

U C B E R K E L E Y

C E N T E R F O R L O N G - T E R M C Y B E R S E C U R I T Y



Save Money, Build Talent, and Defend Communities

A WHOLE-OF-STATE CYBERSECURITY GUIDEBOOK

GRACE MENNA

May 2026

CLTC WHITE PAPER SERIES

Save Money, Build Talent, and Defend Communities

A Whole-of-State Cybersecurity Guidebook

Grace Menna

Senior Fellow, Public Interest Cybersecurity

UC Berkeley Center for Long-Term Cybersecurity

May 2026



Contents

- Executive Summary** 3
- Introduction** 4
- Section I: Mapping State-Led Cyber Defense Programs** 6
 - Program Scope 6
 - Common State Cybersecurity Governance, Resources, and Infrastructure 7
 - Top Whole-of-State Cyber Defense Programs 9
 - Cybersecurity Clinics 10
 - Regional Security Operations Centers (RSOCs) 11
 - State Cyber Corps 13
- Section II: Constructing a Built-to-Last State Cyber Ecosystem** 16
- Section III: Return on Investment of Cyber Defense Programs** 18
 - Saving Taxpayer Money 19
 - Improving State Fiscal Health through Bond Rating Preservation or Improvement 20
 - Workforce Development 21
 - Defense of Community Services 22
- Section IV: Best Practices of Successful Programs — and Common Barriers** 24
 - Best Practices of Successful Programs 24
 - Common Hurdles Across Programs 25
 - Statewide Ecosystems of Cyber Defense Programs 27
 - Texas 27
 - Wisconsin 29
 - New Jersey 31
- Conclusion** 33
 - Further Action 33
 - Reading and Resources 34
- Acknowledgments** 36
- Bibliography** 37
- Appendix 1A: Cybersecurity Clinic Case Study** 42
- Appendix 1B: State Cyber Corps Case Study** 43

Executive Summary

Community organizations that are vital to delivering essential services to the public — including nonprofits, rural hospitals, schools, local utilities, counties, municipalities, and small businesses — are often the least resourced and prepared to protect themselves from cyberattacks. These organizations are often wholly responsible for their own defense against cyber criminals and even nation-states like China and Russia. Disruptions to community services due to cyber attacks can have dramatic and far reaching consequences, including children missing school, disruption of local EMS services, and food banks closing.

In response, state governments are turning to community support ecosystems to provide a safety net that strengthens civic organizations' cyber defenses, ensuring they can continue their vital work securely and without disruption. As part of a growing “whole-of-state” cybersecurity strategy, many states are piloting cyber defense programs that rely on local talent to provide hands-on assistance to fill critical gaps in the cyber defenses of communities. These programs lean on civilian participation to help bolster defenses, often by upskilling students and deploying local skilled volunteers to save money, develop the local cybersecurity workforce, and build resilience. However, these programs cannot succeed in a vacuum; they need financial and administrative support from state leaders.

In this guidebook, the UC Berkeley Center for Long-Term Cybersecurity (CLTC) Public Interest Cybersecurity Program highlights a collection of

community cyber defense programs: cybersecurity clinics, regional security operation centers (RSOCs), and state cyber corps. The guidebook then outlines the return on investment of these programs.

Key insights from this guidebook explore how community cyber defense programs:

- 1. Save taxpayer dollars,**
- 2. Develop the local workforce,**
- 3. Strengthen community cyber defense, and**
- 4. Are most effective when they are part of a wider local defense ecosystem.**

Addressing the operational realities of these programs, the guidebook explores shared aspects of successful programs, as well as common hurdles and examples of how to overcome them. Zooming out, the guidebook then highlights how these programs can work together to create a cohesive and resilient state cyber ecosystem. Through case studies centered on initiatives in Texas, Wisconsin, and New Jersey, the paper shows how a network of programs collaborating and sharing intelligence can be a force multiplier for a state's investment in local cyber defense.

This guidebook provides a path forward for state legislators, chief information security officers (CISOs), chief information officers (CIOs), and governors to double down on their whole-of-state cybersecurity strategy by investing in and connecting their local cyber defense programs.

Introduction

As technology has become embedded in nearly every aspect of society, the majority of organizations that provide essential public services lack both the cybersecurity expertise to protect themselves and the resources to hire outside help. This lack of resources — sometimes referred to as the “cyber poverty line” or “target-rich, resource-poor” organizations — leaves essential public services uniquely vulnerable to disruption. With the recent enhanced capabilities of artificial intelligence, it has never been easier for threat actors to automate and deploy frequent attacks on the small organizations that power our local and state economies.

The attack surface of community organizations expands each year, but their ability to manage the increased risks does not. Disconnecting from the online space is not an option; the internet underpins the economy, and nearly every service people rely on in daily life requires an internet connection. Without this interconnected technology, public life comes to a halt: schools close, ATMs stop functioning, and utilities shut off. According to the United States House Homeland Security Committee, major cyber attacks on state and local governments were observed in at least 44 U.S. states during the first ten months of 2025.¹

At the same time, state governments are being asked to take on more cybersecurity leadership

and responsibility than ever before. An Executive Order signed by President Trump in March 2025, “Achieving Efficiency Through State and Local Preparedness,” pushed states to “play a more active and significant role in national resilience and preparedness.”² However, many states’ cybersecurity initiatives are threatened as key federal funding programs are not guaranteed to renew. Such programs include the State and Local Cybersecurity Grant Program (SLCGP)³ and the Tribal Cybersecurity Grant Program (TCGP),⁴ which together directed \$1 billion in cybersecurity funding to state and local governments and tribal communities between FY 2022 and FY 2025. Funding from these grant programs has helped states stop active cyber attacks, fund endpoint protection for thousands of devices, increase information sharing, and train cybersecurity talent, yet these important programs now face uncertainty without guaranteed long-term funding.

Federal funding for key information-sharing mechanisms, such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), was withdrawn in 2025. This led to the MS-ISAC pivoting to a paid membership-based model, further placing financial responsibility on state and local governments. Additionally, the burden on states is dramatically increasing as federal agencies — including the Cybersecurity and Infrastructure

¹ Andrew Garbarino, *Cyber Threat Snapshot* (House Homeland Security Republicans, 2025), <https://homeland.house.gov/wp-content/uploads/2025/10/Cyber-Threat-Snapshot.pdf>.

² Executive Office of the President, *Achieving Efficiency Through State and Local Preparedness*, FR Doc 2025-04973 (2025), <https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/>.

³ Cybersecurity and Infrastructure Security Agency, “State and Local Cybersecurity Grant Program,” accessed March 13, 2026, <https://www.cisa.gov/cybergrants/slcgp>.

⁴ Cybersecurity and Infrastructure Security Agency, “Tribal Cybersecurity Grant Program,” accessed March 13, 2026, <https://www.cisa.gov/cybergrants/tcgp>.

Security Agency (CISA), the Department of Education, the Department of Energy, the Department of Justice, and other sector risk management agencies (SRMAs) — are losing critical staff due to budget cuts and federal restructuring. This rollback of federal cybersecurity support to local communities further requires states to take up the gauntlet to protect their citizens from the consequences of cyberattacks and data breaches.

*“New Jersey continues to mature its whole-of-state cybersecurity framework [...] recogniz[ing] that true resilience is achieved not through isolated efforts, but through collective defense — linking state agencies, county and municipal governments, educational institutions, critical infrastructure operators, the private sector, and civil society under a unified collaborative model”.*⁵

— New Jersey Cybersecurity and Communications Integration Cell Strategic Plan 2026–2030

The whole-of-state cybersecurity model, a relatively new strategy for cybersecurity on the state and local levels, challenges the status quo that individual organizations should face the threats of cyber attacks alone. Whole-of-state cybersecurity

strategy is a coordinated, collaborative approach to cybersecurity that unites state agencies, local governments, educational institutions, critical infrastructure partners, and other community organizations. As defined by the Center for Internet Security, this strategy provides “shared governance, resources, standards, and support mechanisms to reduce risk, improve preparedness, and enhance the prevention, detection, response, and recovery capabilities for cyber, physical, and information operations threats.”⁶ While every state’s approach to implementing the whole-of-state strategy varies, this model fundamentally redefines cybersecurity by emphasizing shared responsibility, shared risk, and shared response.

Many of these state-adopted models are showing early signs of promise and have led to increased resilience and cost savings. States like New York, Arizona, and New Jersey have adopted strategic plans that shift the burden of securing and protecting vital civic services away from organizations that are least equipped to protect themselves, both in terms of expertise and financial resources. However, state government agencies cannot undertake this work alone, and states have the opportunity to establish cyber support ecosystems that can sustainably protect their residents in the long term.

⁵ New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), *NJCCIC Strategic Plan 2026-2030* (2026), <https://www.cyber.nj.gov/grants-and-resources/state-resources/njccic-strategic-plan>.

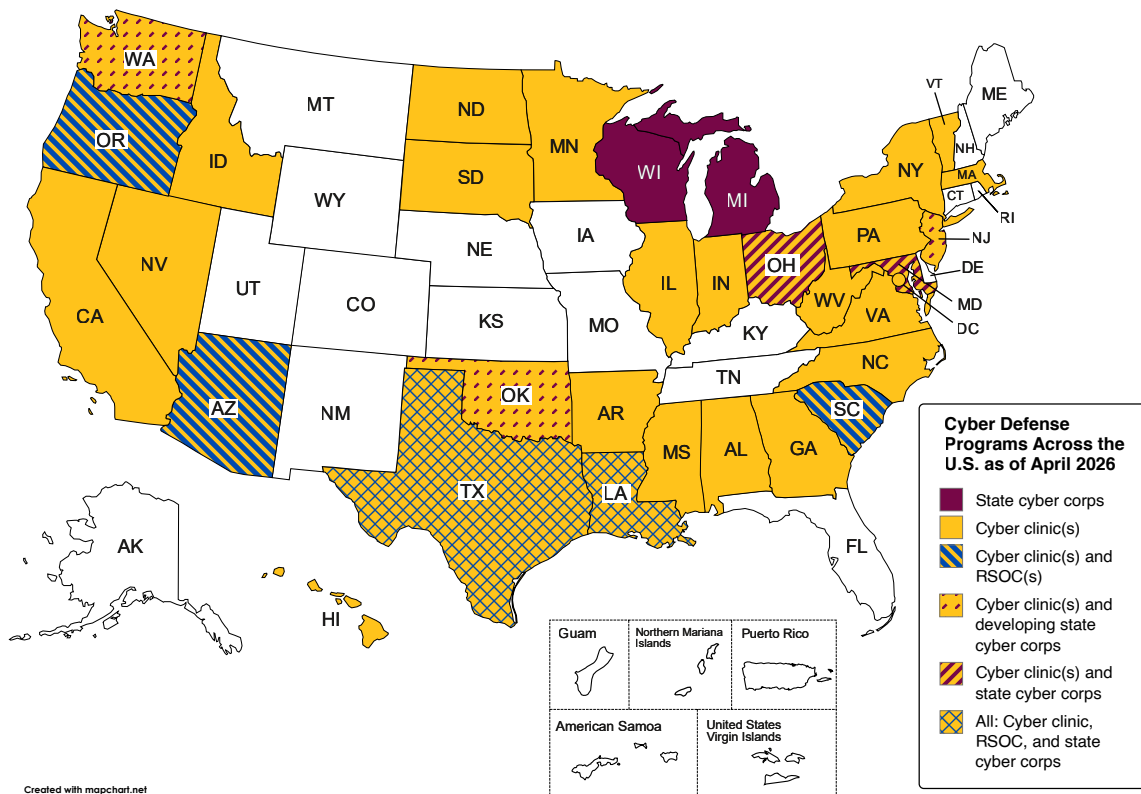
⁶ Center for Internet Security, “Whole-of-State Security,” accessed April 16, 2026, <https://www.cisecurity.org/whole-of-state-security>.

Section I: Mapping State-Led Cyber Defense Programs

Whole-of-state cybersecurity is supported by a wide range of mechanisms, including but not limited to shared intelligence, tools, and products, shared training and education, and streamlined procurement processes for cybersecurity software

and hardware. This section will map existing programs across different states, with a focus on three community cyber defense programs: cybersecurity clinics, RSOCs, and state cyber corps.

Figure 1: Cyber Defense Programs in the U.S. as of April 2026



Program Scope

For the purposes of this guidebook, “community cyber defense programs” are defined as programs that rely on local talent to provide hands-on assistance to fill critical gaps in the cyber defenses of communities. The authors selected this definition to focus only on programs that provide direct services to organizations, and that serve as workforce development and maturation vehicles.

The programs covered in this guidebook are: cybersecurity clinics, regional security operations centers (RSOCs), and state cyber corps.

This guidebook will not go into depth on specific policy or procurement strategies, or on state-led programs that exclusively serve the state government or critical infrastructure.

Common State Cybersecurity Governance, Resources, and Infrastructure

Existing state infrastructure for cybersecurity provides resources like governance (including strategy and policies that help prevent the interruption of activities due to cyber threats or attacks), funding, and threat intelligence. Below, we provide an overview of some of the most common state cyber initiatives, in part to clarify how they are different from community cyber defense programs, which we focus on in the next section. Expanding the connections between these existing resources and infrastructure to community cyber defense programs could greatly boost whole-of-state cybersecurity efforts.

1. Fusion centers/integration cells are owned and operated by states, often with some support from the U.S. Department of Homeland Security, and serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information between state, local, tribal, and territorial (SLTT) entities, federal agencies, and private-sector partners.⁷ State and local police departments often provide both space and resources for these centers, which can be staffed by representatives spanning the private sector, military, federal government, and local law enforcement.⁸

2. Information Sharing and Analysis Centers (ISACs) are nonprofit, member-driven organizations that help critical infrastructure owners and operators share, analyze, and mitigate cyber and physical threats. Prominent examples include

the Multi-State Information Sharing and Analysis Center (MS-ISAC), Electricity Information Sharing and Analysis Center (E-ISAC), and NGO Information Sharing and Analysis Center (NGO-ISAC). Some states operate their own independent, state-specific ISACs or equivalent integration cells to provide more localized threat intelligence and coordination.

3. Cyber risk pools are groups of entities that share the costs of cybersecurity risk. Instead of individual entities buying independent coverage from a traditional, for-profit insurance company, participating entities contribute to a collective fund that covers losses while providing risk management services such as cyber risk assessments, training, policy templates, and incident response planning. These funds are often designed to help participating entities meet mandatory security standards.

4. State-led centralized procurement of shared services facilitate the procurement of tools, products, and services that can be utilized by public entities, reducing the time, cost, and expertise required for the procurement process. These programs often help participating entities attain better prices, as the state government has greater leverage than individual entities when negotiating contracts. The benefits can include reduction in technology costs: for example, security information and event management (SIEM) and security orchestration, automation, and response (SOAR) cost less per endpoint when acquired at scale. Centralized procurement can also lead to reductions in management costs by centralizing specialist talent rather than distributing generalists, enabling bulk licensing and consolidated vendor contracts, and increasing investment capacity for advanced

⁷ United States Department of Homeland Security, “Fusion Centers,” accessed March 13, 2026, <https://www.dhs.gov/fusion-centers>.

⁸ Torin Monahan and Priscilla M. Regan, “Zones of Opacity: Data Fusion in Post-9/11 Security Organizations,” *Canadian Journal of Law and Society* 27, no. 3 (2012): 301–17, <https://doi.org/10.1017/S0829320100010528>.

infrastructure.⁹ Common products offered through state governments' centralized procurement include external vulnerability scans, anti-phishing/security awareness training (SAT), advanced endpoint protection (AEP), converged endpoint management (XEM), multi-factor authentication (MFA), and web application firewalls (WAFs).

5. Funding (typically through grants)

includes the allocation of money specifically for cybersecurity tools, products, and services. In addition to state-level funding, programs like the State and Local Cybersecurity Grant Program (SLCGP)¹⁰ and the Tribal Cybersecurity Grant Program (TCGP)¹¹ — federal grant programs that direct money specifically to local communities — have provided financial and functional support to local governments, particularly those in under-resourced rural areas. Some states offer novel cybersecurity grant programs specifically for nonprofit organizations. Arizona's Nonprofit Security Grant Program (NSGP) is an example of one of these programs.¹²

6. Cyber ranges are secure, sandboxed virtual environments used to train security and IT professionals and students on realistic cyber scenarios, equipping them with hands-on skills that can be applied in the workforce. Cyber ranges serve as laboratories for assessing talent, validating new technologies, and ensuring critical infrastructure remains resilient against evolving threats.

Cyber ranges simulate real-world network attacks and defenses as training environments for students and professionals. They often offer a combination

of offensive and defensive exercises and guided labs to facilitate learning specific tools. At these ranges, incident response teams can test their emergency plans to see if their communication and technical steps actually work under pressure. Some ranges specialize in operational technology (OT), which controls physical machinery and is often a component of critical infrastructure. Ranges that specialize in OT provide a unique opportunity for technicians to practice defending against attacks that could cause physical damage. University-based cyber ranges in particular help bridge an essential gap in the cybersecurity field by preparing entry-level talent for the job market.

7. A centralized state cybersecurity authority,

sometimes referred to as a “state cyber command center” or “integration cell,” is responsible for 24/7 monitoring, incident response, cybersecurity governance and policy, and cybersecurity operations for state government networks. These centers operate under state law and, when the National Guard is involved, Title 32 (i.e., maintaining state control but providing federal funding). Command centers' authority is strictly limited to their states' borders and specific state-managed networks, and they are sometimes housed in a state's emergency management, homeland security, or IT department. These authorities create operational efficiency by centralizing coordination instead of relying on different agencies to share responsibility. Centralizing authorities can also help bolster digital defenses across the state by providing proactive preparation through simulation exercises, strategic planning, and collaboration with critical infrastructure partners.

⁹ Drew Leatherby, *IT Consolidation and Shared Services: States Seeking Economies of Scale* (NASCIO, 2006), https://www.nascio.org/wp-content/uploads/2019/11/NASCIO-Con_and_SS_Issue_Brief_o3o6.pdf

¹⁰ Cybersecurity Infrastructure and Security Agency, “State and Local Cybersecurity Grant Program.”

¹¹ Cybersecurity Infrastructure and Security Agency, “Tribal Cybersecurity Grant Program.”

¹² Arizona Department of Homeland Security, “Nonprofit Security Grant Program (NSGP),” October 31, 2023, <https://azdohs.gov/az-nsgp>.

Top Whole-of-State Cyber Defense Programs

This section outlines three community cyber defense programs and details the benefits they provide to states, what gaps they fill, and their current scale across U.S. states.

Figure 2: Comparing Cyber Defense Programs

Cyber Defense Program Type	Lead Entity	Scale	Services	Gross Economic Value
Cyber Clinics	Higher education institutions (universities and community colleges)	Each clinic can serve, on average, between 8 and 20 community organizations a year	<ul style="list-style-type: none"> Vulnerability and risk assessments Cybersecurity policy templates Incident response plans Ransomware training NIST and CMMC certifications 	Between \$12,000–\$150,000/year in economic value from risk assessments + Workforce development investments in students
RSOCs	Higher education institutions (universities and community colleges)	Each RSOC can monitor up to approximately 22,000 devices	<ul style="list-style-type: none"> Real-time monitoring Alerts Incident response 	Between \$1.1M–\$2.6M per year in economic value
State Cyber Corps	State agency (often Emergency Management, Homeland Security, IT, or National/State Guard)	Between 2 – 80 organizations provided with incident response services per year 125+ organizations provided proactive services per year	<ul style="list-style-type: none"> Education and training Vulnerability and risk assessment On-call expertise, incident response, and recovery efforts 	Between \$1.4M–\$7.5M per year in economic value

Cybersecurity Clinics

Program details: Modeled after legal and medical school clinics, cybersecurity clinics train students at colleges and universities to provide pro bono cybersecurity services to community organizations, including small businesses, nonprofits, cities and towns, rural school districts, small utilities, and others. Cybersecurity clinics offer real-world experience to students from diverse backgrounds and degree paths, while also providing a source of free cybersecurity assistance to organizations that would otherwise be unable to afford these services. Clinics serve as a skills-based learning environment for students and as a vital local resource for improving the cybersecurity of community-based organizations. Many cybersecurity clinics rely on extramural funding, including government grants and private philanthropy, to launch and sustain their programs.

Services offered: University-based cybersecurity clinics help clients develop long-term cybersecurity defense, increase their resilience, and expand their cybersecurity capacity. Students provide a range of

digital security services, such as vulnerability and risk assessments, cybersecurity policy templates, incident response plans, ransomware training, NIST and CMMC certification readiness, and more. (See Appendix 1A for a case study outlining how the San Diego Cyber Clinic supported a local municipal water district.)

Gap addressed: There is no substitute for face-to-face discussions in building lasting cyber resilience, but many community organizations cannot afford costly professional consulting services.¹³ Cybersecurity clinics fill this gap by providing proactive assessments to organizations that are currently underserved by the cyber market.

Program scale: According to the Consortium of Cybersecurity Clinics,¹⁴ as of March 2026, 45 cybersecurity clinics operate in at least 29 states in the U.S., with a total of over 61 clinics worldwide. Globally, clinics have trained over 3700 students to provide pro bono cybersecurity risk assessments, and have provided free assistance to over 900 community organizations, including nonprofits, cities, healthcare organizations, schools, and more.¹⁵

¹³ Sarah Powazek and Shannon Pierson, *CyberCAN: Cybersecurity for Cities and Nonprofits* (UC Berkeley Center for Long-Term Cybersecurity, November 2024), <https://cltc.berkeley.edu/publication/cybercan-cybersecurity-for-cities-and-nonprofits/>.

¹⁴ Consortium of Cybersecurity Clinics, “Home,” accessed March 13, 2026, <https://cybersecurityclinics.org/>.

¹⁵ Matthew Nagamine and Nick Perematko, “Growth and Impact: Clinics Reach New Heights,” Consortium of Cybersecurity Clinics, October 1, 2025, <https://cybersecurityclinics.org/blog/growth-and-impact-clinics-reach-new-heights/>.

RSOC model is a “win-win” for communities as it provides both a cost-efficient and practical solution for protecting target-rich, resource-poor entities while also training the next generation of cyber talent locally. While many existing RSOCs are run out of higher educational institutions, they differ from the standard university cyber clinic model because they actively monitor an organization’s IT infrastructure on an ongoing basis, whereas cyber clinics typically operate on a one-time basis and offer preventive services, such as vulnerability and risk assessments.

Under-resourced organizations supported by RSOCs gain cyber support and protection that otherwise might not be available to them, and local students who work in the centers gain invaluable training. Under the supervision of instructors, students learn to operate and utilize cutting-edge, industry-standard tools. This hands-on experience translates into real workforce readiness for a cohort of students in a way that a standard degree program may not. This not only gives students a

potential leg-up in a competitive job market after graduation, but also creates a pipeline of skilled cyber talent who can help fill local skills gaps.

RSOCs also make information sharing between disparate entities easier, as standard RSOC ticketing and tracking systems help create data and insights that can be shared with other public entities. Increased information sharing, particularly around indicators of compromise (IOCs), helps prevent similar attacks from happening to multiple entities. RSOCs typically limit their beneficiaries to public entities, making them a great solution for small municipalities, but there are some types of community organizations that still fall through the cracks, such as nonprofits and small businesses.

Scale: RSOCs have been established in five states, with all programs based at higher education institutions, including universities or community colleges. States that currently operate at least one university-based RSOC include Arizona,¹⁶ Texas,¹⁷ Louisiana,^{18,19} Oregon²⁰, and South Carolina.²¹

¹⁶ Pima Community College, “Governor Hobbs Announces New Cybersecurity Partnership between PCC and Arizona Department of Homeland Security,” accessed March 13, 2026, <https://www.pima.edu/news/press-releases/2025/202510-25-cybersecurity-partnership.html>.

¹⁷ Texas Department of Information Resources, “An Overview of Regional Security Operations Centers (RSOCs) in Texas,” accessed March 13, 2026, <https://dir.texas.gov/resource-library-item/overview-regional-security-operations-centers-rsocs-texas>.

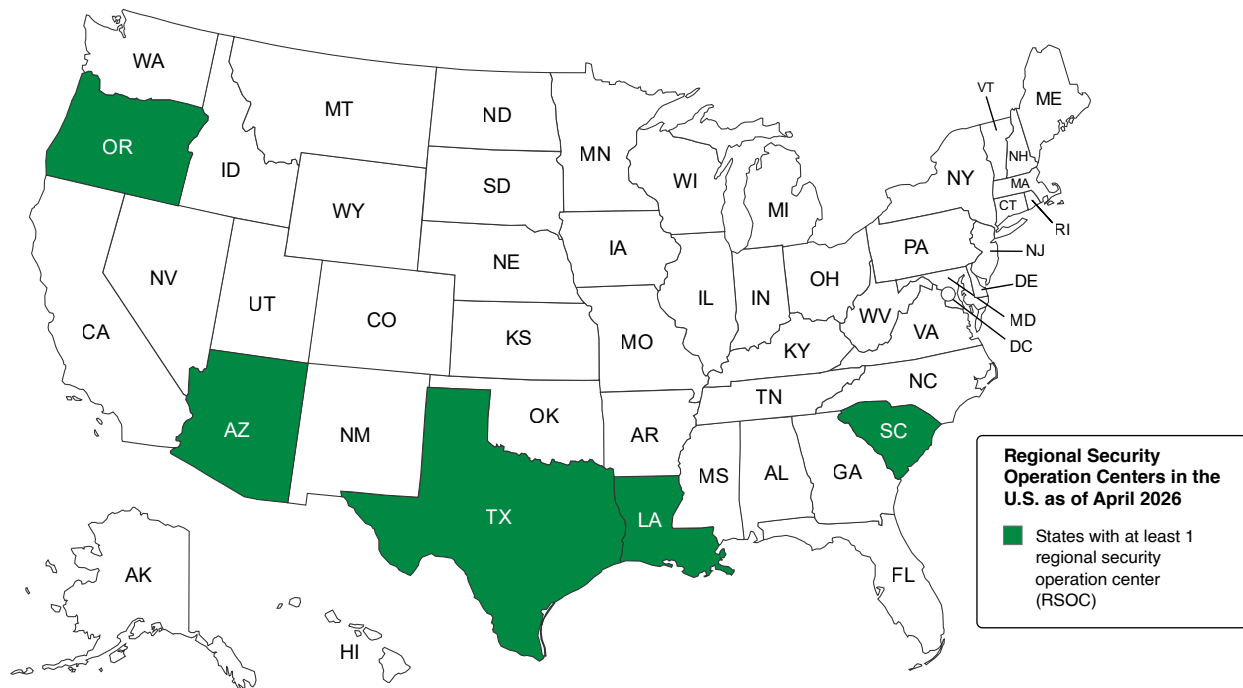
¹⁸ Louisiana State University, “Louisiana Enables Cyber Protection for Higher Ed in the State Through LSU,” accessed March 13, 2026, <https://www.lsu.edu/mediacenter/news/2023/09/wfl-soc.php>.

¹⁹ Louisiana State University, “Trailblazing Partnership with Industry, State: LSU Leads the Way in Cyber Protection for Louisiana Higher Ed,” accessed March 13, 2026, <https://www.lsu.edu/mediacenter/news/2023/03/wfl-cyber.php>.

²⁰ University of Oregon School of Computer and Data Sciences, “Teaching Security Operations Center,” accessed April 8, 2026, <https://scds.uoregon.edu/cs/cybersecurity/experiential-learning/TSOC>.

²¹ University of South Carolina Aiken, “Regional Security Operations Center (RSOC),” accessed March 13, 2026, <https://www.usca.edu/research/facilities-and-centers/rsoc>

Figure 4: Regional Security Operations Centers (RSOCs) in the U.S. as of April 2026



Created with mapchart.net

State Cyber Corps

Program Details: A state cyber corps (also referred to as a cyber reserve team, cyber response team, or civilian cyber corps) is a team of cybersecurity professionals who volunteer to provide preventive and reactive cybersecurity services to designated beneficiaries. State cyber corps operate under the authority of a state government department or agency. The teams of professionals who volunteer can come from any background as long as they apply for the program, meet minimum technical requirements, and pass the program’s vetting process. Once they officially become part of the state cyber corps program, volunteers gain access to free professional certifications and trainings, as well as a community

of professionals united by a shared mission. These programs are usually funded by new appropriations from state legislatures, but are sometimes funded through existing budgets for the state agency or guard unit in which they are housed.

Services Offered: State cyber corps typically offer services that include: (1) education and training; (2) vulnerability and risk assessments; and (3) on-call expertise, incident response, and recovery efforts. States with cyber corps have utilized them to provide cybersecurity awareness training to nonprofit organizations and schools, conduct risk assessments for government and critical infrastructure organizations, and assist in responding to cybersecurity incidents. Cyber

corps have responded to numerous cyberattacks in multiple states; however, the effectiveness of state cyber corps extends well beyond incident response. State cyber corps can provide incident post-mortems, including monitoring and detection, thereby increasing the cyber resilience of community organizations even after an attack. (See Appendix 1B for a case study on how the Wisconsin Cyber Response Team responded to a ransomware attack on a county government.)

Gap addressed: State cyber corps programs deliver high value: by fostering a culture of proactive awareness and containment, they can significantly reduce the financial burden of cyber incidents on taxpayers and state budgets. They act as a primary engine for cyber defense, delivering essential education and vulnerability remediation to fortify local infrastructure before a crisis occurs.

Furthermore, cyber corps can provide critical “surge capacity,” ensuring a state has a ready

reserve of expert talent to deploy during large-scale emergencies. State cyber corps can also address the persistent talent gap facing small- and mid-sized businesses (SMBs) and SLTT governments by cultivating a robust, homegrown workforce. Ultimately, cyber corps function as a central hub for civic engagement, bridging the gap between governmental institutions and the public through credible, community-driven technical training and shared defense.

Scale: As of March 2026, six states (Louisiana,²² Maryland,²³ Michigan,²⁴ Ohio,²⁵ Texas,²⁶ and Wisconsin²⁷) have active cyber corps programs,²⁸ which together have over 900 volunteers.²⁹ Louisiana and Maryland’s programs are run out of a unit in the State Guard, which limits participation to members of the guard, who train in a military capacity and operate under the governor’s authority. The remaining four programs are run solely as civilian volunteer programs out of state agencies, meaning they are open to non-military

²² Duncan Foote, “La. Guard Announces Stationing of the 178th Cyber Protection Team at Cyber Innovation Center in Bossier,” Louisiana National Guard, April 11, 2025, <https://geauxguard.la.gov/2025/04/11/la-guard-announces-stationing-of-the-178th-cyber-protection-team-at-cyber-innovation-center-in-bossier/>.

²³ Maryland Defense Force, “Home,” accessed March 13, 2026, <https://md.mddf.us/>.

²⁴ Michigan Department of Technology, Management & Budget, “Michigan Cyber Civilian Corps (MiC3),” accessed March 13, 2026, <https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3>.

²⁵ Ohio Cyber Reserve, “Home,” accessed March 13, 2026, <https://ohcr.ohio.gov/>.

²⁶ Texas Department of Information Resources, “Texas Volunteer Incident Response Team (VIRT),” accessed March 13, 2026, <https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/texas-volunteer-incident>.

²⁷ Wisconsin Emergency Management, “Wisconsin Cyber Response Team,” December 22, 2025, <https://wem.wi.gov/wisconsin-cyber-response-team/>.

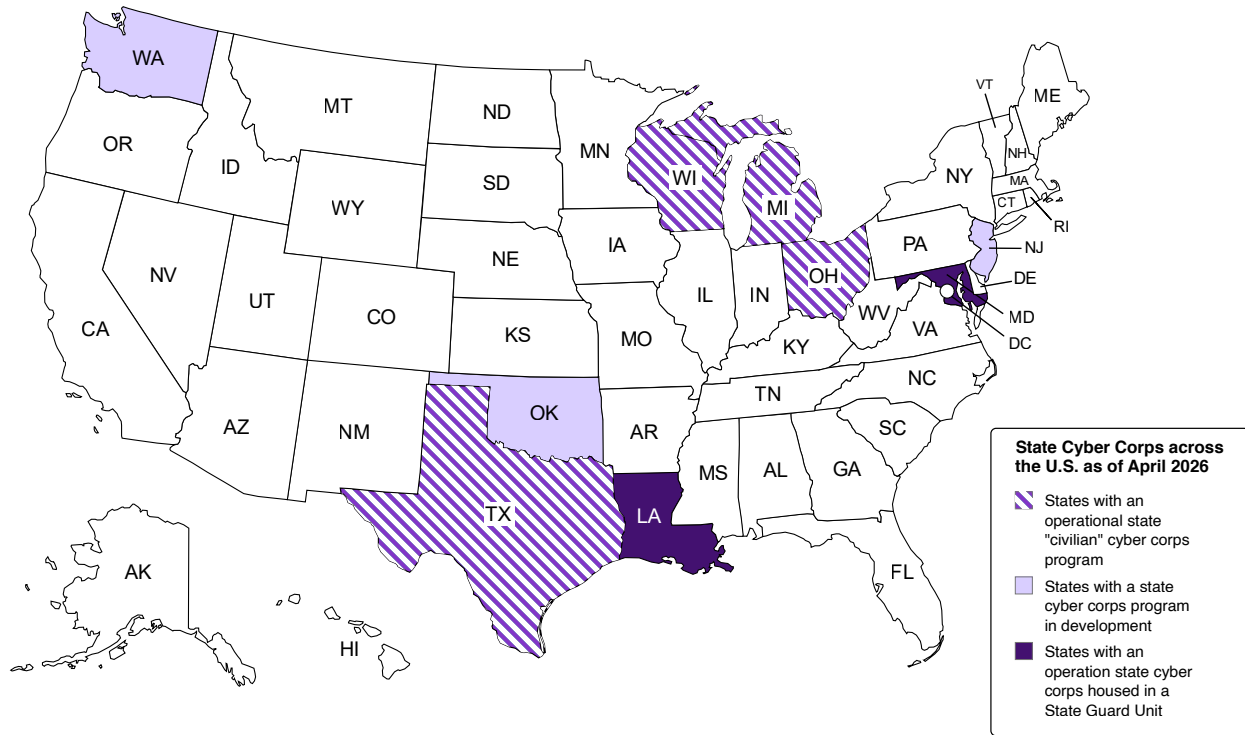
²⁸ Though not a formal cyber corps program, California’s Cybersecurity Integration Center comprises personnel from various state agencies and is tasked with sharing threat intelligence and providing incident response services.

²⁹ Michael Razeq, *Civilian Cyber Corps: A Model Law for States* (New America, 2024), <http://newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/>.

affiliated volunteers. Three states (New Jersey,³⁰ Oklahoma,³¹ and Washington³²) are in the process of forming cyber corps programs. Some states, including Maryland, currently have one type of

cyber corps program (either civilian or state guard-based), but are actively considering establishing the other type as a complementary program.³³

Figure 5: State Cyber Corps in the U.S. as of April 2026



Created with mapchart.net

³⁰ New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), "New Jersey Civilian Cyber Resilience Corps," accessed March 13, 2026, <https://www.cyber.nj.gov/grants-and-resources/new-jersey-civilian-cyber-resilience-corps>.

³¹ Oklahoma Office of Homeland Security, "Cybersecurity," accessed March 13, 2026, <https://oklahoma.gov/homeland-security/cyber-security.html>.

³² Washington Military Department, "Washington Cyber Incident Response Team (WA CIRT)," accessed March 13, 2026, <https://mil.wa.gov/washington-cyber-incident-response-team-wa-cirt>.




³³ Maryland Senate, SB 183, 2026 Reg. Sess. (introduced Jan. 14, 2026), <https://mgaleg.maryland.gov/2026RS/bills/sb/sb0183f.pdf>.

Section II: Constructing a Built-to-Last State Cyber Ecosystem

The impact of individual community cyber defense programs, like most other traditional defense models, increases when they are part of a wider defense ecosystem. To better understand the role of these programs, imagine the state and all its community organizations as an apartment, with the threat of cybersecurity attacks managed akin

to how U.S. communities commonly manage fire risk. Various tools and people are needed to help prevent fire from breaking out in the building, and if a fire does break out, there are detection and response capabilities that can be activated to reduce the damage.

Figure 6: Cyber Defense Programs as Disaster Prevention

Architectural Element	Program Equivalent	Strategic Function
 Smoke Alarms	RSOCs	Visibility: Providing early warning, situational awareness, and alerting response teams.
 The Maintenance Crew	Cybersecurity Clinics	Maintenance: Identifying structural risks and recommending repairs.
 The Fire Volunteer Department	State Cyber Corps	Incident Response + Safety Inspections: Responding to the fires and conducting proactive safety inspections.

The Smoke Detectors (RSOCs)

When the system (RSOC) detects smoke (a potential threat), it sends a signal for further action from a response team.

The Maintenance Crew (Cybersecurity Clinics)

Cybersecurity clinics serve as the proactive maintenance crew that identifies faulty electrical wiring (vulnerabilities) and recommends repairs (policies or configurations).

The Volunteer Fire Department (State Cyber Corps)

State cyber corps' role is to provide two essential public safety functions: rapid response and preventive inspection. These programs act as a specialized,

high-readiness force, sourced from local citizens who protect the structural integrity of the community.

The Proactive: Fire Marshal and Safety Inspections

Much like a fire inspector walks a building to check for blocked exits or faulty wiring, state cyber corps members conduct vulnerability and risk assessments for beneficiary organizations.

The Reactive: Incident Response Fire Engine

When the alarm sounds, perhaps triggered by the RSOCs (serving as the smoke detectors), the state cyber corps quickly deploys boots on the ground (or hands on the keyboard) to respond to and contain an incident.

Figure 7: The Community Fire Department (State Cyber Corps)

Service Type	ROI Category	Public Safety Equivalence
Training and Drills	Workforce Development	Preparing the cyber defense programs (local IT staff) to handle minor issues on their own.
Safety Inspections	Cost Savings	Reducing the “insurance premiums” (risk) by preventing a fire from starting.
Incident Response	Community Defense	Extinguishing a fire before it spreads.

The total return on investment for these programs ultimately benefits from collaboration. If alert systems (RSOCs) are funded, but there are no emergency services (state cyber corps) to respond to a fire, the building burns down. If emergency

services are funded (state cyber corps), but not the proactive maintenance crew (cybersecurity clinics), the state is constantly fighting costly and preventable fires.

Section III: Return on Investment of Cyber Defense Programs

Cyber defense programs offer a significant return on investment in terms of cost savings, workforce development, and community defense.

Figure 8: Key Benefits of Cyber Defense Programs

Saving Taxpayer Money	Workforce Development	Community Defense	Improving State Fiscal Health
A state cyber corps program can create an estimated total economic impact of \$20.1M over 4 years, yielding up to a 747% return on yearly state investment, which means for every \$1 invested, a state can receive up to \$8.47 in value per year.	A university cyber clinic program trains an average of 15 - 70 students per year. Leading states are home to several cyber clinics.	An RSOC program can monitor 22,000 devices per year, with some states' RSOCs serving 65 county governments at once.	Cyber defense programs can directly contribute to preserving or improving a state's bond rating.

Figure 9: Program Value Comparisons

Benefit	University Cyber Clinics	State Cyber Reserve Corps	Regional SOCs
Workforce Development	★ ★ ★	★	★ ★ ★
Community Defense	★ ★	★ ★ ★	★ ★
Average Yearly Operating Cost	\$300K for the first year, and \$100K/year in operating costs	\$1M/year for mature programs \$250K for small pilot programs	Unknown yearly operating costs RSOCs can cost between \$3M - \$4M to build ³⁴

³⁴ Chandler Treon, "UT Austin to Construct Regional Security Operations Center," *Industry Insider Texas*, September 12, 2024, <https://insider.govtech.com/texas/news/ut-austin-to-construct-regional-security-operations-center>.

Saving Taxpayer Money

Cyber incidents can be expensive: in 2024, the mean cost for state and local government organizations to recover from a ransomware attack was \$2.83M, more than double the previous year's average of \$1.21M.³⁵ In addition to the cost of a ransom (should an entity choose to pay), there are massive transaction costs associated with ransomware and other cyberattacks. These costs cover a wide range of actions that must be taken during incident response, including locating and coordinating parties and information, contracts and negotiations, inventory and monitoring, and compliance and enforcement.³⁶

Community cyber resilience programs have a proven return on investment for taxpayer dollars. The data collected by the authors for FY2025 indicate that a cyber corps with 200-300 volunteers, delivering approximately 100 engagements annually, can operate at a cost of between \$0.9M to \$1.2M. Operating budgets typically include salaries for a small number of full-time employees to manage the program; physical

equipment, such as laptops, blade servers, and wifi hotspots; software; and training for volunteers through existing industry certification programs or through training providers such as Hack the Box.

One state cyber corps that responded to our survey estimated that, with an annual operating budget of \$1.15M, it provided a total service value of \$20.1M over the four fiscal years between 2022-2025, including \$10.3M in incident response and \$9.9M in preventive services and hardening. These numbers point to an average return on security investment of 339% over the four years for which data is available. Money that would have been spent on costly incident recovery can instead be invested in developing local talent prepared to respond to cyber incidents. Because state civilian cyber corps' services are provided by volunteers, the costs per engagement are significantly lower. By driving down the cost per incident, these programs shift the focus from reactive spending to proactive preparation, delivering real savings to the communities they serve.

³⁵ Sophos, "The State of Ransomware in State and Local Government 2024," accessed March 13, 2026, <https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-state-and-local-government-2024>.

³⁶ Rowland Herbert-Faulkner, *The Transaction Costs of Municipal Cyber Risk Management* (UC Berkeley CLTC, 2024), <https://cltc.berkeley.edu/publication/the-transaction-costs-of-municipal-cyber-risk-management/>.

Figure 10: Comparing the Economic Value of Three State Cyber Corps Programs

FY 2025	Cyber Corps A	Cyber Corps B	Cyber Corps C
Number of engagements	125	N/A	80
Percentage of engagements from provided data that were incident response	<1%	N/A	100%
Number of volunteers	229	29	293
Annual budget	\$1,150,000	N/A	\$910,000
Hours of service	Unknown	2,421	Unknown
Program’s estimate of total service value*	\$9,739,981	\$1,540,000	\$1,460,000
Estimated value per engagement	\$77,920	N/A	\$18,250
Return on security investment	747%	N/A	60%

* The methodology for calculating the value of services varies by state, and includes savings in ransomware payments, market value of corps members’ time, and the market value of equivalent cybersecurity services.

** Cyber Corps C also conducts extensive non-incident response-related engagements; however, for benchmarking purposes, only incident response services were included in the estimates of total service value, value per engagement, and return on security investment. As a result, the program’s actual total service value and return on security investment likely far exceed the estimates presented.

Improving State Fiscal Health through Bond Rating Preservation or Improvement

State cyber corps and other cyber defense programs can improve the fiscal health of a state by providing financial returns on investment and by evidencing a strong bond rating.

A major unmitigated cyber attack can lead to a state or municipal credit downgrade. Fitch Ratings,

one of the “big three” credit rating bureaus, states in its 2025 U.S. Public Finance State Governments and Territories Rating Criteria that it “assumes state and territory leaders have the capacity to manage through the risks to which they might be exposed, including [...] cyber-attacks. Evidence of weak management in these areas may cause the rating to be lower, all other things being equal.”³⁷ In a follow-up to the release of its criteria, Fitch noted, “Recent rating actions highlight the importance of robust cyber resilience measures to withstand and

³⁷ Eric Kim and Marco Longinotti-Buitoni, *U.S. Public Finance State Governments and Territories Rating Criteria* (Fitch Ratings, 2025), <https://www.fitchratings.com/research/us-public-finance/us-public-finance-state-governments-territories-rating-criteria-04-02-2025>.

quickly recover from cyber incidents.”³⁸ A one-notch downgrade in credit rating (e.g., from AAA to AA+) can increase interest costs on state bonds by millions of dollars.

Cyber defense programs like cyber corps improve a state’s ability to manage cyber risk statewide, which can help maintain or improve a state’s bond rating. These programs function as a high-efficiency insurance layer, providing immediate value to affected organizations while simultaneously insulating the state’s economy from the “black swan” costs of unmitigated cyberattacks. In August 2025, S&P Global Ratings, one of the three major credit rating agencies, raised its long-term and underlying ratings on New Jersey’s general obligation (GO) bonds by one notch (from A to A+), explicitly citing the state’s new cybersecurity strategy as a contributing factor: “...we view the state’s cyber security support for its local governments and school districts, through the New Jersey Cybersecurity and Communication Integration Cell, as indicative of good governance and risk mitigation.”³⁹

Workforce Development

State-led cyber defense programs bolster cybersecurity and IT workforce development. They widen the pipeline of technology professionals and increase the number of skilled people

entering the cyber workforce, including in rural or underserved communities that often struggle to find talent. During the 2024-2025 academic year, 2,238 students were trained across 56 university cyber clinics (41 of which were in the United States).⁴⁰ These students provided pro bono digital security assistance to more than 700 community organizations, of which 47.5% were small critical infrastructure organizations (including utilities, state and local governments, healthcare providers, and K-12 schools), 30.4% were small businesses, and 17.3% were nonprofits. As of May 2025, Texas’s three operational RSOCs enlisted approximately 117 students.⁴¹

According to the December 2025 ISC2 Cybersecurity Workforce Study, the cybersecurity field suffers from a “shortage of skills rather than *just* people.”⁴² To help bridge that gap, the existing workforce needs to be continuously trained and upskilled. State cyber corps provide existing talent with training, community, and opportunities to build more sophisticated skillsets, all while providing service to local communities. In addition to upskilling the existing workforce, cyber defense programs can also equip students who may eventually enter fields other than cybersecurity. For example, university cybersecurity clinics often draw students from across disciplines, including both cyber-related domains and fields such as business, law, and the humanities. All students are trained to

³⁸ Gerry Glombicki and Laura Kaster, “Cyber Attack Credit Risk Reduced by Operational Resiliency, Vigilance,” *Fitch Wire*, July 1, 2025, <https://www.fitchratings.com/research/insurance/cyber-attack-credit-risk-reduced-by-operational-resiliency-vigilance-01-07-2025>.

³⁹ Oscar Padilla and Geoffrey E. Buswick, “New Jersey GO Bond Rating Raised One Notch To ‘A+,’” S&P Global Ratings, August 11, 2025, <https://www.spglobal.com/ratings/en/regulatory/article/-/view/type/HTML/id/3422456>.

⁴⁰ Matthew Nagamine, *Scaling Cybersecurity for the Public Good: Highlights from 2025* (Consortium of Cybersecurity Clinics, 2026), <https://cybersecurityclinics.org/wp-content/uploads/2026/03/TheConsortium2025Highlights.pdf>.

⁴¹ Tony Sauerhoff, *Whole of State in the Lone Star State: The Texas Regional Security Operations Centers 2.0* (Texas Department of Information Resources, 2025), https://www.nascio.org/wp-content/uploads/2025/09/TX_Cybersecurity.pdf.

⁴² ISC2, *2025 ISC2 Cybersecurity Workforce Study: Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities* (ISC2, 2025), <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>.

the same level, and while they may not all become part of the traditional cybersecurity workforce, they will enter their careers with an above-average level of cyber education and knowledge, which will ultimately benefit their future employers and the wider community by helping embed a culture of cyber hygiene.

Defense of Community Services

State-led cyber defense programs can help bolster the defense of critical community services. Because organizations such as hospitals, schools, utilities, cities, municipalities, and nonprofits provide essential services to the public, preventing disruptions to their operations is a matter of public safety.

Cyber Risk to Community Services

Demand for cybersecurity expertise and funding far exceeds supply for many community organizations, leaving their vast attack surfaces vulnerable. As of 2022, there were over 90,000 local governments in the U.S., including counties, townships, and municipal and special purpose entities.⁴³ Recent research estimates that there are more than 2.5 million nonprofits currently registered in the U.S.⁴⁴

Cyberattacks can lead to the complete loss of critical resources for residents in areas already under strain. In 2021, St. Margaret's Health, a small hospital in rural Indiana, experienced a ransomware attack that sent it into a "financial spiral," and the hospital closed in 2023, reducing or eliminating care for the region's residents.⁴⁵ Over 151 rural hospitals have closed since 2010,⁴⁶ and many rural hospitals are at risk if a cyberattack proves to be one challenge too many.

State civilian corps programs increase both the skill level and the number of boots-on-the-ground responders available to a state for deployment during an emergency. These programs can reduce the negative impacts of a cyber incident, such as financial loss and disruption of critical services.

Increased security monitoring capacity also greatly supports community defense. Student-staffed RSOC programs can expand the number of endpoints monitored. Texas's three operational RSOCs serve 65 counties in the West, Central, and Rio Grande Valley areas of Texas.⁴⁷ During the first year of operation of the RSOC at Angelo State University, more than 22,000 endpoints were monitored by 60 students.⁴⁸

⁴³ Federal Reserve Bank of St. Louis, "Local Governments in the U.S.: A Breakdown by Number and Type," accessed March 13, 2026, <https://www.stlouisfed.org/publications/regional-economist/2024/march/local-governments-us-number-type>.

⁴⁴ Indiana Nonprofits Project, "The Nonprofit Sector in the US," Indiana University, accessed March 13, 2026, <https://nonprofit.indiana.edu/our-focus/nonprofit-sector.html>.

⁴⁵ Kevin Collier, "An Illinois Hospital Is the First Health Care Facility to Link Its Closing to a Ransomware Attack," *NBC News*, June 12, 2023, <https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983>.

⁴⁶ Cecil G. Sheps Center for Health Services Research, "Rural Hospital Closures," University of North Carolina, accessed March 13, 2026, <https://www.shepscenter.unc.edu/programs-projects/rural-health/rural-hospital-closures/>.

⁴⁷ Sauerhoff, *Whole of State in the Lone Star*.

⁴⁸ Michael Wyatt, Don Topliff, and Doug Fox, "Enhancing Local Cybersecurity: Angelo State University's Leadership in Texas," National Association of Counties, February 6, 2025, <https://www.naco.org/event/enhancing-local-cybersecurity-angelo-state-universitys-leadership-texas>.

Beyond the incident response-related benefits, state-led cyber defense programs may also offer preventive services to eligible organizations, which can make them less likely to fall victim to common cyberattacks. According to a report published by the cybersecurity insurance provider Corvu, nearly 30% of ransomware attacks during the third quarter of 2024 were caused by poor

cybersecurity hygiene, such as outdated software and weak passwords.⁴⁹ Free cybersecurity training and vulnerability or risk assessment services from university cybersecurity clinics, state civilian cyber corps, or cyber command centers can help ensure organizations follow basic cybersecurity best practices, thereby reducing the risk of attack.

⁴⁹ Jason Rebholz and Ryan Bell, *Q3 Threat Report: The Ransomware Ecosystem Is Increasingly Distributed* (Corvus Insurance Holdings, 2024), <https://info.corvusinsurance.com/hubfs/ransomware%2oreports/Q3%202024%20Cyber%20Threat%20Report.pdf>.

Section IV: Best Practices of Successful Programs — and Common Barriers

Successful community cyber defense programs share common traits that enable them to mature and scale the volume and sophistication of services they provide to client organizations. At the same time, cyber defense programs may encounter hurdles that slow their progress. This section takes a bird’s-eye view of some of the hallmarks of successful cyber defense programs, as well as challenges they may face along the way.

Best Practices of Successful Programs

Successful programs, which for the purpose of this guidebook are defined as programs actively and consistently providing services, typically share the following characteristics:

1. Clearly defined authority to operate: Cyber defense programs need sufficient and clearly defined authority to carry out their work. Programs often require legal and administrative oversight to manage issues such as liability, activation, and data protection. Some can require legislative action or authorization from state agencies, such as Departments of Emergency Management or Homeland Security, or the National Guard. Michigan’s cyber civilian corps, formed in 2014, was initially unable to be fully deployed unless the governor called a state

of emergency, leaving pools of willing and able volunteers waiting for years to help. In 2018, Michigan enacted new legislation that enabled educational organizations, critical infrastructure providers, municipal agencies, and nonprofits to directly request assistance from the cyber corps.⁵⁰

2. Robust and stable funding: To operate effectively, cyber defense programs rely on predictable ongoing funding for expenses like equipment, background checks, training, and full-time program management. The cost to start up and maintain a university cyber clinic depends on faculty teachers, paid student internships, materials, enrollment, and full-time support staff or teaching assistants. Member clinics within the Consortium of Cybersecurity Clinics have estimated that \$300K is an appropriate funding target for the first year, with \$100K allocated for each year thereafter.⁵¹ Fully operational state cyber corps programs currently require, on average, a yearly operational budget of \$1 million to cover expenses.⁵²

3. Regular training to maintain and upskill talent: To keep pace with rapidly evolving threats, combat high burnout rates, and close critical skills gaps, programs need to conduct regular training and exercises. Many state cyber corps programs send volunteers to annual joint

⁵⁰ Cyber Civilian Corps Act, Mich. Pub. Act 132 of 2017 (codified at Mich. Comp. Laws §§ 18.221–18.230), <https://www.legislature.mi.gov/documents/mcl/pdf/mcl-act-132-of-2017.pdf>.

⁵¹ Sarah Powazek, *Clinic Development Toolkit* (UC Berkeley Center for Long-Term Cybersecurity, June 14, 2023), <https://cybersecurityclinics.org/wp-content/uploads/2023/06/CCDS-Clinic-Development-Toolkit-2023.pdf>.

⁵² Interviews conducted by the author with representatives from state cyber corps programs on the condition of anonymity, March 2026.

training exercises, such as the Department of War’s Cyber Shield exercise, which convenes approximately 1,000 participants, including international partners, civilians, and joint military forces.⁵³ Similar trainings also occur on the state level, where volunteers, law enforcement, state and national guard units, and industry partners run joint exercises to practice coordination and collaboration to prepare for cyber incidents.

- 4. Strong community infrastructure and management:** Keeping volunteers and staff engaged, connected, and invested increases retention. Programs that build strong interpersonal relationships create a positive feedback loop that leads participants to reinvest their time and resources. Many university cyber clinics allow standout students who successfully complete the course to return in future years as senior students or program advisors, providing a resource for advising and coaching new students, increasing program capacity, and maintaining institutional knowledge.
- 5. Trusted partnerships:** Cyber defense programs that build and maintain connective tissue with external partners from both the public and private sectors are able to leverage shared knowledge and resources. Partnerships that foster trust and repeated interactions are critical for success. For example, the Wisconsin Cyber Response team (CRT) maintains a close and mutually beneficial relationship with the University of Wisconsin-Whitewater. Through

this partnership, UW-Whitewater students and faculty can be trained by expert CRT volunteers. These trainings expose advanced cybersecurity students to the CRT’s operations, which can help them consider joining the CRT in the future.⁵⁴ In addition, the Wisconsin CRT’s enduring relationships with county officials have reinforced the team’s commitment to serving local communities as “cyber fiduciaries.”

Common Hurdles Across Programs

As they develop and grow, cyber defense programs often struggle with shared obstacles, including challenges with measuring progress, vetting volunteers, and navigating legal issues. Some of these common hurdles are detailed below.

- 1. Programs face difficulty collecting standardized metrics:** Collecting metrics helps prove the impact of cyber volunteering services and creates opportunities to learn more about the organizations they serve. Yet programs frequently struggle with measurement due to a combination of privacy and security concerns for their client beneficiaries, and because of the largely bespoke nature of the engagements themselves. At a minimum, successful programs collect data about the number of volunteers who participate and the number of engagements undertaken each year. Increased standardization and collection of metrics would be invaluable in helping support the growth of these programs.

⁵³ Samantha Hircock, “Cyber Shield 2025,” U.S. Army, June 16, 2025, https://www.army.mil/article/286378/cyber_shield_2025.

⁵⁴ Eric Franco, Roger Yin, and Balaji Sankaranarayanan, “Building Critical Statewide Cybersecurity Capabilities: The Wisconsin Model,” in *Proceedings of the 25th Annual International Conference on Digital Government Research* (New York, NY: Association for Computing Machinery, 2024), 224–31, <https://doi.org/10.1145/3657054.3657083>.

2. An efficient, standardized volunteer vetting process is needed: Vetting potential volunteers can be both time-consuming and costly. State cyber corps, for example, need to ensure that volunteers — particularly those who will be handling incident response — are technically qualified and are not a security risk. Technical assessments or certifications can be one way to assess the capabilities of volunteers, but they are imperfect measures of skill. Background checks are also frequently required, given volunteers’ potential to access sensitive data and critical infrastructure, but running checks frequently can be financially costly. Some programs have chosen to leverage existing programs and certifications that pre-vet candidates for them, with some requiring volunteers to become InfraGard members or provide a TSA Known Traveler Number as evidence of a background investigation.⁵⁵

3. Legal and liability challenges can be complicated: Legal agreements between individual volunteers, the volunteer group, and the community organizations they work with are necessary to protect all parties involved. Yet there can be significant time and financial costs associated with securing these agreements. The burden of ensuring adequate liability protection is particularly acute for volunteer groups that provide incident response support. Getting proper liability protection in place can slow a volunteer group’s response time and limit the types of volunteer organizations that can assist. Incident response is also a relatively specialized skill, with a limited number of individuals possessing the requisite level of experience to be effective. Any obstacles to enlisting and deploying the help of skilled individuals on a volunteer basis can have an outsized negative impact on community organizations in need. Creating legal agreements can be complicated, often requiring expert legal counsel; however, some basic templates do exist to help guide organizations.⁵⁶ For state cyber corps programs, extending civil liability protections to volunteers through state legislation, as was done in Michigan⁵⁷ and Texas,⁵⁸ significantly improves volunteers’ deployability.

⁵⁵ Wisconsin Emergency Management, “Wisconsin Cyber Response Team.”

⁵⁶ Mark E. Schreiber et al., *Creating a Cyber Volunteer Force: Strategy and Options* (McDermott Will & Emery, 2023), <https://www.mcdermottlaw.com/pdf/creating-a-cyber-volunteer-force-strategy-and-options/>.

⁵⁷ Cyber Civilian Corps Act, Mich. Pub. Act 132 of 2017.

⁵⁸ Act of May 31, 2021, 87th Leg., R.S., ch. 856, 2021 Tex. Gen. Laws 2111 (codified at Tex. Gov’t Code Ann. § 2054), <https://capitol.texas.gov/tlodocs/87R/billtext/pdf/SBoo475F.pdf>.

The Creation and Impact of the Wisconsin Cyber Response Team (CRT)

The Wisconsin Cyber Response Team (WI CRT) is a volunteer-based group that provides rapid incident response and cybersecurity assistance to public-sector entities across Wisconsin. The program was established in 2015 within Wisconsin Emergency Management (WEM), a division of the Wisconsin Department of Military Affairs (DMA). Unlike state cyber corps programs in other states, the WI CRT was launched without direct legislative action, with WEM using unique existing authorities to establish and operate the program.

The CRT has two tiers of “members,” both comprising individual volunteers. Tier 2 comprises general members, and is open to almost anyone with a professional interest and role in public-sector infrastructure.⁵⁹ Tier 2 members can participate in a statewide information-sharing network for notification about vulnerabilities, exploits, techniques, tactics, and procedures of threat actors. Tier 1 members are individuals who meet additional vetting criteria and can assist with incident response, fusion, assessments, or administration of the program.

The WI CRT is guided by a whole-of-community approach that engages public agencies across Wisconsin through a unified strategic plan to prepare for, mitigate, respond to, and recover from disasters. In 2025, the WI CRT had over 200 individual volunteers, with over half designated as incident responders.

Statewide Ecosystems of Cyber Defense Programs

This section highlights three unique ecosystems — in Texas, Wisconsin, and New Jersey — that combine different programs in a whole-of-state strategy for community cyber defense. Each of these states has a volunteer state cyber corps that operates in combination with other community cyber defense programs, such as a cyber clinic, RSOC, or cyber range. States that deploy cyber defense programs approach defending their communities in unique ways, but a key trend has become clear across the three states: **effective integration of cyber defense programs requires a designated coordination authority with a statutory mandate and dedicated funding.**

Texas

Texas has explicitly integrated its cyber defense programs through statute. The state has invested aggressively in cybersecurity in recent years, most recently through legislative action (HB 150)⁶⁰ taken in 2025⁶¹ establishing a \$135-million Texas Cyber Command Center in San Antonio. Texas envisions this center acting as a centralized coordination and strategy hub linking statewide cyber defense programs, including university-hosted RSOCs, cybersecurity clinics, the state cyber corps program, military cybersecurity units, and federal agencies. State officials anticipate that the center

⁵⁹ Franco, Yin, and Sankaranarayanan, “Building Critical Statewide Cybersecurity Capabilities,” 224–31.

⁶⁰ Texas House of Representatives, HB 150, 89th Leg., Reg. Sess. (2025), <https://capitol.texas.gov/BillLookup/History.aspx?LegSess=89R&Bill=HB150>.

⁶¹ Office of the Texas Governor, “Governor Abbott Signs Texas Cyber Command Into Law In San Antonio,” accessed March 13, 2026, <https://gov.texas.gov/news/post/governor-abbott-signs-texas-cyber-command-into-law-in-san-antonio>.

will create 130 jobs and be operational by late 2027 or early 2028.⁶²

RSOCs are key to Texas’s defense strategy. The state already has three operational RSOCs: Angelo State University, serving West Texas; UT Austin, serving Central Texas; and UT Rio Grande Valley, serving South Texas.⁶³ The state aims to establish 12 RSOCs in total, one for each economic region, with combined coverage across the entire state. Texas also has an operational state cyber corps program, known as the Texas Volunteer Incident Response Team (VIRT), which was previously housed in the state’s Department of Information Resources but is planned to be folded into the Texas Cyber Command Center, which will have centralized decision-making authority on how and where to deploy volunteers.⁶⁴

In addition to the state cyber corps program, Texas also maintains a State Guard Cyber Security Unit⁶⁵ and a National Guard Cyber Protection Team,⁶⁶ which conduct regular training and serve as surge support in the event of a major cyber incident. Additionally, Texas is home to two major cyber ranges — at Texas A&M and at the University of Texas San Antonio — that serve as key resources for cyber workforce development.⁶⁷

“Texas government entities will form a secure and resilient cybersecurity environment by using their resources efficiently, collaboratively, and effectively.”

— Texas 2024 - 2029 Cybersecurity Strategic Plan

⁶² Brandon Lingle and Scott Huddleston, “Gov. Abbott Signs Bill to Bring Texas Cyber Command to UTSA,” *GovTech*, June 3, 2025, <https://www.govtech.com/education/higher-ed/gov-abbott-signs-bill-to-bring-texas-cyber-command-to-utsa>.

⁶³ Rae D. DeShong, “UT Rio Grande Valley RSOC Added to Growing Statewide Network,” *Industry Insider Texas*, November 13, 2024, <https://insider.govtech.com/texas/news/ut-rio-grande-valley-rsoc-added-to-growing-statewide-network>.

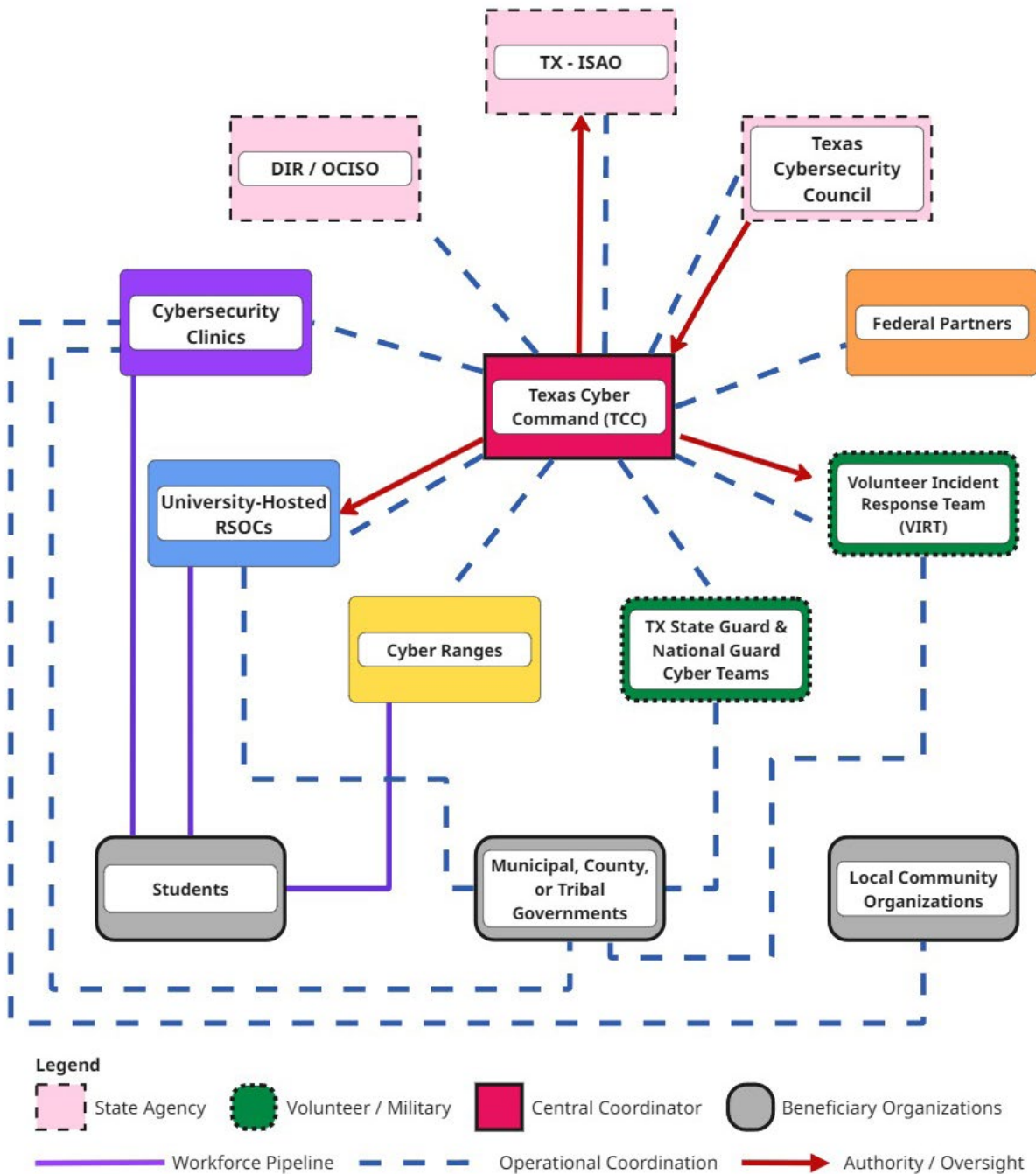
⁶⁴ Texas House of Representatives, HB 150.

⁶⁵ David Brown, “On the Front Lines of the Cyberwars: Texas State Guard Stages Virtual War Games,” Texas Military Department, October 12, 2022, <https://tmd.texas.gov/on-the-front-lines-of-the-cyberwars-texas-state-guard-stages-virtual-war-games->.

⁶⁶ Phil Fountain, “Texas Air National Guard Readies for Cyber-Protection Mission Expansion,” *National Guard*, accessed March 13, 2026, <https://www.nationalguard.mil/News/Article-View/Article/738305/texas-air-national-guard-readies-for-cyber-protection-mission-expansion/>.

⁶⁷ Texas Department of Information Resources, State of Texas Cybersecurity Strategic Plan 2024–2029 (2024), <https://dir.texas.gov/sites/default/files/2024-05/State%20of%20Texas%20Cybersecurity%20Strategic%20Plan%202024%E2%80%932029.pdf>.

Figure 11: Texas Cyber Defense Ecosystem



Wisconsin

Wisconsin is a “home rule” state, meaning that local jurisdictions are primarily responsible for handling emergencies and incidents. If their resources are depleted or near depleted, jurisdictions may

contact Wisconsin Emergency Management (WEM) for support with finding additional resources. WEM does not distribute its own resources, but rather brokers the distribution of resources from various state agencies and public-private partnership

agreements. Members of the Homeland Security Council Cyber Security Subcommittee serve as subject-matter experts for the Homeland Security Council, which in turn advises The Adjutant General, who by statute is the official Homeland Security Advisor — and cybersecurity advisor — to the Governor.

WEM is a division of the Wisconsin Department of Military Affairs. The Adjutant General is appointed by the Governor to oversee, by statute, the Wisconsin National Guard and the state's emergency management enterprise. The State of Wisconsin is divided into six Emergency Management Regions to help organize local emergency management efforts to align with the National Incident Management System and provide state liaison support to local jurisdictions for all five emergency management mission areas (prevention, mitigation, preparedness, response, and recovery). Each region has a Wisconsin Emergency Management Regional Director to lead those efforts.

The Wisconsin Cyber Response Team (CRT) is a volunteer resource administered by WEM, but it has no jurisdictional authority to take control of the management of cyber incidents. The CRT provides additional resources to support local IT and Emergency Management Directors in responding to an incident.

The Wisconsin Department of Administration's Division of Enterprise Technologies (DET) effectively serves as the state IT department. The DET is not in charge of the Wisconsin Cyber Response Team, nor does it have broad statutory authority to respond to or support cyber incidents for

local jurisdictions. The Wisconsin Department of Justice's Division of Criminal Investigations – Cyber Crimes Unit (DOJ; CCU) has statutory authority to conduct criminal investigations for computer-related and cyber crimes. The CCU supports local jurisdictional requests for criminal investigations. In that role, the Wisconsin Cyber Response Team can support the CCU in responding to local jurisdictional incidents with digital forensics analysis and incident response. The CCU also assists the CRT with training volunteers in digital forensics analysis.

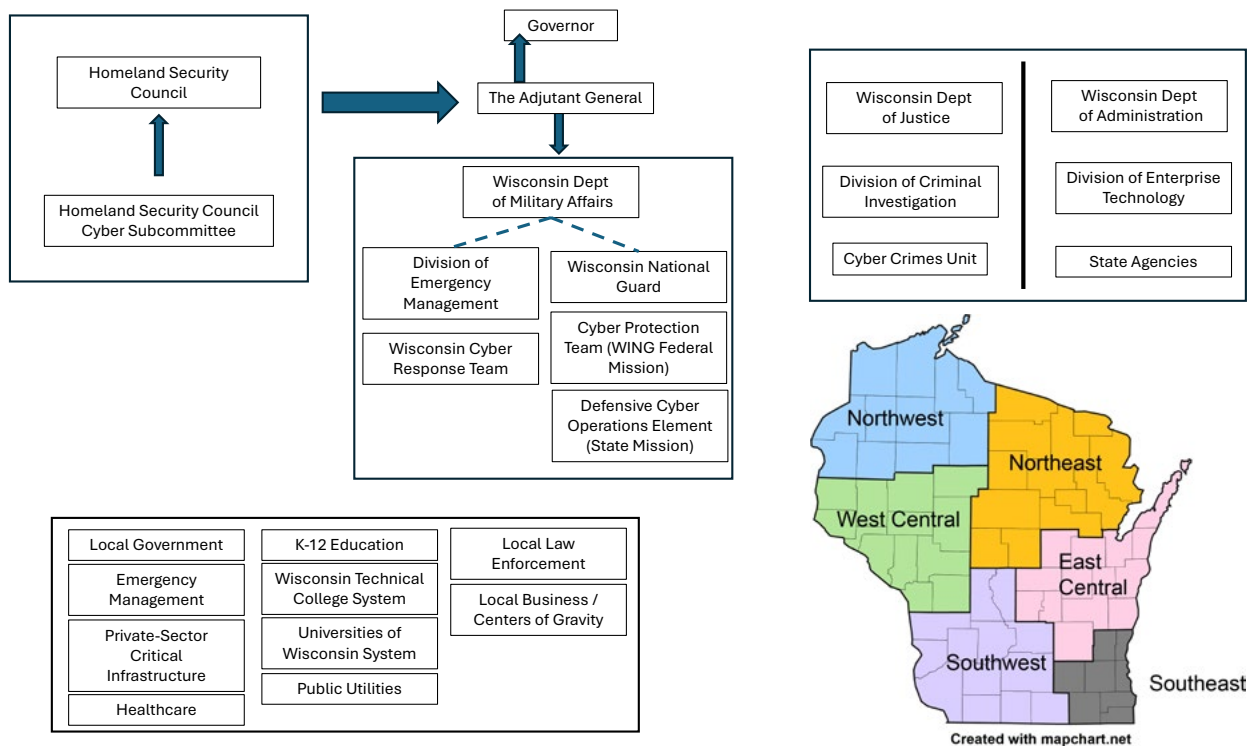
Due to changing federal cybersecurity priorities that have reduced the number of CISA regional advisors, Wisconsin Emergency Management is working to help empower local capacity to ensure the current CRT volunteer network can be leveraged to local jurisdictional advantage. In short, local governments, led by WEM and local jurisdictional centers of gravity, will begin to develop local advisory councils and continue to build locally-centered mutual aid and training support while, at the same time, the Wisconsin CRT will serve as a resource to assist local jurisdictions when requested.

“Our greatest force multiplier... is our people and our partnerships. Wisconsin has been looked at by others as the state to model because of our partnerships and connections that exist with our federal state and other states, private sector, tribal nations, schools and libraries, and local and county entities.”

— Trina Zanow, CIO of Wisconsin, quoted from a presentation at the 2025 Cyber Volunteering Day.⁶⁸

⁶⁸ Grace Menna, “Cyber Volunteers Convene in Madison, Wisconsin,” UC Berkeley Center for Long-Term Cybersecurity, November 7, 2025, <https://cltc.berkeley.edu/2025/11/07/cyber-volunteers-convene-in-madison-wisconsin/>.

Figure 12: Wisconsin Cyber Defense Ecosystem



New Jersey

New Jersey’s cybersecurity ecosystem revolves around a single institution: the New Jersey Cybersecurity and Communication Integration Cell (NJCCIC), which became the country’s first state-level cyber fusion center upon its establishment in May 2015. The NJCCIC functions as the state’s leading provider of “comprehensive active cyber defense, incident response, and continuous risk monitoring.”⁶⁹ NJCCIC is co-located at the New Jersey Regional Operations Center (NJ ROIC), which is the state’s intelligence fusion center, and is staffed by personnel from multiple state agencies, including the Office of Homeland Security and Preparedness (NJOHSP), Office of Information Technology (OIT), NJ National Guard (NJNG), Office of Emergency Management (NJ OEM), Office of Attorney General (NJ OAG), Board of

Public Utilities (NJ BPU), Department of State (NJ DOS), and NJ State Police (NJSP). This cross-agency staffing enables stronger and more effective interagency collaboration.

Kean University, located in Union, New Jersey, operates a cybersecurity clinic that provides free cybersecurity risk assessments to small businesses. The NJCCIC provides a cyber range to its partners, state agencies, and local governments. The range provides video-based training, hands-on labs, and live-fire cyberattack simulation exercises. The NJCCIC hosts regular range exercises with multiple states, state agencies, the National Guard, and students to practice for real-life events. Every year, the NJCCIC sponsors the JerseyCTF and the Garden State CTF, annual capture-the-flag competitions for students and professionals that

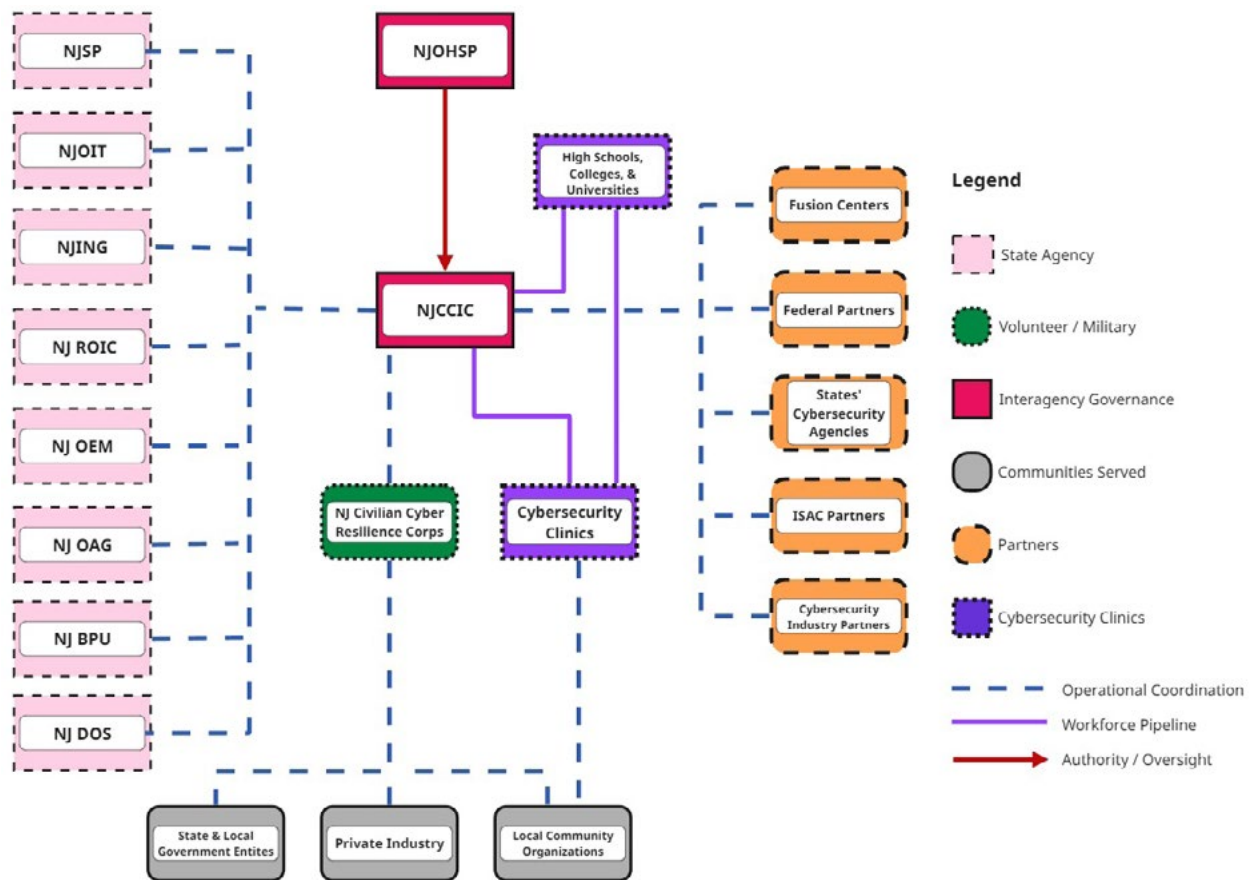
⁶⁹ New Jersey Office of Homeland Security and Preparedness, “NJOHSP Celebrates a Decade of Cyber Defense Excellence Through the NJCCIC,” May 20, 2025, <https://www.njohsp.gov/Home/Components/News/News/1701/555>.

serve as a key workforce development program. In late 2025, the state announced it was launching the New Jersey Civilian Cyber Resilience Corps, which is in development as of March 2026 and will support government, critical infrastructure, and community organizations.⁷⁰ The Cybersecurity Incident Annex to the State’s Emergency Operations Plan directs incident response and recovery efforts by leveraging resources from the NJCCIC’s federal, state, local government, and industry partners, providing surge capacity as needed.

“Integrating volunteers into NJCCIC’s operational framework significantly increases the State’s capacity to support local government entities, schools, critical infrastructure providers, and civil society organizations in preventing and responding to cybersecurity incidents.”

— Michael Geraghty, New Jersey State CISO and NJCCIC Director⁷¹

Figure 13: New Jersey Cyber Defense Ecosystem



⁷⁰ New Jersey Office of Homeland Security and Preparedness, “New Jersey Launches Civilian Cyber Resilience Corps to Strengthen Statewide Cyber Defense,” December 3, 2025, <https://www.njohsp.gov/Home/Components/News/News/1883/555>.

⁷¹ New Jersey Office of Homeland Security and Preparedness, “New Jersey Launches Civilian Cyber Resilience Corps to Strengthen Statewide Cyber Defense.”

Conclusion

Amidst increasing cyber threats and decreasing federal support, state governments are tasked with taking on more cybersecurity responsibility than ever to protect their communities. In response, states are meeting the challenge by building state-led collective cyber defense models featuring diverse programs — including cybersecurity clinics, RSOCs, and state cyber corps — that serve a three-pronged purpose: saving taxpayer money, developing a local cybersecurity workforce, and building structural cyber resilience.

Lessons learned from the development and operation of existing cyber defense programs can be applied to launch new programs more quickly and avoid potential roadblocks. While cybersecurity clinics, RSOCs, and state cyber corps yield impressive results as standalone programs, they are most impactful when part of a broader network of support, in which all levels of cybersecurity talent are deployed when and where they are needed most. **States that weave multiple types of**

programs together benefit from diversifying the unique strengths and limitations of each type of program.

Some states are already working to establish a mature ecosystem of cyber defense programs to ensure that community organizations that provide essential services to the public can access necessary cybersecurity assistance. These programs, combined with other key state infrastructure and programs — such as shared state-led centralized procurement/shared services, cyber risk pools, and intelligence-sharing mechanisms and networks — fortify communities' cyber resilience as part of a whole-of-state cybersecurity strategy.

We strongly recommend that state leaders establish, sponsor, fund, and champion cyber defense programs as investments in their communities, and to protect citizens from the digital threats that already exist and those yet to come.

Further Action

For state leaders: Additional resources for scoping, resourcing, and starting new cyber defense programs, such as cybersecurity clinics, state cyber corps programs, and RSOCs, are included in the “Reading and Resources” section below. The resources include a model bill, relevant coalitions, toolkits, and additional research on cyber defense.

For regional defenders: Community cyber defense programs can benefit greatly from sharing best practices both within their local borders and across the country. The Cyber Resilience Corps, a national initiative that mobilizes cybersecurity

expertise to protect the digital infrastructure of high-risk organizations, maintains an interactive platform at cybervolunteers.us that aims to connect prospective cyber volunteers and community organizations.

For researchers: This paper is based on the experiences of best-in-class experts running community cyber defense programs. Future research could significantly advance this work as the programs continue to grow by comprehensively studying shared best practices and creating replicable standards for programs to meet.

Reading and Resources

Collective Cyber Defense Research

[The Roadmap to Community Cyber Defense: A Path Forward from the Cyber Resilience Corps](#)

Whitepaper report examining the structural barriers that lead to cyber insecurity among community organizations, and charting a path forward to mobilize more cyber civil defenders and protect a growing number of community organizations from cyberattacks.

[Cyber Resilience Corps Volunteer Platform](#)

Platform connecting and mapping university cyber clinics, state civilian cyber corps, and nonprofit cyber-volunteering groups across the United States.

[CyberCAN: Cybersecurity for Cities and Nonprofits](#)

Report providing guidance to help government leaders in cities more effectively support the digital security of local nonprofits.

[Measuring the size and severity of the integrated cyber attack surface across US county governments](#)

OSINT-based methodologies to measure the attack surface and assess the size and vulnerability of publicly accessible county infrastructures.

Cybersecurity Clinics

[The Consortium of Cybersecurity Clinics Toolkit](#)

Toolkit from the Consortium of Cybersecurity Clinics providing concrete advice on how to launch and sustain a cybersecurity clinic.

[Protecting Communities while Training Future Cybersecurity Professionals: Lessons from the Consortium of Cybersecurity Clinics](#)

Whitepaper exploring the role of clinical education not only in training cybersecurity professionals, but also in scaling the development of clinics to improve the security posture of critical infrastructure providers.

[Cybertrack Report: Aggregate Results & Analysis from 145 Assessments \(May 2023 - May 2025\)](#)

Results from a no-cost cybersecurity assessment program designed for Indiana local government entities, including water and wastewater facilities, to evaluate and strengthen their digital defenses.

RSOCs

[Texas RSOCs Project](#)

NASCIO briefing on the development of the Texas RSOC program.

[Arizona’s Experiential Learning Opportunities: Regional Security Operations Centers and Cybersecurity Clinics](#)

Paper examining Arizona’s approaches to experiential cybersecurity education through the establishment of regional security operations centers (RSOCs) and the Arizona Cybersecurity Clinic.

State Cyber Corps

[Civilian Cyber Corps: A Model Law for States](#)

Model legislation for starting a state civilian cyber corps.

[Building Critical Statewide Cybersecurity Capabilities: The Wisconsin Model](#)

Deep dive on Wisconsin’s state cyber corps, the Wisconsin Cyber Response Team (CRT).

[Creating a Cyber Volunteer Force: Strategy and Options March 2023](#)

Pro bono project to provide a detailed examination of existing cyber volunteer programs, including cyber volunteering models, best practices, and relevant legal issues. A sample Volunteer Agreement can be found in Appendix 3 (pp. 53–62).

[Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening Our Systems](#)

2022 Report from the National Governors’ Association outlining cyber corps programs in Michigan, Wisconsin, and Ohio.

Acknowledgments

This report would not exist without the unwavering support of Sarah Powazek, whose championship of this research never faltered from its earliest conception through to publication, and whose incisive feedback proved invaluable at every stage of its development. Sincere gratitude is also owed to Chuck Kapelke and Ann Cleaveland, whose considerable contributions were instrumental in shepherding this report through to its final published form.

This report is immeasurably enriched by the contributions of those who have long been torchbearers for state and local cyber resilience. Deep gratitude is extended to Eric Franco, Francesca Lockhart, Krista Valenzuela, Katherine Schroeder, Michael Geraghty, Ray Davidson, and others who have generously contributed their insights while choosing to remain unnamed. Thanks to Iranga Kahangama, whose thoughtful

early feedback proved foundational in shaping the intellectual framework of this report.

Additional thanks to the Cyber Resilience Corps Community, particularly members who contributed to the creation of the Roadmap to Community Cyber Defense Report published in June 2025, and representatives from state cyber corps programs who generously shared their financial impact data for this report. Without their willingness to share lessons learned from their deep, lived expertise in cybersecurity for under-resourced organizations, none of this work would be possible.

Finally, the Public Interest Cybersecurity Program at the Center for Long-Term Cybersecurity (CLTC) is generously supported by Craig Newmark Philanthropies and Okta for Good, whose championing of cybersecurity for organizations big and small enables the pursuit of research projects like this one.

Bibliography

- Cecil G. Sheps Center for Health Services Research. “Rural Hospital Closures.” University of North Carolina. Accessed March 13, 2026. <https://www.shepscenter.unc.edu/programs-projects/rural-health/rural-hospital-closures/>.
- Center for Internet Security. “Whole-of-State Security.” Accessed April 16, 2026. <https://www.cisecurity.org/whole-of-state-security>.
- Collier, Kevin. “An Illinois Hospital Is the First Health Care Facility to Link Its Closing to a Ransomware Attack.” *NBC News*, June 12, 2023. <https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983>.
- Consortium of Cybersecurity Clinics. “Home.” Accessed March 13, 2026. <https://cybersecurityclinics.org/>.
- Cybersecurity and Infrastructure Security Agency. “State and Local Cybersecurity Grant Program.” Accessed March 13, 2026. <https://www.cisa.gov/cybergrants/slcgp>.
- Cybersecurity and Infrastructure Security Agency. “Tribal Cybersecurity Grant Program.” Accessed March 13, 2026. <https://www.cisa.gov/cybergrants/tcgp>.
- DeShong, Rae D. “UT Rio Grande Valley RSOC Added to Growing Statewide Network.” *Industry Insider Texas*, November 13, 2024. <https://insider.govtech.com/texas/news/ut-rio-grande-valley-rsoc-added-to-growing-statewide-network>.
- Executive Office of the President. *Achieving Efficiency Through State and Local Preparedness*. FR Doc 2025-04973. 2025. <https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/>.
- Federal Reserve Bank of St. Louis. “Local Governments in the U.S.: A Breakdown by Number and Type.” Accessed March 13, 2026. <https://www.stlouisfed.org/publications/regional-economist/2024/march/local-governments-us-number-type>.
- Foote, Duncan. “La. Guard Announces Stationing of the 178th Cyber Protection Team at Cyber Innovation Center in Bossier.” Louisiana National Guard, April 11, 2025. <https://geauxguard.la.gov/2025/04/11/la-guard-announces-stationing-of-the-178th-cyber-protection-team-at-cyber-innovation-center-in-bossier/>.
- Fountain, Phil. “Texas Air National Guard Readies for Cyber-Protection Mission Expansion.” *National Guard*, Accessed March 13, 2026. <https://www.nationalguard.mil/News/Article-View/Article/738305/texas-air-national-guard-readies-for-cyber-protection-mission-expansion/>.
- Franco, Eric, Roger Yin, and Balaji Sankaranarayanan. “Building Critical Statewide Cybersecurity Capabilities: The Wisconsin Model.” In *Proceedings of the 25th Annual International Conference on Digital Government Research*, 224–31. dg.o ’24. New York, NY: Association for Computing Machinery, 2024. <https://doi.org/10.1145/3657054.3657083>.

- Garbarino, Andrew. *Cyber Threat Snapshot*. House Homeland Security Republicans, 2025. <https://homeland.house.gov/wp-content/uploads/2025/10/Cyber-Threat-Snapshot.pdf>.
- Glombicki, Gerry, and Laura Kaster. “Cyber Attack Credit Risk Reduced by Operational Resiliency, Vigilance.” *Fitch Wire*, July 1, 2025. <https://www.fitchratings.com/research/insurance/cyber-attack-credit-risk-reduced-by-operational-resiliency-vigilance-01-07-2025>.
- Herbert-Faulkner, Rowland. *The Transaction Costs of Municipal Cyber Risk Management*. UC Berkeley Center for Long-Term Cybersecurity, 2024. <https://cltc.berkeley.edu/publication/the-transaction-costs-of-municipal-cyber-risk-management/>.
- Hircock, Samantha. “Cyber Shield 2025.” U.S. Army, June 16, 2025. https://www.army.mil/article/286378/cyber_shield_2025.
- Indiana Nonprofits Project. “The Nonprofit Sector in the US.” Indiana University. Accessed March 13, 2026. <https://nonprofit.indiana.edu/our-focus/nonprofit-sector.html>.
- ISC2. *2025 ISC2 Cybersecurity Workforce Study: Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities*. ISC2, 2025. <https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study>.
- Kim, Eric, and Marco Longinotti-Buitoni. *U.S. Public Finance State Governments and Territories Rating Criteria*. Fitch Ratings, 2025. <https://www.fitchratings.com/research/us-public-finance/us-public-finance-state-governments-territories-rating-criteria-04-02-2025>.
- Leatherby, Drew. *IT Consolidation and Shared Services: States Seeking Economies of Scale*. NASCIO, 2006. https://www.nascio.org/wp-content/uploads/2019/11/NASCIO-Con_and_SS_Issue_Brief_0306.pdf.
- Lingle, Brandon, and Scott Huddleston. “Gov. Abbott Signs Bill to Bring Texas Cyber Command to UTSA.” *GovTech*, June 3, 2025. <https://www.govtech.com/education/higher-ed/gov-abbott-signs-bill-to-bring-texas-cyber-command-to-utsa>.
- Louisiana State University. “Louisiana Enables Cyber Protection for Higher Ed in the State Through LSU.” Accessed March 13, 2026. <https://www.lsu.edu/mediacenter/news/2023/09/wfl-soc.php>.
- Louisiana State University. “Trailblazing Partnership with Industry, State: LSU Leads the Way in Cyber Protection for Louisiana Higher Ed.” Accessed March 13, 2026. <https://www.lsu.edu/mediacenter/news/2023/03/wfl-cyber.php>.
- Maryland Defense Force. “Home.” Accessed March 13, 2026. <https://md.mddf.us/>.
- Maryland. General Assembly. Senate. *Public Safety – Maryland Cyber Reserve – Established*. SB 183. 2026 Reg. Sess. Introduced January 14, 2026. <https://mgaleg.maryland.gov/2026RS/bills/sb/sbo183f.pdf>.
- Menna, Grace. “Cyber Volunteers Convene in Madison, Wisconsin.” UC Berkeley Center for Long-Term Cybersecurity, November 7, 2025. <https://cltc.berkeley.edu/2025/11/07/cyber-volunteers-convene-in-madison-wisconsin/>.

- Michigan Department of Technology, Management & Budget. “Michigan Cyber Civilian Corps (MiC3).” Accessed March 13, 2026. <https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3>.
- Monahan, Torin, and Priscilla M. Regan. “Zones of Opacity: Data Fusion in Post-9/11 Security Organizations.” *Canadian Journal of Law and Society* 27, no. 3 (2012): 301–17. <https://doi.org/10.1017/S0829320100010528>.
- Nagamine, Matthew. *Scaling Cybersecurity for the Public Good: Highlights from 2025*. Consortium of Cybersecurity Clinics, 2026. <https://cybersecurityclinics.org/wp-content/uploads/2026/03/TheConsortium2025Highlights.pdf>.
- Nagamine, Matthew, and Nick Perematko. “Growth and Impact: Clinics Reach New Heights.” Consortium of Cybersecurity Clinics, October 1, 2025. <https://cybersecurityclinics.org/blog/growth-and-impact-clinics-reach-new-heights/>.
- New Jersey Cybersecurity and Communications Integration Cell (NJCCIC). “New Jersey Civilian Cyber Resilience Corps.” Accessed March 13, 2026. <https://www.cyber.nj.gov/grants-and-resources/new-jersey-civilian-cyber-resilience-corps>.
- New Jersey Cybersecurity and Communications Integration Cell (NJCCIC). *NJCCIC Strategic Plan 2026-2030*. 2026. <https://www.cyber.nj.gov/grants-and-resources/state-resources/njccic-strategic-plan>.
- New Jersey Office of Homeland Security and Preparedness. “New Jersey Launches Civilian Cyber Resilience Corps to Strengthen Statewide Cyber Defense.” December 3, 2025. <https://www.njohsp.gov/Home/Components/News/News/1883/555>.
- New Jersey Office of Homeland Security and Preparedness. “NJOHSP Celebrates a Decade of Cyber Defense Excellence Through the NJCCIC.” May 20, 2025. <https://www.njohsp.gov/Home/Components/News/News/1701/555>.
- Ohio Cyber Reserve. “Home.” Accessed March 13, 2026. <https://ohcr.ohio.gov/>.
- Oklahoma Office of Homeland Security. “Cybersecurity.” Accessed March 13, 2026. <https://oklahoma.gov/homeland-security/cyber-security.html>.
- Padilla, Oscar, and Geoffrey E. Buswick. “New Jersey GO Bond Rating Raised One Notch To ‘A+’.” S&P Global Ratings, August 11, 2025. <https://www.spglobal.com/ratings/en/regulatory/article/-/view/type/HTML/id/3422456>.
- Pima Community College. “Governor Hobbs Announces New Cybersecurity Partnership between PCC and Arizona Department of Homeland Security.” Accessed March 13, 2026. <https://www.pima.edu/news/press-releases/2025/202510-25-cybersecurity-partnership.html>.
- Powazek, Sarah. *Clinic Development Toolkit*. UC Berkeley Center for Long-Term Cybersecurity, June 14, 2023. <https://cybersecurityclinics.org/wp-content/uploads/2023/06/CCDS-Clinic-Development-Toolkit-2023.pdf>.

- Powazek, Sarah, and Shannon Pierson. *CyberCAN: Cybersecurity for Cities and Nonprofits*. UC Berkeley Center for Long-Term Cybersecurity, November 2024. <https://cltc.berkeley.edu/publication/cybercan-cybersecurity-for-cities-and-nonprofits/>.
- Razeeq, Michael. *Civilian Cyber Corps: A Model Law for States*. New America, 2024. <http://newamerica.org/future-security/reports/civilian-cyber-corps-a-model-law-for-states/>.
- Rebholz, Jason, and Ryan Bell. *Q3 Threat Report: The Ransomware Ecosystem Is Increasingly Distributed*. Corvus Insurance Holdings, 2024. <https://info.corvusinsurance.com/hubfs/ransomware%2oreports/Q3%202024%2oCyber%2oThreat%2oReport.pdf>.
- Schreiber, Mark E., Brian Long, Scott Ferber, et al. *Creating a Cyber Volunteer Force: Strategy and Options*. McDermott Will & Emery, 2023. <https://www.mcdermottlaw.com/pdf/creating-a-cyber-volunteer-force-strategy-and-options/>.
- Sophos. “The State of Ransomware in State and Local Government 2024.” Accessed March 13, 2026. <https://www.sophos.com/en-us/blog/the-state-of-ransomware-in-state-and-local-government-2024>.
- Texas. General and Special Laws of the State of Texas Passed by the 87th Legislature at the Regular Session. 87th Leg., R.S., ch. 856 (SB 475), 2021 Tex. Gen. Laws 2111. <https://capitol.texas.gov/tlodocs/87R/billtext/pdf/SBoo475F.pdf>.
- Texas Department of Information Resources. “An Overview of Regional Security Operations Centers (RSOCs) in Texas.” Accessed March 13, 2026. <https://dir.texas.gov/resource-library-item/overview-regional-security-operations-centers-rsocs-texas>.
- Texas Department of Information Resources. *State of Texas Cybersecurity Strategic Plan 2024–2029*. 2024. <https://dir.texas.gov/sites/default/files/2024-05/State%2oof%2oTexas%2oCybersecurity%2oStrategic%2oPlan%2o2024%E2%80%932029.pdf>.
- Texas Department of Information Resources. “Texas Volunteer Incident Response Team (VIRT).” Accessed March 13, 2026. <https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/texas-volunteer-incident>.
- Sauerhoff, Tony. *Whole of State in the Lone Star State: The Texas Regional Security Operations Centers 2.0*. Texas Department of Information Resources, 2025. https://www.nascio.org/wp-content/uploads/2025/09/TX_Cybersecurity.pdf.
- Treon, Chandler. “UT Austin to Construct Regional Security Operations Center.” *Industry Insider Texas*, September 12, 2024. <https://insider.govtech.com/texas/news/ut-austin-to-construct-regional-security-operations-center>.
- United States Department of Homeland Security. “Fusion Centers.” Accessed March 13, 2026. <https://www.dhs.gov/fusion-centers>.
- University of Oregon School of Computer and Data Sciences. “Teaching Security Operations Center.” Accessed April 8, 2026. <https://scds.uoregon.edu/cs/cybersecurity/experiential-learning/TSOC>.

University of South Carolina Aiken. “Regional Security Operations Center (RSOC).” Accessed March 13, 2026. <https://www.usca.edu/research/facilities-and-centers/rsoc/>.

Washington Military Department. “Washington Cyber Incident Response Team (WA CIRT).” Accessed March 13, 2026. <https://mil.wa.gov/washington-cyber-incident-response-team-wa-cirt>.

Wisconsin Emergency Management. “Wisconsin Cyber Response Team.” December 22, 2025. <https://wem.wi.gov/wisconsin-cyber-response-team/>.

Wyatt, Michael, Don Topliff, and Doug Fox. “Enhancing Local Cybersecurity: Angelo State University’s Leadership in Texas.” National Association of Counties, February 6, 2025. <https://www.naco.org/event/enhancing-local-cybersecurity-angelo-state-universitys-leadership-texas>.

Appendix 1A: Cybersecurity Clinic Case Study

The Challenge: A Municipal Water District in southern California provided critical water and wastewater treatment to nearby residents. They contacted the San Diego Cyber Clinic to strengthen their cyber defenses amid a surge in cyberattacks on water utilities and the pre-positioning of malicious actors on IT networks in critical infrastructure.

What the Cyber Clinic Did: A team of five students from the San Diego Cyber Clinic recently performed several free services for the water district, including a comprehensive cybersecurity assessment of their implementation of key protections. The students also conducted a penetration test, a phishing test, and a social engineering test to develop a holistic view of the water district's defensive abilities.

Outcomes: From these assessments, the students learned that the water district had a gap in policies they could rely on in the event of an emergency. They developed and customized this essential documentation for the water district, including an Incident Response Plan, Disaster Recovery Plan, and a Business Continuity Plan (BCP). The students also provided an overview of the results of their assessment, penetration, and phishing tests so that the water district could improve. By integrating these components, the project not only uncovered risks but also provided a roadmap for the district to enhance its resilience against cyber threats.

Appendix 1B: State Cyber Corps Case Study

What Happened?

A ransomware group attacked a Wisconsin county government, destroying the entire network infrastructure and all data backups. With the exception of a few terabytes of departmental data, the county lost a significant amount of service data.

The Cyber Corps Response

The Wisconsin Cyber Response Team, operating under the Wisconsin Department of Emergency Management, mobilized a small team of volunteers to arrive on site, assess the situation, and develop a course of action with the network owner and the cyber insurance company.

The Wisconsin Cyber Response Team (CRT) performed immediate actions to contain the attack and began obtaining random-access memory (RAM) and drive images, Kroll Artifact Parser and Extractor (KAPE) captures, and logs to preserve as much forensic data as possible. Working in collaboration with a third-party digital forensics and incident response (DFIR) vendor, remote members of the CRT continued to perform data forensics analysis to confirm the data integrity of compromised data backups, identify an attack timeline, and provide additional analytical support while the on-site team developed a support plan with the network owner and DFIR vendor.

- Given the likely scope of the county's data loss, the Wisconsin Cyber Response Team also assisted the network owner's efforts with:
- Fully implementing multi-factor authentication with a newly de-federated M365 environment, a key control in preventing unauthorized access to sensitive data;
- Migrating county users to a new domain controller and creating strong passwords, further protecting accounts from unauthorized use;
- Leveraging the inherent security of the M365 environment to leverage Microsoft SharePoint as a de facto file server for the county's departments, improving protections for sensitive data;
- Configuring CISCO High-Power switches with updated security control configurations; and
- Creating a new ESXi network infrastructure with segmented immutable backups.

Outcome

The Wisconsin Cyber Response Team continued to support the county in conducting a post-mortem analysis, including by providing an initial round of cybersecurity assessments using CISA's CSET protocol, with the intention for the network owner to further harden the network based on the assessment findings.

- Wisconsin Emergency Management officials continued to engage with the county's emergency management director to collaborate with the IT director on developing an incident response plan. This plan included a maintenance schedule, annual assessments, and training.
- Emergency management officials continued to provide awareness training for county department heads and elected officials in the form of table-top and functional exercises.
- The Wisconsin CRT performed a second round of cybersecurity assessments using the CSET protocol for additional security hardening and incident response planning.

- A two-week penetration test engagement was conducted following the second-round hardening to provide the network owner with additional findings and establish opportunities for further hardening, thereby providing reasonable assurance that the county's network conditions would establish a new security baseline.

One of the most significant outcomes of this engagement was the establishment and

development of deeper interpersonal and state-to-county relationships. The Wisconsin Cyber Response Team's enduring relationships with county officials over the "long haul" have reinforced that the team's commitment to serving local communities and serving as "cyber fiduciaries" was not hyperbole or lip service. The Wisconsin Cyber Response Team views each incident as an opportunity to serve and support entities that require a high level of cybersecurity expertise but cannot afford to invest in such resources.



Center for Long-Term Cybersecurity

cltc.berkeley.edu

@CLTCBerkeley