to those aged 14 and older with non-violent, lower-level offenses (those convicted of violent crimes, sex offenses, domestic violence, financial-related crimes and cyber-related crimes are not eligible to participate). Applications are reviewed by multiple advisors, including at least one probation officer, an attorney and a national job recruiter. The curriculum consists of six courses that can be taken in a standard in-person, virtual or self-paced online classroom. The program usually takes three to six months to complete but varies depending on the student's experience and prior knowledge. Upon completion and graduation from Second Chances, students are qualified to start a new career in one of the following roles: junior network administrator, system engineer, network field engineer, security specialist, cyber-crime investigator, security administrator, IT auditor, penetration tester, vulnerability tester or security analyst (II).

While concrete return on investment data is not publicly available, direct testimonials indicate the positive impact of the Second Chances Program. Second Chances instructor Gregory Evans stated that, "The reason why cyber crime is on the rise and will likely never decline, is because many of the people who are hired to protect government and corporate networks, are not hackers. They have often only learned how to protect networks in theory in a classroom and from books… This is because those protecting networks are not taught to think like criminals. You have to learn how to think outside of the box."

State and Local Government Implementation

State CIOs, CISOs and other state leaders have a unique opportunity to work together to build a program that can benefit the cybersecurity workforce, underserved communities and better the lives of justice-involved people. To build a program, states should do the following:

1. **Establish Program and Curriculum**
   - Partner with existing cybersecurity education programs to establish a curriculum that combines basic education, cybersecurity training, and soft skills
   - Focus on industry-recognized certifications such as CompTIA Security+ or Certified Ethical Hacker
   - Incorporate a continuity-of-care model linking pre-release training to post-release employment support
2. **Establish Partnerships**
   - Collaborate with correctional facilities to establish prison-based training programs
   - Partner with local educational institutions to provide instructors and resources
   - Engage private sector cybersecurity companies for mentorship and potential employment opportunities
3. **Secure Funding and Resources**
   - Utilize reinstated Pell Grant eligibility for incarcerated students to fund educational components
   - Seek additional funding through state budgets or federal, non-profit and/or foundation grants
   - Explore public-private partnerships for equipment and software donations
4. **Pre-Release Training**
   - Implement a program similar to the Department of Labor's LEAP initiative, which had an 85 percent completion rate
   - Provide both theoretical knowledge and hands-on practical skills in cybersecurity including modules on ethics, professional conduct and responsible use of technology
5. **Post-Release Support**
   - Establish a transition program to help participants integrate into the state workforce
   - Offer ongoing mentorship and professional development opportunities
   - Create a probationary employment period to allow participants to demonstrate their skills and reliability
6. **Program Evaluation**
   - Track key metrics such as program completion rates, certification attainment and post-release employment rates
   - Conduct long-term studies on recidivism rates and career progression of program participants
   - Calculate ROI to justify program continuation and expansion

A state implementing a program to train incarcerated individuals for cybersecurity roles would need to consider hiring or outsourcing the following types of personnel:

Educational Staff/Contractors

- Instructors with expertise in cybersecurity to deliver the technical curriculum
- Adult education specialists to address basic educational needs and literacy challenges

Program Administrators

- Project managers to oversee the program implementation and coordination
- Liaison officers to work with correctional facilities and workforce development agencies

Support Services

- Career counselors to assist with job readiness and placement
- Mentors, potentially including reformed ex-offenders, to provide guidance and support
- Technical specialists
- IT professionals to set up and maintain training environments
- Cybersecurity practitioners to ensure curriculum aligns with industry needs

Evaluation and Compliance Personnel

- Data analysts to track program metrics and outcomes
- Compliance officers to navigate legal and ethical considerations

Post-Release Support Staff

- Case managers to assist with the transition from incarceration to employment
- Job placement specialists with knowledge of the cybersecurity industry

By assembling a diverse team with these skill sets, states can create a comprehensive program that addresses the educational, technical and support needs of incarcerated individuals pursuing cybersecurity careers.

Finding Second Chances in Cybersecurity Careers

The cybersecurity workforce shortage, projected to drive over 50 percent of critical incidents by 2025, demands innovative solutions. The 2023 NASCIO-NGA publication Securing States: Modernizing to Attract and Retain Cyber Talent provided two key recommendations:

- States must focus on diversity, equity, inclusion and belonging (DEIB) in their recruitment, hiring and retention practices.
- States need to collaborate with key tech and cybersecurity stakeholders, including the private sector, academia, nonprofit organizations, the federal government, minority-serving institutions and professional associations, to provide development opportunities and build workforce pipelines.

A cybersecurity training program for formerly incarcerated individuals is an approach that embodies both key strategies in recruiting and retaining cyber talent to close the gap. Vocational cybersecurity training programs in correctional institutions offer a dual benefit: reducing recidivism by equipping low-level, non-violent offenders from underserved communities with in-demand skills and addressing the industry's four million-person global talent gap. While research suggests that prison education programs are successful in reducing recidivism, the stigma surrounding those formerly incarcerated prevents the nation from rewriting this narrative on a wider scale.

States can help undo this stigma by implementing ethical reentry and prison education programs that pair technical cybersecurity training with mentorship, role-based access controls and regular compliance workshops. These measures empower formerly incarcerated employees to navigate workplace expectations, build trust through accountability, and demonstrate responsibility in cybersecurity roles. By aligning with workforce demands—where jobs requiring more than two years of experience face a 23 percent supply gap—these initiatives not only mitigate systemic inequities but also strengthen national cybersecurity resilience, fostering safer communities and a more inclusive workforce.

Primary Author

Kalea Young-Gibson
Policy Analyst
NASCIO

NASCIO®
Representing Chief Information
Officers of the States

About NASCIO

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.NASCIO.org.