SALVE REGINA UNIVERSITY
PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

November 2015

STATE OF THE STATES ON CYBERSECURITY

CALIFORNIA | MARYLAND | MICHIGAN | NEW JERSEY
NEW YORK | TEXAS | VIRGINIA | WASHINGTON

FRANCESCA SPIDALIERI

SENIOR FELLOW

About the Author

Francesca Spidalieri is the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University, where she leads the Cyber Leadership Research Project and the Rhode Island Corporate Cybersecurity Initiative (RICCI). Francesca has been appointed by Governor Gina Raimondo to the Rhode Island Cybersecurity Commission, and serves also as subject-matter expert for the Potomac Institute for Policy Studies' Cyber Readiness Index Project, the Center for Internet Security's Roles & Controls Panel, and the Ponemon Institute. Her academic research and publications have focused on cyber-strategic leadership, cyber risk management, cyber education and awareness, cybersecurity workforce development, and the professionalization of the cybersecurity industry. She regularly speaks at cyber-related events nationwide and lectures on cybersecurity issues at Salve Regina University and other local organizations.

She holds a B.A. in Political Science and International Relations from the University of Milan, Italy; an M.A. in International Affairs and Security Studies from the Fletcher School at Tufts University; and has completed additional coursework in cybersecurity at the U.S. Naval War College's Center for Cyber Conflict Studies.

The author would like to thank Melissa E. Hathaway for her insights, encouragement, and collaboration, which were essential in creating this study. Special gratitude is also owed to Gabrielle Lefrancois and Myca San Miguel for providing background research and graphic support.

STATE OF THE STATES ON CYBERSECURITY

Francesca Spidalieri

Information communication technologies (ICTs), and the Internet in particular, have become critical to economic growth and social development in the 21st century. Over the last 40 years—and especially in the last 15—governments and businesses have embraced the Internet and ICTs for several reasons, including: generating income and employment; increasing productivity and efficiency; improving information-sharing; fostering e-learning; enhancing workforce skills; driving innovation; and facilitating government activities.[1] Many essential services, from the delivery of electronic payments to next-generation power grids to air traffic control systems, have become digitized and reliant on ICTs. With that trajectory, there can be little doubt that government and business reliance on the Internet will continue to increase in the years ahead. The Internet's ability to deliver positive economic growth and social progress, however, can only be sustained if its core infrastructure is accessible, available, affordable, secure, interoperable, resilient, and stable.[2]

As a result of our increased dependence on the Internet and ICTs, cybersecurity has emerged as one of the most critical issues facing governments, businesses, and individuals in the 21st century. But our reliance on this complex infrastructure has come with a price: by embracing the Internet so widely, we have exposed ourselves to a range of nefarious cyber activities by a spectrum of hackers, criminals, and terrorists from state and non-state actors. Governments and businesses alike have been victims of cyber thefts, cyber crime, and cyber disruption (e.g. denial-of-service attacks). Despite recent heightened attention and increased levels of security investments in cybersecurity, the number of cyber incidents, their associated costs, and their impact on people's lives continue to rise. As computing and communications technologies become more entrenched in the global economy and as we enter the era of the "Internet of Everything" (IoE), incentives to compromise the security of these systems will rise as well.

Against this background, it is critical to understand that the individual states of the United States, like national governments, have a responsibility to secure their critical infrastructure—including electric power grids, air traffic control systems, financial systems, and communication networks—as well as the data that has been entrusted to them by their citizens. At a minimum, states must ensure that their citizens can rely on safe and secure Internet connectivity. Indeed, much can be done at the state level to: reduce exposure to cyber risks; promote best practice security solutions to ensure the confidentiality, integrity, and availability of information assets; increase resilience; develop business continuity plans in the event of a cyber incident; and build a culture of security. The predominant method to combat cyber risks today is to pursue the latest security products, tools, and technology plans. While technology is a key component in this effort, it alone is insufficient—there must be an increased focus on educating and training users as well.[3] No matter how good any particular technology or plan may be, its efficacy is limited if it is not adopted and implemented effectively

[1] Melissa Hathaway, "Change the Conversation, Change the Venue and Change Our Future," *CIGI Governing the Internet: Chaos, Control or Consensus,* May 13, 2013, https://www.cigionline.org/publications/2013/5/change-conversation-change-venue-and-change-our-future.

[2] Melissa Hathaway, "Connected Choices: How the Internet Is Challenging Sovereign Decisions," *American Foreign policy Interests* 36, no. 5 (November 2014): 301.

[3] Francesca Spidalieri and Sean Kern, "Professionalizing Cybersecurity: A Path to Universal Standards and Status," Pell Center, August 2014, http://pellcenter.org/wp-content/uploads/2014/07/Professionalization-of-Cybersecurity-7-28-14.pdf.

by management teams and used correctly by employees who follow well-defined processes and act in a concerted way.

To this end, states should work on building partnerships with the larger security community—including federal, state, and local stakeholders—to coordinate security efforts and equip state employees with the education and training necessary to understand their specific roles and responsibilities in protecting citizens information and maintaining the highest ethical standards.

Media headlines in recent years have shown a spike in high-impact cyber incidents in U.S. states—which have attracted broad public and legislative attention—and as a result, governors in affected states have had to respond quickly to restore public trust.[4] Others have taken note and started to focus on improving their state's cybersecurity posture, finding creative ways to turn cybersecurity challenges into business opportunities, and attracting the right talent to their states. In 2011, for example, Michigan Governor Rick Snyder launched the Michigan Cyber Initiative, a blueprint for protecting Michigan's cybersecurity ecosystem and making his state a top location for the cybersecurity industry. The same year, former Maryland Governor Martin O'Malley approved the establishment of the Maryland Commission on Cybersecurity Innovation and Excellence and charged it with developing comprehensive, coordinated, and rapid response strategies to help protect the state from cyber incidents and to promote cyber innovation and job creation. Since then, six other states—California, Idaho, North Dakota, Rhode Island, Virginia, and Texas—have followed suit and established state specific cybersecurity commissions, councils, or task forces assigned with assessing cybersecurity infrastructure and activities within the state, recommending ways to enhance the resiliency of government operations, and promoting the growth of their cybersecurity industry and workforce.[5] These initiatives from Governors and states reflect the priority and urgency at which coordination, strategy, and preparation must be implemented.

This report provides a general overview of the current level of "cyber readiness" across different states in the United States and explores some of the effective mechanisms and activities at the state-level to protect infrastructure, information, and operations in both the public and private sectors, and to promote cybersecurity workforce development and business opportunities.

The assessment is based on a modified version of the Cyber Readiness Index 1.0 (CRI), a comprehensive, comparative, experience-based methodology created to evaluate a country's maturity and commitment to cybersecurity.[6] Countries around the world can use this methodology to clarify responsibility for assuring the availability, integrity, resilience, and defense of their core cyber infrastructure and its increasing connectedness. States around the U.S. can adopt many of the same cybersecurity measures and activities detailed in the CRI to prepare and defend from malicious cyber activities and secure their own cyber infrastructure. The states selected for this analysis have been chosen based on their recognition of the importance of cybersecurity, chiefly by prioritizing their state's security and development strategy and through their commitment to increasing their resilience to cyber threats. Although insufficient funding, lack of senior level engagement, increasingly sophisticated threats, and shortage of skilled talent continue to plague efforts across the United States, there are some great examples of states that have devised innovative ways to raise awareness and implement creative solutions to protect state governments and their constituencies. While this list is by no means complete, it intends to highlight leading best practices and efforts at the state level to adopt comprehensive cybersecurity policies and strategies, increase funding and education, and develop programs to attract and retain qualified talent. As more states come to recognize the importance of cybersecurity and taking a proactive approach to cyber defense, awareness, education, and workforce development, updates to this report will monitor, track, and evaluate those developments. It is also our hope that this work catalyzes additional research and efforts into the development of effective mechanisms and innovative solutions

[4] Deloitte-NASCIO, "2014 Deloitte-NASCIO Cybersecurity Study: State Governments at Risk: Time to Move Forward," Deloitte Developmental LLC, October 2014, http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf.

[5] Office of the Rhode Island Governor, "Raimondo to Promote Cybersecurity Planning, Growth," Press Releases, May 7, 2015, http://www.ri.gov/press/view/24764.

[6] Melissa Hathaway, "Cyber Readiness Index 1.0," Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2013, http://belfercenter.ksg.harvard.edu/files/cyber-readiness-index-1point0.pdf.

for states to protect their cyber assets, improve cyber resilience, and promote cyber industry growth and workforce development.

Background

National and state governments alike are praising the Internet as a catalyst of economic growth and development, and championing the benefits of fast, reliable, and affordable communications in terms of GDP growth, job creation, access to information, and ability to innovate. Few of them, however, are considering the exposure and costs of less resilient critical services, disruption of service(s), e-crime, identity theft, intellectual property theft, fraud, and other malicious cyber activities in terms of economic loss and threat to people's safety and well being.[7] As Melissa Hathaway, former cyber advisor in both the Bush and Obama Administrations, stated:

> Leaders must recognize that increased Internet connectivity can lead to economic growth, but only if that Internet connection and the devices connected to it are safe and secure. If countries, and states alike, do not invest equally in the security of the Internet—and the ICT infrastructure that underpins it—the promise of economic growth will be transformed into a tax on growth.[8]

In recent years, U.S states have faced a growing number of evolving and sophisticated cyber threats, from data breaches to tax fraud to political hacktivism. As the 2014 Deloitte-NASCIO Cybersecurity Study reports, states have been victim of a number of high-profile attacks that "have resulted in the loss of Personally Identifiable Information (PII) of million of citizens, including Social Security Numbers, payment card records, dates of birth, driver's license numbers, and tax data."[9] In addition to serving as a repository of such sensitive data about their citizens, states are also increasingly utilizing the Internet to deliver important services, to maintain critical infrastructure such as public utilities, to share information across states and federal networks, and to ensure first responders receive the data they need in crisis situations. Unfortunately, states' increased reliance on this complex infrastructure has also opened the door to a wide range of nefarious cyber activities, from cyber crimes, to cyber espionage, to data breaches, to other types of cyber incidents, targeting governments' IT facilities, networks, and systems. Moreover, although 90 percent of critical infrastructure is privately owned, state governments—under whose jurisdiction the critical infrastructure is located—are increasingly responsible for coordinating security efforts to prevent, protect, mitigate, and respond to cyber incidents, as well as fostering collaboration between the public and private sectors to minimize cyber risks. As affirmed in the Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience, such activities should be a shared responsibility between all levels of governments and the operators of critical infrastructure.[10]

While some progress has been made to increase states' cybersecurity preparedness and resilience, there is still much more work to be done to increase the maturity, readiness, and risk awareness of state governments and their agencies. The 2013 Nationwide Cyber Security Review—a joint effort between the U.S. Department of Homeland Security (DHS), the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo)—found that "states' progress in cybersecurity preparedness has not kept up with advances in cyber threats" and that there was "little progress in the overall maturity of security programs in place across state, local, tribal and territorial (SLTT) governments to defend against the attacks."[11]

[7] Melissa Hathaway et al., "Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index," Potomac Institute for Policy Studies, (forthcoming).

[8] Author's interview with Melissa Hathaway, President of the Hathaway Global Strategies LLC and Senior Advisor at the Harvard Kennedy School's Belfer Center for Science and International Affairs, June 2, 2015.

[9] Deloitte-NASCIO, "2014 Deloitte-NASCIO Cybersecurity Study."

[10] White House, "Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience," February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[11] U.S. Department of Homeland Security and Center for Internet Security, "2013 Nationwide Cyber Security Review: Summary Report," March 2014.

Moreover, while comprehensive cybersecurity legislation continues to be stalled in Congress and concerns over the increasing sophistication of threats, lack of sufficient funds to address those threats, and shortage of cybersecurity professionals represent a common challenge across state governments, some states have started to embrace cybersecurity as part of their business and technology culture. They have recognized that the traditional approach to managing security through preventive and risk-based protective measures, while important and necessary, is no longer enough. A handful of states are now leveraging state laws, regulation, standards, market incentives, and other initiatives to align state priorities with national priorities for critical infrastructure security; increase their situational awareness; lower cyber risks; improve their resilience, response, and recovery capabilities; and even turn the cybersecurity challenge into a business opportunity. Charismatic state leaders, aided by effective public-private partnerships, excellent local research and development institutions, business-friendly policies, receptive cyber ecosystems, and in some cases convenient geographical locations, have been able to find innovative ways to bolster the cybersecurity posture of their states and position themselves as leaders of a growing ‘cyber pack’ among states in the United States. This report intends to highlight some of those effective mechanisms and creative solutions that state governments have devised to take advantage of existing state assets and increase funding and education, catalyze economic growth from the cyber industry, and attract and retain qualified talent.

Some of the more common practices have been to adopt and implement security controls based on the National Institute of Standards and Technology (NIST) special publications or other well-known benchmarks, such as the International Organization for Standardization (ISO) 27001 and 27002 and the Control Objectives for Information Technology (CoBIT), which can help states protect their critical infrastructure and digital assets, assess their programs effectiveness, and identify and address weaknesses in their systems.[12] Other steps that most states have taken, although the level of engagement differs from state to state, include joining mechanisms like MS-ISAC, the National Fusion Center Association (NFCA), and the National Governors Association (NGA) among others. In particular, the MS-ISAC—the DHS designated ISAC and focal point for SLTT governments—provides 24X7 real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and support in mitigation and incident response.[13] Indeed, information sharing plays a key role in states’ ability to improve preparedness and respond to cyber incidents. Different models of cyber information sharing and integration centers have emerged in recent years to provide a vital link between governments, the private sectors, and academia. As William Pelgrin, former CEO of the Center for Internet Security and founder of the MS-ISAC, stated:

> Building trust and awareness is key for any type of information sharing partnership to succeed, as well as providing a transparent way to share information and a non-attribution, safe-haven type venue for the public and private entities to come together and exchange valuable and actionable intelligence.[14]

In the past few years, some states have even created formal or informal commissions, committees, task forces, and working groups to promote the exchange of information among key stakeholders; examine gaps in the states’ cybersecurity posture; and make important recommendations to improve the states’ preparedness, mitigation, response, and resilience capabilities. Other more advanced and aggressive solutions have included the establishment of specific state cybersecurity offices or roles with authority over the other state agencies; the use of state National Guard units to combat cyber attacks and responds to cyber incidents; the creation of dedicated Computer Emergency Response Teams (CERTs) or integration centers for information sharing; and the launch of various partnerships among industry, academia, state and federal agencies to promote cyber industry growth, attract federal funding to local universities and companies, and train a new generation of cybersecurity professionals. In addition to state-sponsored initiatives, universities and research institutions around the country are taking advantage of federal grants and scholarships to grow their cybersecurity programs and advance cyber R&D, education, and capacity building in their respective states. For example, the National Science Foundation (NSF) sponsors the CyberCorps: Scholarship for Service

[12] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity: Appendix A,” version 1.0, February 12, 2014.
[13] Multi-State Information Sharing & Analysis Center, http://msisac.cisecurity.org.
[14] Author’s interview with William Pelgrin, former CEO of the Center for Internet Security and Chair of the MS-ISAC, June 12, 2015.

(SFS), which provides funding to qualified institutions to support undergraduate and graduate students in cybersecurity and seeks innovative proposals leading to an increase in the ability of the United States higher education enterprise to produce cybersecurity professionals.[15] Moreover, DHS and the National Security Agency (NSA) jointly sponsor designated National Centers of Academic Excellence in Information Assurance Education at qualified academic institutions.[16] States that have established themselves as cybersecurity leaders in the country host many of the academic institutions that have received these types of designations, grant, and scholarships.

These and many other examples will be discussed in more details in the following pages, along with an assessment of the maturity and commitment to cybersecurity of the states leading the cyber pack in this country.

Methodology

This study summarizes the findings of current efforts by U.S. states to improve their cybersecurity posture and promote the development and expansion of their cyber industry and talent pool. It seeks to identify effective approaches; review specific initiatives effectiveness in promoting information sharing and coordinated incident response; as well as highlight more creative solutions to promote cyber industry growth. The findings are based on open source data and extensive interviews with state representatives, including state Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs), to highlight specific programs and initiatives. The results have been collected and organized following a modified version of the Cyber Readiness Index 1.0 (CRI).[17]

The CRI 1.0 and subsequent iterations provide an objective methodology through which each state can assess its maturity and commitment to securing its cyber infrastructure. The CRI methodology defines what it means for a country—and in this case, a state—to be cyber ready, and assesses the core components of cyber readiness across five essential elements. For the purposes of this study, these five key areas and their respective sub-elements have been adjusted to apply at the state level. The assessment of where each state stands in its maturity and commitment to cybersecurity is based on whether or not a given state has the elements listed below, and on the steps the state has taken to date on each of these five essential areas:

1. **State Cybersecurity Strategic Plan** (that would include: specific cyber threats to the state and necessary steps, programs, and initiatives that should be undertaken to address identified cyber threats and increase resilience; competent authority—the responsible and accountable entity—that ensures the implementation and execution of the plan, and the adoption of well-established standards and policies; annual threat assessment to government agencies and critical infrastructure networks; adoption of well-known benchmarks, standards, and policies developed by nationally respected groups like NIST; and a strong linkage to the economic health of the state.[18])

2. **Incident Response** (state entity responsible for facilitating incident response in the event of a cyber incident—natural or man-made—that affects critical services and information infrastructure; published and regularly exercised incident response plan for emergencies and crisis that addresses continuity of operations and recovery mechanisms; role of the Homeland Security Advisor and integration with first responder community in the state; role of the state National Guard and/or local Fusion Center in the response to cyber incidents.)

3. **E-crime and Law Enforcement** (commitment to protect residents against cyber crime through laws, such as data breach notification law, and other regulatory governance mechanisms; established

[15] National Science Foundation, "Cyber Corps: Scholarship for Service," http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228.
[16] NSA/DHS Centers of Academic Excellence Institutions, https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.
[17] The modified version of the CRI 1.0 used to assess current levels of cyber readiness across the United States is the result of a joint research effort between Melissa Hathaway, author of the original CRI 1.0, and the author of this study, June 2015.
[18] Melissa Hathaway, "Strategic Advantage: Why you should care about cybersecurity." (Presentation at the Pell Cener Cybersecurity Lecture Series, Newport, RI, November 6, 2013.)

relationship with law enforcement officials to interdict and investigate events of fraud, crime, IP theft, privacy breach, and other cyber activities; state's ability to fight cyber crime, including training of law enforcement specialists, forensics specialists, judges, and legislators, and state law enforcement's ability to use tools at their disposal to combat cyber crime.)

4. Information Sharing (state information sharing and analysis center and/or mechanisms to enable the exchange of actionable intelligence/information between the state and critical industries; cross-sector and cross-stakeholder coordination mechanisms to address critical interdependencies, share situational awareness, and coordinate incident management; state Fusion Center's capability to collect, analyze, and disseminate timely cyber threat intelligence and information; official state platform/website available to its broader constituency to stay informed on latest cyber threats and other relevant Internet problems and possible solutions.)

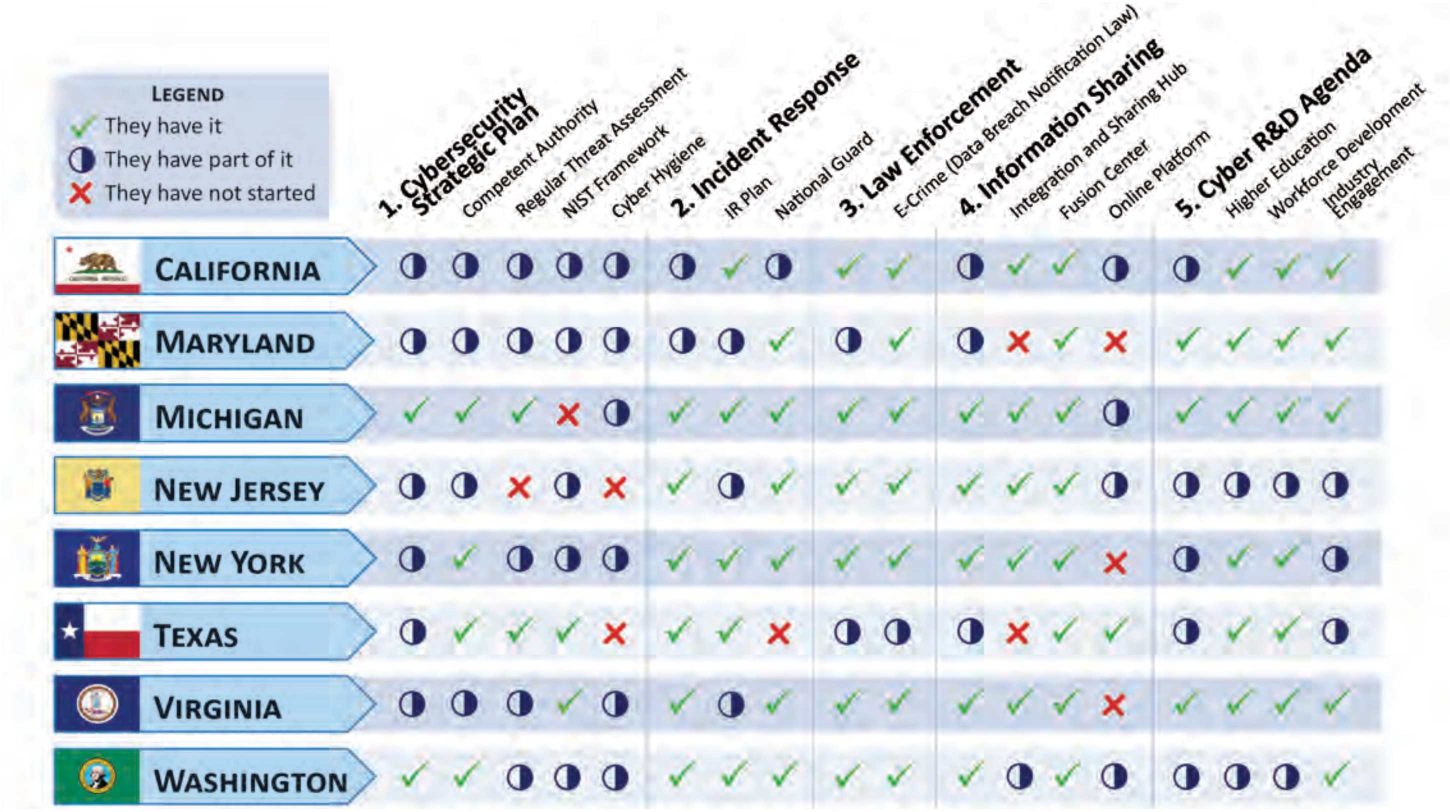
5. Cyber R&D, Education, and Capacity Building (state investments in cybesecurity research and development; funding dedicated to universities offering degree programs in cybersecurity, information security or similar programs, and to K-12 cybersecurity programs and cyber challenges; partnerships between academia, public and private sectors to promote cyber innovation; state incentives (e.g. tax credit, scholarships, funds and innovation vouchers) to encourage cybersecurity training and workforce development, and to create jobs to serve the tech industry.)

Partial credit is given to states that have established some of these initiatives, even if they are still in development, and to those that have well-established cyber-related programs not supported by the state, such as cybersecurity education and training programs in qualified academic institutions.

In addition, success stories as well as the challenges experienced by states commissions or councils created to guide the development of state-specific cybersecurity strategies and policies will be discussed and compared.

State of the States on Cybersecurity

Current levels of cyber readiness among the U.S. states leading the "cyber pack"



Legend
✓ They have it
◐ They have part of it
✗ They have not started

	1. Cybersecurity Strategic Plan	Competent Authority	Regular Threat Assessment	NIST Framework	Cyber Hygiene	2. Incident Response	IR Plan	National Guard	3. Law Enforcement	E-Crime (Data Breach Notification Law)	4. Information Sharing	Integration and Sharing Hub	Fusion Center	Online Platform	5. Cyber R&D Agenda	Higher Education	Workforce Development	Industry Engagement
California	◐	◐	◐	◐	◐	◐	✓	◐	✓	✓	◐	✓	✓	◐	◐	✓	✓	✓
Maryland	◐	◐	◐	◐	◐	◐	◐	✓	◐	✓	◐	✗	✓	✗	✓	✓	✓	✓
Michigan	✓	✓	✓	✗	◐	✓	✓	✓	✓	✓	✓	✓	✓	◐	✓	✓	✓	✓
New Jersey	◐	◐	✗	◐	✗	✓	◐	✓	✓	✓	✓	✓	✓	◐	◐	◐	◐	◐
New York	◐	✓	◐	◐	◐	✓	✓	✓	✓	✓	✓	✓	✓	✗	◐	✓	✓	◐
Texas	◐	✓	✓	✓	✗	✓	✓	✗	◐	◐	◐	✗	✓	✓	◐	✓	✓	◐
Virginia	◐	◐	◐	✓	◐	✓	◐	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
Washington	✓	✓	◐	◐	◐	✓	✓	✓	✓	✓	✓	◐	✓	◐	◐	◐	◐	✓

California

Total Population: 38,802,500
Current Governor: Jerry Brown

California, the nation's most populous state, is home to Silicon Valley, a robust IT infrastructure, and some of the most well-regarded universities in the country—all of which make it a prime target for cyber attacks. Often considered the "test state" for all things cyber, California's efforts to prevent and mitigate cyber incidents remain largely decentralized and the various jurisdictions operate in silos. That being said, California has been able to improve its overall cybersecurity posture through a series of innovative solutions and various public-private partnerships.[19] In 2013, California Governor Jerry Brown announced the launch of a California Cybersecurity Task Force, the first-of-its-kind advisory workgroup composed of high-level security experts from state and local governments, universities, laboratories, major corporations, and technology companies.[20] The Task Force has been charged with advancing the state's cybersecurity and positioning California as a national leader and preferred location for cyber business, education, and research. Recently, the Governor called for the creation of a California Cybersecurity Integration Center (Cal-CSIC) and the establishment of a multi-agency Cyber Incident Response Team in order to bolster California's preparedness and responsiveness to destructive cyber attacks.

State Cybersecurity Strategic Plan & Competent Authority

The overall responsibility for the cybersecurity posture of the State of California is shared between the Governor's Office of Emergency Services (Cal OES), as a direct mission of their homeland security function, and the California Department of Technology. The California Information Security Office (CISO)—part of the Department of Technology—actively collaborates with federal, county, and city security professionals to protect the state's IT infrastructure and to provide security incident management, security policy development, risk management, security training and awareness. California is also one of the few states to require all state employees to complete annual cybersecurity training. Moreover, agency information security officers participate with the state CISO in setting security and privacy policy and developing education and training programs for the state's workforce. This novel collaborative governance model focuses authority and accountability at the cabinet agency level. CISO has also recently established an information security audit function to validate state departments' compliance with security and privacy policies, standards, and practices.

[19] NASCIO & California Department of Technology, "NASCIO 2014 State IT Recognition Awards: California Cybersecurity Task Force," May 2013: 2.
[20] Governor's Office of Emergency Services, "Cybersecurity Task Force," California Department of Technology, http://www.caloes.ca.gov/for-individuals-families/cybersecurity-task-force.

Although California has yet to publish a dedicated cybersecurity strategic plan, its State IT Strategic Plan is regularly updated and has a strong focus on cybersecurity, emergency preparedness, information security awareness, and IT workforce development.[21] In addition, the California Cybersecurity Task Force, co-chaired by both the Department of Technology and the Cal OES, has been charged, among other things, with developing a California Cybersecurity Strategy to address concerns across government, education, and critical infrastructure. As Justin Cain, Cybersecurity Task Force Coordinator, explained:

> The Task Force is made up of seven subcommittees, each created to address specific objectives. Although many of their efforts are still in the incipient stages, they have been able to accomplish some of their objectives through engaging a wide-range of public-private stakeholders across the state, and are fostering a culture of cybersecurity through education, information sharing, workforce development, and economic growth.[22]

The Task Force also acts as an advisory body to the State of California Senior Administration Officials on all matters related to cybersecurity, including: areas where statewide collaboration can enhance security; emergency response; information sharing; contingency planning; development of threat preventions; remediation; response; recovery strategies; promotion of public outreach; and cybersecurity awareness programs.[23]

Incident Response

California has a comprehensive incident response plan that is both regularly updated and exercised. Cal OES is the agency responsible for facilitating incident response in the event of a cyber or physical incident that affects critical services and information infrastructure, and it works closely with the California National Guard and the Fusion Center to coordinate response and threat analysis. The Task Force Cyber Emergency Preparedness subcommittee is also involved in facilitating cyber exercises with public and private partners to examine cyber incident response and information sharing capabilities within the region.

All state agencies are required to report cyber incidents to the Department of Technology (and also to law enforcement and Cal OES depending on the severity and nature of the incidents), and follow a well-established process when breaches occur. The Office of Information Security's webpage offers detailed instruction to assist state agencies in compliance with incident response and reporting requirements, including establishing and maintaining internal incident management functions.[24] The state has also partnered with the California Military Department's Computer Network Defense team to offer security assessments for state departments on a consulting basis.[25]

Moreover, Governor Brown has recently signed an executive order that outlines ways to bolster California's preparedness and response to destructive cyber-attacks, including the creation of a California Cybersecurity Integration Center (Cal-CSIC) under Cal OES and a dedicated incident response team.[26] Cal-CSIC will act as the state's hub for incident reporting and will include representatives from state information technology, education, healthcare, and law enforcement agencies, as well as from federal agencies, like the FBI, the Department of Homeland Security and the U.S. Coast Guard. The newly announced multi-agency Cyber Incident Response Team will be responsible for coordinating cyber threat detection, reporting, and response with public and private entities across the state.

[21] California Department of Technology, "California Information Technology Strategic Plan: Delivering Results – 2015 Updates," http://www.cio.ca.gov/pdf/2015-Strategic-Plan.pdf.

[22] Author's interview with Justin Cain, Cybersecurity Coordinator for the Governor's Office of Emergency Services, September 4, 2015.

[23] NASCIO, "NASCIO 2014 State IT Recognition Awards: California Cybersecurity Task Force," 3.

[24] California Information Security Office, "Incident Management," http://www.cio.ca.gov/OIS/Government/incident.asp.

[25] Matt Williams, "State's New Procurement System Coming This Summer," *TechWire*, February 2015, https://www.techwire.net/wp-content/uploads/TW15-News_Feb_v1.pdf.

[26] California Office of the Governor Edmund G. Brown, "Governor Brown Signs Executive Order to Bolster Cybersecurity," August 31, 2015, http://gov.ca.gov/news.php?id=19082.

E-crime and Law Enforcement

California has demonstrated a strong commitment to protect its residents against cyber crimes, such as network intrusions, computer hacking, counterfeiting and piracy, theft of trade secret, theft of high tech equipment, and telecommunication fraud. Indeed, California was the first state to require data breach notifications and to establish clear courses of action for companies and state agencies to follow in the event of a data breach, including reporting any such breach to the Office of the Attorney General (if the breach involves more than 500 California residents), the State Police, and the Department of State.[27]

In 2011, California Attorney General Kamala Harris established an eCrime Unit, whose primary mission is to investigate and prosecute large-scale identity theft and technology crimes.[28] In addition, the eCrime Unit engages state legislators and policymakers and provides training for judges, prosecutors, law enforcement officers, and the public on the importance of strong information-security practices and evolving technology-related crime issues. The eCrime Unit plays also a supporting role in the investigation and prosecution of cyber crimes carried out through the High Technology Theft Apprehension and Prosecution (HTTAP) Program. The HTTAP Program is managed by the California Emergency Management Agency (Cal EMA) and includes five regional high-tech task forces.[29] The HTTAP task forces partner with the private sector to help companies prevent, detect, and respond to computer-related crimes. Their highly trained professionals draw upon the expertise of private industry, academia, and government IT specialists to better serve their constituency. Moreover, the Office of the California Attorney General works closely with its Privacy Unit, as well as the California Chamber of Commerce and other cybersecurity experts at leading security companies to produce guides and recommendations on how to prevent fraud and fight cyber crime, best practices to help manage risks posed by cyber threats, and advices on developing response plans in the event of a cyber incident.[30]

Finally, the California Cybersecurity Task Force has helped establish a state-run digital forensics laboratory—the Silicon Valley Regional Computer Forensics Laboratory (SVRCFL)—to support law enforcement's digital forensics capabilities in the state.[31] While the SVRCFL provides assistance primarily to law enforcement agencies located in Silicon Valley, they may take on significant cases from other agencies as deemed appropriate. In addition to defense and incident related services, SVRCFL offers also a series of training courses for law enforcement agencies, students, forensic specialists, and other investigators.

Information Sharing

Currently, Cal OES relies heavily on the California Fusion Center and other regional partners to gather important threat information and provide actionable intelligence. The newly announced Cal-CSIC, however, will work closely with the California State Threat Assessment System and the U.S. Department of Homeland Security to facilitate more integrated information sharing and communication with local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions and non-governmental organizations.

Cyber R&D, Education, and Capacity Building

California is home to some of the best universities, research institutions, and tech companies in the nation. The job market for cybersecurity professionals is thriving, and the state is very active in supporting both private enterprises and government entities as they proactively try to prevent new cyber threats, grow the pipeline of cybersecurity professionals, and create more jobs in this field. Indeed, one of the California Cybersecurity Task Force's major objectives is to promote cybersecurity workforce development and industry

[27] State of California Department of Justice, Office of the Attorney General, "Data Security Breach Reporting," https://oag.ca.gov/ecrime/databreach/reporting.

[28] State of California Department of Justice, Office of the Attorney General, "eCrime Unit," https://oag.ca.gov/ecrime.

[29] State of California Department of Justice, Office of the Attorney General, "High Technology Theft Apprehension and Prosecution (HTTAP) Program," https://oag.ca.gov/ecrime/httap.

[30] Office of the California Attorney General, "Cybersecurity in the Golden State," https://oag.ca.gov/cybersecurity.

[31] Regional Computer Forensics Laboratory, "Silicon Valley RCFL," https://www.rcfl.gov/silicon-valley.

growth. In particular, the Workforce Development and Education Subcommittee obtained the California Human Resources Department's support to study and address cybersecurity workforce challenges within state government, and to identify the specific skill requirements for cybersecurity professionals to be employed by California state agencies. In partnership with the Economic Development Subcommittee, they are also working to strengthen the workforce pipeline across the state, connect it to industry needs, and help senior state administrators devise creative ways to improve cybersecurity education, research, and innovation.[32] There is also a singular effort to accommodate returning combat veterans in local cybersecurity training programs and provide them with educational and job opportunities whether or not their military job was cyber-related.

Although most jurisdictions still operate separately from one another, there are some great examples of public-private partnerships aiming at coordinating outreach to stakeholders around the state and aligning different efforts to make California the preferred location for cyber business, education, and research. For instance, the Task Force's Economic Development Subcommittee launched the CyberCalifornia initiative to "help further position California as a leader in cybersecurity as it relates to commerce and the Internet of Things (IoT) technology."[33] CyberCalifornia is intended to facilitate cybersecurity research and innovation in the state; educate California businesses about cybersecurity needs and resources; and connect California's robust workforce development system with the needs of employers in the state. As the Chair of this Subcommittee, Darin Andersen, explained: "CyberCalifornia was established to help 'spotlight' the work of the Task Force, with a particular emphasis on the connections between cybersecurity and economic development, and connect it to other important initiatives throughout the state."[34] CyberCalifornia will also work in conjunction with the Innovation Hub (iHub) Network, a program administered by the Governor's Office of Business and Economic Development, dedicated to facilitating cybersecurity innovation and job creation for the benefit of California's businesses and consumers. The iHubs provide an innovation platform for startup companies, economic development organizations, business groups, and venture capitalists by leveraging such assets as research parks, technology incubators, universities, and federal laboratories.

In addition to California setting the pace for other states seeking innovative ways to approach cybersecurity challenges, it also hosts some of the most advanced tech labs and well-regarded institutions of higher education, many of which offer undergraduate and graduate degrees in computer science and cybersecurity and have established dedicated research centers. The University of Southern California (USC), for instance, launched a Center for Computer Systems Security (CCSS), which focuses on the study of security technologies supporting confidentiality, integrity, resiliency, privacy, intrusion detection and response, and survivability of critical infrastructure. CCSS works closely with DETER—the Cyber Defense Technology Experimental Research project—which operates a leading cybersecurity experimentation lab and supports research and development of next-generation cybersecurity technologies.[35] In 2011, USC was awarded a 5-year, $16-million contract from the U.S. Department of Homeland Security to further expand and improve the DETERlab testbed and provide additional research and experimental opportunities at the USC Viterbi School of Engineering's Information Sciences Institute.

Moreover, UC Berkeley, Stanford University, and San José State University are part of the Team for Research in Ubiquitous Secure Technology (TRUST), a National Science Foundation Science and Technology Center dedicated to "the development of cybersecurity science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure."[36] These and other higher education institutions in California have been able to take advantage of federal funding opportunities to enhance and expand their cybersecurity education and research programs. The California State Polytechnic University, the California State University in Sacramento, and the Naval Postgraduate School offer the highly selective NSF CyberCorps Scholarship for Service for students to

[32] Author's interview with Oliver Rosenbloom, California Governor's Office of Business and Economic Development, July 15, 2015.

[33] CyberCalifornia, "Mission," http://cybercalifornia.biz.

[34] Author's interview with Darin Andersen, Chairman of the California Task Force's Economic Development Subcommittee, September 4, 2015.

[35] The DETER Project, "About," http://deter-project.org/about_deter_project.

[36] Team for Research in Ubiquitous Secure Technology (TRUST), "Our Mission," https://www.truststc.org.

study cybersecurity and, along with five other academic institutions, have received designation as NSA/DHS Centers of Excellence in Information Assurance Education & Research.

Finally, the California Office of Information Security, the College of Engineering and Computer Science, and the College of Continuing Education at Sacramento State have partnered to deliver an Information Security Leadership Academy Certificate Program to state and local government employees in the information security field that want to upgrade their skills and ensure that their agency's information is reliable, available, and secure.[37]

[37] California Department of Technology, "Information Leadership Academy," http://www.cio.ca.gov/OIS/Government/library/training.asp.

Maryland

Total Population: 5,976,407
Current Governor: Larry Hogan

Maryland has effectively leveraged its existing assets, proximity to the federal government, and strong leadership both at the gubernatorial and congressional delegation level to brand itself as the ‘cybersecurity epicenter’ of the country. Home to resources such the Defense Information System Agency, the National Cybersecurity Center of Excellence, the National Security Agency, U.S. Cyber Command, the University of Maryland System institutions, and various cyber incubators and start-up companies, Maryland has become a valued contributor to national cybersecurity and a trendsetter among the states leading the cyber pack. Indeed, Maryland was the first state in the country to establish a dedicated commission—the Maryland Commission on Cybersecurity Innovation and Excellence—tasked with developing comprehensive, coordinated, and rapid response strategies to proactively protect the state against cyber attacks, and promote cyber innovation and job creation. It was also the first state to create a National Cybersecurity Center of Excellence (NCCoE) to help businesses secure their data and digital infrastructure, and a Federally Funded Research and Development Center (FFRDC) exclusively dedicated to enhancing cybersecurity and protecting national information systems.

State Cybersecurity Strategic Plan & Competent Authority

The Department of Information Technology (DoIT) is responsible for developing, maintaining, and revising IT policies, procedures, and standards; providing technical assistance, advice, and recommendations to the Governor and state agencies concerning IT matters; developing and maintaining a statewide IT master plan; and adopting and enforcing standards to be used in the procurement of IT services by or on behalf of units of state government. As Maryland CIO David Garcia explained, “the state is working to solidify an enterprise model statewide. DoIT is working to modernize and provide a baseline model across Maryland executive branch agencies and become the one-stop for all commodity IT services.”[38]

Although Maryland does not have a dedicated state cybersecurity strategic plan, the DoIT website provides various cybersecurity-related information, policies, and guidelines for state agencies to follow to protect the confidentiality, integrity, and availability of state owned information. The State of Maryland Information Security Policy v.3.1, for example, lays out a comprehensive framework for stronger critical infrastructure protection, including compliance regulations, agency guidelines, risk management, and incident reporting guidance, and

[38] Author’s interview with David Garcia, Maryland Chief Information Officer, October 6, 2015.

encourages agencies to refer to NIST information security related standards and guidelines when developing their own security policies.[39] The Maryland Commission on Cybersecurity Innovation and Excellence, however, noted that "DoIT did not have a formal process in place to enforce the provisions of its information security policy" and that it should "improve guidance to help agencies address certain security issues."[40]

The statewide Information Technology Master Plan (ITMP) provides additional guidance, instructions, and a required format for state agencies to create and produce their own annual ITMP, which should include information on the cybersecurity measures taken to protect the agency's systems containing sensitive information. The FY 2016 ITMP offers a template to help state agencies with the planning, procurement, development, and use of state information technology and telecommunications systems, and allows them to operate under a common framework aligned with the state's strategic objectives.[41] The Commission had also recommended that the master plan include a cybersecurity framework based on the NIST guidelines, but their proposed bill did not pass in the state legislature.

Incident Response

All state agencies are required to report IT incidents to DoIT by completing an IT Incident reporting form, and provide as much information about the incident as possible. The Maryland Information Security Policy also includes specific incident response and disaster recovery guidance, and a requirement for all state agencies to use a common taxonomy in order to clearly communicate incidents and events throughout Maryland state government and supported agencies. Finally, another recommendation published in the Maryland Commission's 2014 report encouraged DoIT to "establish a comprehensive statewide Incident Response Process and Capabilities," but the state has yet to act upon this recommendation.

E-crime and Law Enforcement

The Maryland Commission was instrumental in proposing and supporting the passage of cybersecurity-related legislation. Although not all of the bills they recommended and endorsed moved forward, two important updates to existing laws were passed by the state legislature: (1) a law setting provisions to protect the state databases against cyber attacks and requiring that citizens be notified if there is a breach of their personal information held by state agencies (the judicial and legislative branches, however, were excluded from this bill); (2) a law expanding the identity fraud statute to include health care information and allowing for the prosecution of those type of identity theft crimes and for victim to seek restitution.[42]

Worth noting is the recent effort by the 175th Wing of the Maryland National Air Guard to build a cyber intelligence, surveillance, reconnaissance facility that would house a network warfare group and ISR squadron and help support law enforcement's efforts to combat cyber crime, a move that reflect the National Guard's expanding role in the nation's cyber defenses.[43]

Information Sharing

Although there is no formal state information sharing mechanism to enable the exchange of actionable intelligence between the state and critical industries, Maryland is an active participant in the MS-ISAC and the DoIT website offers tips and information on cyber hygiene and other cybersecurity best practices. Moreover, the Maryland Commission recommended that the state government "improve information sharing, monitoring, and countermeasures," and "fully participates in the cyber information sharing exchanges with the federal government and private companies."

[39] Maryland Department of Information Technology, "State of Maryland Information Security Policy, version 3.1" February 2013, http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf.

[40] Commission on Maryland Cybersecurity Innovation and Excellence, "Final Report: Findings and Recommendations," September 1, 2014: 24.

[41] Maryland Department of Information Technology, "Policies and Guidance," http://doit.maryland.gov/policies/Pages/default.aspx.

[42] Commission on Maryland Cybersecurity Innovation and Excellence, "Final Report," 10.

[43] Mark Pomerleau, "Maryland National Air Guard to build a New Cyber Center," *Defense Systems*, July 8, 2015, http://defensesystems.com/Articles/2015/07/08/MD-air-national-guard-cyber-center.aspx?Page=1.

Cyber R&D, Education, and Capacity Building

The state continues to effectively leverage partnerships between industry, universities, state and federal agencies, while also aggressively attracting cybersecurity companies and investments to the state. Maryland has participated in numerous large trade shows and expos, such as RSA conferences, and launched the CyberMaryland initiative to bring together entrepreneurs, investors, academics, students, enterprises, and government officials to reinforce Maryland's leadership in cybersecurity and information technology. Since its launch in 2010, the CyberMaryland initiative has helped attract nationally-recognized experts and leaders in cybersecurity, and has organized conferences, competitions, cyber hiring events, and awards celebrations designed to showcase industry innovations, connect military veterans as well as young graduates with cybersecurity jobs, recognize cyber pioneers, and groom the next generation of cyber experts.

In 2012, NIST, together with the state of Maryland and the Montgomery County, established the first National Cybersecurity Center of Excellence (NCCoE), a public-private partnership among industry, academic, and government experts to provide businesses with cybersecurity solutions based on commercially available technologies.[44] As Rear Admiral (Ret.) Michael Brown, who spearheaded the creation of this center, stated: "It took years to realize the plan for this center of excellence, but today NCCoE is probably the best example in the country of government working with world-class IT companies to tackle the cybersecurity challenge."[45] The NCCoE is also a hub for innovation and development, and serves as a testbed for users and vendors to collaborate on new ideas and technologies prior to deployment. This encourages the rapid identification, integration, and adoption of practical, standards-based cybersecurity solutions and approaches that support automated and trustworthy online activities. Furthermore, the Center launched the National Cybersecurity Excellence Partnership (NCEP) to facilitate the collaboration of U.S companies interested in joining their efforts.[46] Current partners include Cisco, Intel, McAfee, Microsoft, RSA, Symantec, and many other tech companies.

In addition, NIST recently awarded a $29 million contract to the MITRE Corporation to operate the first Federally Funded Research and Development Center (FFRDC) solely dedicated to cybersecurity, which will support the work of the NCCoE.[47] MITRE partnered with the University System Maryland (USM), including the University of Maryland, College Park (UMD), and the University of Maryland, Baltimore County (UMBC) to run this unique federal-university-private partnership and help NCCoE develop practice guides that will aid industry in more readily adopting standards-based approaches to tackle cybersecurity challenges.[48] As Adam Sedgewick, NIST senior information technology policy advisor, explained: "This first-of-its-kind partnership is allowing the NCCoE to bring in industry experts without all the constraints of the government hiring process and with a higher degree of flexibility. It also provides a highly efficient way to leverage and rapidly assemble physical resources and scientific and engineering talent, both public and private."[49] The MITRE contract, which has a maximum amount of $5 billion over the next twenty-five years, is enabling the center to expand and accelerate its efforts to develop use cases and building blocks of small vendors and providing operations management and facilities planning.[50] While federal staff provides overall management of the NCCoE, MITRE will continue to operate the FFRDC.

Moreover, Maryland has sixteen NSA/DHS Centers of Excellence in Information Assurance Education & Research—the largest concentration of academic institutions with this designation in the country—and various

[44] NCCoE & NIST, "About the Center," https://nccoe.nist.gov/about_the_center.

[45] Author's interview with Rear Admiral (Ret.) Michael A. Brown, Vice President of the Global Public Sector at RSA, July 14, 2015.

[46] NCCoE & NIST, "Partners," https://nccoe.nist.gov/partners.

[47] Federally Founded Research and Development Centers operate in the public interest and are required to be free from organizational conflicts of interest as well as bias toward any particular company, technology or product—key attributes given the NCCoE's collaborative nature.

[48] University of Maryland, "UMD Partners with MITRE on Cybersecurity Research and Development Center," October 13, 2014, http://www.umdrightnow.umd.edu/news/umd-partners-mitre-cybersecurity-research-and-development-center.

[49] Author's interview with Adam Sedgewick, NIST Senior Information Technology Policy Advisor, July 13, 2015.

[50] NIST, "NIST Awards Contract to MITRE to Support Cybersecurity Center of Excellence," September 24, 2014, http://www.nist.gov/itl/nccoe-092414.cfm.

SFS participating institutions, including the John Hopkins University Information Security Institute and the UMBC's Center for Information Security and Assurance. This is helping to develop the ecosystem necessary to promote cybersecurity innovation and job growth in the state.

Finally, former Governor Martin O'Malley approved a Cybersecurity Investment Incentive Tax Credit (CIITC), which provides a refundable income tax credit to qualified Maryland cybersecurity companies that secure investment from investors.[51] The purpose of this program is to incentivize and attract cybersecurity companies to startup in or move to Maryland, and to attract investment for them to grow, create jobs, and retain intellectual property in the state.

[51] Maryland Department of Business and Economic Development, "Cybersecurity Investment Incentive Tax Credit," http://business.maryland.gov/fund/programs-for-businesses/cyber-tax-credit.

Michigan

Total Population: 9,909,877
Current Governor: Rick Snyder

The State of Michigan has established itself as a leader among states in implementing state government cybersecurity measures and in promoting cyber industry growth. The cornerstone of Michigan's strategy to enhance cybersecurity has been its collaborative and inclusive nature and an enterprise approach to information security that allows state agencies and private and public sector organizations to work in a highly coordinated and efficient manner.[52] Its commitment to providing the highest achievable levels of cybersecurity[53] and to positioning the state to take advantage of opportunities in the growing cybersecurity industry has been further strengthened with the launch of the Michigan Cyber Initiative under the leadership of Governor Rick Snyder.[54]

State Cybersecurity Strategic Plan & Competent Authority

Michigan is the only state to have an actual Cybersecurity Strategic Plan, which establishes their vision, principles, goals and objectives. The Michigan Department of Technology, Management & Budget (DTMB) is responsible for monitoring the state IT infrastructure and coordinating state protection, prevention, response, and recovery from cyber incidents. The DTMB Director acts also as Michigan's chief information officer. Michigan was also the first state to create a chief security officer position that brings together both physical security and cybersecurity functions under a single division. The Michigan Public Services Commission, the regulatory agency for the energy and telecommunications sectors, supports the protection of the energy control systems, and helps strengthen public-private collaboration to protect critical infrastructure.[55]

Incident Response

The Michigan Cyber Disruption Response Strategy, developed by state and local government representatives and private sector experts, outlines a framework for the prevention of, protection from, response to, and

[52] State of Michigan, "Cyber Security Strategic Plan 2009," 4, https://www.michigan.gov/documents/itstrategicplan/I_Cyber_Security_Web_234559_7.pdf.
[53] "Michigan Cyber Initiative 2011: Defense and Development for Michigan Citizens, Businesses and Industry," 2011, https://www.michigan.gov/documents/cybersecurity/MichiganCyberInitiative2011_365631_7.pdf.
[54] "Michigan Cyber Initiative 2015: An Interagency Public-Private Collaboration," 2015, http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf.
[55] Michigan Public Services Commission, "About MPSC," http://www.michigan.gov/mpsc/.

recovery from a significant cyber incident. The plan is regularly exercised and includes both government agencies and private entities.[56]

The Michigan National Guard provides active support for the prevention, protection, mitigation, and response to cyber incidents, and they regularly participate in national and international cyber and emergency response exercises.

In addition, Michigan has taken a proactive approach to cyber defense and incident response with the creation of four unique entities:

- The Michigan Intelligence Operations Center (MIOC), which handles threat detection and monitoring, and works in close collaboration with local, state, and federal agencies;
- The Michigan Cyber Command Center (MC3), directed by the Michigan State Police from within the state's Emergency Operations Center. The Command is tasked with restoring computer systems, minimizing damage in response to cyber threats, and coordinating response to statewide cyber emergencies via the State Emergency Operations Center;
- The Michigan Cyber Civilian Corps, a volunteer IT force to provide additional technical assistance in the event of a governor-declared cyber emergency; and
- The Michigan Cyber Range, established in partnership with Merit Network. This state-of-the-art training, research, and testing facility provides a secure environment to test the state's cyber-response capabilities, provide exercises and collective cybersecurity training opportunities for individuals and organizations in the state, and develop and support the Cyber Civilian Corps.

As stated by Thomas MacLellan, FireEye Director of the National Homeland Security Policy and Government Affairs:

> Michigan plays also an active role in ongoing efforts to improve interstate and federal-state coordination in response and recovery operations, and is helping to develop standards for the nation in incident response (in addition to the existing DHS National Cyber Incident Response Plan).[57] Indeed, the Michigan 'Response Annex' will include all main components of a comprehensive incident response plan, with the CIO taking the lead.[58]

E-crime and Law Enforcement

The Michigan Cyber Command Center, part of the Michigan State Police, is the state's lead response to incidents with a criminal nexus and is charged with directing law enforcement operations, including investigation, mitigation, and prosecution of cyber crimes. The State Police serves as a liaison with federal law enforcement agencies, too.

Information Sharing

Many of the entities responsible for incident response play an important role in information sharing. The Michigan Intelligence Operation Center is Michigan's designated fusion center and provides a venue for local, state, and federal agencies, as well as private sector partners to share information and intelligence related to homeland security. In addition, Michigan has been a member of the MS-ISAC since 2003, and in 2006 established its own Michigan Information Sharing & Analysis Center (MI-ISAC) to offer similar services to local

[56] "Michigan Cyber Initiative 2015," 7.

[57] Department of Homeland Security (DHS) National Cyber Incident Response Plan (NCIRP), https://www.us-cert.gov/nccic.

[58] Author's Interview with Thomas M. MacLellan, FireEye Director of the National Homeland Security Policy and Government Affairs, June 11, 2015.

governments. The Center, led by the Office of Enterprise Security and the Michigan CISO, provides real-time intelligence on cyber threats and 24/7 coordination for cyber emergencies and incidents. Other partnerships between state governments and federal agencies and centers, such as the Michigan InfraGard and the DHS National Cybersecurity and Communication Integration Center (NCCIC),[59] provide additional forums to share sensitive cybersecurity information and coordinate national response to significant cyber incidents.

Finally, Michigan has created an award-winning website (Michigan.gov/cybersecurity) to foster the sharing of information on current cyber threats, train employees, and report cyber crime.

Cyber R&D, Education, and Capacity Building

Michigan has a long history of participation and innovation in security initiatives. In 2009, for example, Michigan participated in a proof of concept of the federal government's Einstein traffic monitoring system that was eventually turned over to the MS-ISAC.[60]

Some of Michigan's strongest assets in this area are its leading research universities and five NSA/DHS Centers of Excellence in Information Assurance Education & Research, including Eastern Michigan University, Ferris State University, and University of Detroit Mercy. Moreover, the Michigan Cyber Range offers hands-on workshops, exercises, and courses aligned with the National Insititute of Standards and technology's National Initiative for Cybersecurity Education (NICE) to train students, IT professionals, and even the Michigan National Guard on cybersecurity best practices.

In addition to the growing cybersecurity programs in higher education and the strong emphasis on cyber training and awareness statewide—including cybersecurity awareness training for all state employees, cyber toolkits for citizens, schools and small businesses, cyber awareness breakfasts and lunch meetings, cyber summits and in-depth technical training for security professionals—Michigan is home to numerous cybersecurity startups and companies' research and development facilities that can tap into the talented, local workforce. The Michigan Strategic Fund, managed by the Michigan Economic Development Corporation, provides multi-million dollars grants to support the entrepreneurial ecosystem in the state, including university translational research programs, tech incubators, as well as technical and business advisory groups.[61] Over 200 new tech companies were established in Michigan in 2015 as a direct outcome of these funding opportunities.

Finally, the official Michigan.gov/cybersecurity webpage provides helpful tools and information to educate citizens, businesses, and governments on the risks and best practices for cybersecurity.

[59] "National Cybersecurity and Communication Integration Center (NCCIC)," United States Computer Emergency Readiness Team, https://www.us-cert.gov/nccic.

[60] "Michigan Plans Cyber-Defense Squads, New Command Center," Government Technology, October 10, 2011, http://www.govtech.com/policy-management/Michigan-Plans-Cyber-Defense-Squads.html.

[61] Steven Arwood, "House Appropriations Subcommittee on General Government" (FY16 Michigan Strategic Fund Presentation, March 4, 2015), http://www.michiganbusiness.org/cm/Files/Collaborative_Development_Council/Meetings_Material/20150226/FY16-MSF-Budget-Presentation-House-4MAR15.pdf.

New Jersey

Total Population: 8,938,175
Current Governor: Chris Christie

In recent years, New Jersey has embarked on major information security, information sharing, knowledge management, and capability maturity modeling initiatives in order to secure the state's digital assets, ensure continuity of operations in the case of major incidents, and harness the intellectual capital of its workforce. The newly established New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), designed in the spirit of the DHS National Cybersecurity and Communications Integration Center (NCCIC) to exchange cyber threat indicators across local, state, federal, and private sector entities, is helping New Jersey to position itself toward the front of the cyber pack among states. Indeed, New Jersey is the first state to operationalize its own information sharing and analysis organization pursuant to Executive Order 13691.[62]

State Cybersecurity Strategic Plan & Competent Authority

The New Jersey Office of Homeland Security and Preparedness is the primary entity responsible for the overall cybersecurity posture of the state, while the New Jersey Office of Information Technology (OIT) is the central IT organization that oversees the technology infrastructure for the executive branch of the state government.[63] OIT is also responsible for maintaining a secure, reliable, and cost-efficient IT infrastructure, and providing business contingency planning, disaster recovery, and security policy development for all state agencies. Recently, OIT put new security controls in place that cross agency boundaries, updated and expanded statewide policies to reflect the growing sophistication of cyber threats, and increased legal and regulatory requirements for data protection.[64] In addition, OIT publishes annual reports that outline IT progress in the state, and the goals and objectives of this agency to continue to adapt to the ever-changing world of technological advancement and capability.

The state has also developed a cybersecurity framework that aligns controls and procedures with the NIST Framework, although there is no current mechanism in place to compel compliance within each state department or agency.

[62] White House, "Executive Order – Promoting Private Sector Cybersecurity Information Sharing," February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.
[63] "Overview," New Jersey Office of Information Technology, http://www.nj.gov/it/oit/over/.
[64] New Jersey Office of Information Technology, "2014 Annual Report," http://www.nj.gov/it/pdf/2014_annual_report_v4.pdf.

Finally, New Jersey has created a new position that coordinates state level cybersecurity efforts to improve security and resilience across the public and private sectors. The new Deputy Director and state's first Cyber Security Advisor, Dave Weinstein, provides a public face, contact person, and organizational lead for statewide cybersecurity efforts.[65]

Incident Response

OIT has devised clear standards, policies, and procedures to manage cyber risks, and prevent, protect from, mitigate, and respond to cyber incidents. In particular, its one-stop-shop cybersecurity website provides a list of incident management policies, reporting, and response procedures that state agencies are required to follow in the event of a cyber incident.

Moreover, there are efforts underway to transfer the reporting procedures and incident response responsibility to the newly established New Jersey Cybersecurity and Communications Integration Cell, including plans to create a NJ CERT that would be deployed as necessary. OIT personnel is already embedded in the NJCCIC to perform incident response across the executive branch.

Finally, the state has proposed to create a joint National Guard Cyber Protection Team that would utilize resources from both the New Jersey and the New York Army National Guards to counter increasing cyber threats toward the area's network and regional infrastructure. If approved, this would be one of ten Cyber Protection Teams that the U.S. Department of Defense is planning to award for states.

E-crime and Law Enforcement

Law enforcement works closely with the intelligence community, emergency management, and other state and federal agencies involved in the newly established New Jersey Cybersecurity and Communications Integration Cell to enhance the overall understanding of cyber threats to the state, share information in real-time, and provide support with the assessment and investigation of cyber crimes (see next section). NJCCIC is part of the NJ Office of Homeland Security and Preparedness and law enforcement is both physically and operationally integrated in this organization.

Information Sharing

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), established by executive order in May 2015, is designed as a "central state civilian interface for coordinating cybersecurity information sharing, performing cybersecurity threat analysis, and promoting shared and real-time situational awareness between and among the public and private sectors."[66] The center, one of the first state-level ISAO in the country, is already being hailed as one of the best examples of regional cyber threat sharing hubs facilitating public-private transfer of data on hacker's tactics—a key cyber policy priority for the White House, and most lawmakers, government officials, and trade groups alike in 2015.[67] The NJCCIC is located within the Regional Operations Intelligence Center (ROIC), which is home to the state's fusion center as well as the state emergency operations center. The NJCCIC brings together analysts and engineers from the NJ Office of Homeland Security and Preparedness, the State Police, the Office of the NJ Attorney General, the Office of Information Technology, and other state and federal agencies and peer firms to promote statewide awareness of local cyber threats and widespread adoption of cybersecurity best practices.[68] As Dave Weinstein, NJ Cyber Security Advisor, explained: "there is incredible value in combining IT security folks with law enforcement and emergency management, and integrating cybersecurity knowledge and capabilities within

[65] Brian Nussbaum, "State-Level Cyber Security Efforts: The Garden State Model," Stanford Center for Internet and Society, August 24, 2015, http://cyberlaw.stanford.edu/blog/2015/08/state-level-cyber-security-efforts-garden-state-model.

[66] Office of the Governor, "Defending New Jersey's Digital Density: Governor Christie Signs Executive Order Establishing the NJ Cybersecurity and Communications Integration Cell," Press Release, May 20, 2015, http://nj.gov/governor//news/news/552015/pdf/20150520b.pdf.

[67] Cory Bennett, "New Jersey Data Hub Could Give Christie 2016 Cyber Edge," *The Hill*, May 20, 2015, http://thehill.com/policy/cybersecurity/242722-new-jersey-cyber-hub-could-give-christie-2016-cyber-edge.

[68] New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), http://www.cyber.nj.gov.

the state's fusion center."[69] The state has also stood up an online platform to automate information sharing with specific industry sectors. The pilot program has received positive feedback from small and medium-size companies. All these efforts are aimed at reinforcing New Jersey's pro-business environment, empowering small businesses to manage cyber risk, bolstering infrastructure resiliency, and protecting privacy.

Cyber R&D, Education, and Capacity Building

OIT collaborates with other state agencies as well as federal and local government officials, private sector leaders, and universities to offer additional opportunities to train its workforce and raise awareness about cybersecurity challenges. The CIO Collaboration Council, for example, provides a venue where IT personnel from across state government can come to discuss the increasing complexities and challenges of their jobs. The Project Management User Group, initiated in 2013, has become a training ground for all state professionals seeking mastery of best practices in the disciplined oversight of IT projects. The 2014 Annual Digital Summit gave local government professionals access to information about leading-edge technology that some could get almost nowhere else. Additionally, OIT continues to partner with critically important companies such as PSE&G to build out and maintain the infrastructure needed to handle continued growth in state demand for technology. OIT has also created a Big Data Alliance, a partnership of major state public and private universities and state government, to work on best practices to handle and secure the data entrusted in them. The Alliance, which has been designated as the State's 'advanced cyber infrastructure consortium,' comprises eight universities, including Princeton and Rutgers. Moreover, the state has six NSA/DHS National Centers of Excellence in Information Assurance Education, including Princeton University, Rutgers University, and the New Jersey Institute of Technology.

Finally, the NJCCIC has recognized the crucial role that financial services play in the economic wellbeing of the state and is actively engaging in outreach to key industry partners like the Financial Services Information Sharing and Analysis Center (FS-ISAC). The two organizations have recently announced "a partnership to share and analyze cyber threat information on behalf of New Jersey's banking institutions. Under the terms of the agreement, the NJCCIC's cyber threat analysts will correlate data from various global financial institutions to identify trends, adversary tactics, and vulnerabilities."[70] This partnership represents a great example of public-private collaboration to exchange timely and important information and help banking institutions, in this case, manage their growing cyber risk profile and increase their access to real-time and actionable cyber threat data.

[69] Author's interview with Dave Weinstein, New Jersey's Cyber Security Advisor, June 30, 2015.

[70] NJ Cybersecurity & FS-ISAC, "New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) and FS-ISAC Partner to Deliver Cyber Threat Intelligence and Use of Soltra Edge at the State Level," July 8, 2015, https://www.fsisac.com/sites/default/files/news/FS-ISAC_NJCC_Pres_Release_July_8_2015FINAL.pdf.

New York

Total Population: 19,746,227
Current Governor: Andrew Cuomo

The State of New York was among the first to focus on information sharing and cross-sector cooperation to tackle both physical and cyber threats. After 9/11, the country was scrambling to safeguard its critical infrastructure, and New York state government was one of the first to recognize the need to share actionable information about cyber threats to strengthen cybersecurity across the nation's fifty states.[71] This was the idea behind the establishment of the Multi-State Information Sharing and Analysis Center (MS-ISAC) within the state government, which today is a not-for-profit organization run by the Center for Internet Security that serves as the central cybersecurity resource for the nation's state, local, territorial and tribal governments. Not only has the state carried out several other measures in the past two decades to strengthen its overall cybersecurity posture, but in 2013 Governor Andrew Cuomo established a Cyber Security Advisory Board composed of some of the world's leading experts to provide advice on developments in cybersecurity and recommend innovative, actionable policies to ensure that New York is at the forefront of public cybersecurity defense.[72] This ongoing effort works as a sounding board to discuss important and timely issues related to cybersecurity and helps shape government policy and bolster the state response to cyber threats.

State Cybersecurity Strategic Plan & Competent Authority

In 2012, the state decided to move the Office of Cyber Security and Critical Infrastructure Coordination—which used to be part of the Division of Homeland Security and Emergency Services—into a new Office of Information Technology Services (ITS), consolidating over 4,500 IT employees from nearly 50 state agencies in the process. The ITS Enterprise Information Security Office (EISO) is now responsible for protecting the state government's cybersecurity infrastructure and providing statewide coordination of policies, standards, and programs relating to cybersecurity.[73] This dedicated office oversees and coordinates various security services for state agencies, including information security governance, compliance and risk management, incident response, security monitoring and intelligence, vulnerability and threat management, penetration testing, security policy and standard development, and security training and awareness. EISO has developed partnerships with both the government and the private sector to further its objectives.

[71] Steve Towns, "The Center for Internet Security Boosts Government Cybersecurity," *Government Technology*, October 9, 2012, http://www.govtech.com/security/The-Center-for-Internet-Security-Boosts-Government-Cybersecurity-VIDEO.html.
[72] Official Website of the State of New York, "Governor Cuomo Announces Cyber Security Advisory Board," Press Release, May 10, 2013, https://www.governor.ny.gov/news/governor-cuomo-announces-cyber-security-advisory-board.
[73] NY Office of Information Technology Services, "Welcome to the NYS Enterprise Information Security Office!," https://www.its.ny.gov/welcome-nys-enterprise-information-security-office.

The acting CISO for the state of New York, Peter Bloniarz, currently heads EISO (this is a temporary arrangement as they search for a permanent lead for EISO) and is also the executive director and senior policy advisor to the Governor's Cyber Security Advisory Board. As the acting CISO is positioned within the Office of the Governor, Bloniarz can "ensure that risks (cyber, physical, financial) are approached holistically and that his voice is not 'filtered' at a lower level, thus raising the dialogue to the level of somebody who has the authority to make important decisions and compel state agencies to follow specific policies and standards."[74] As Bloniarz affirmed, a side benefit of his current dual-hat position is that he gets to "work closely with both the state CIO (responsible for the overall state's cybersecurity, not just IT) and the state leadership to create effective cybersecurity programs."[75] He is currently working with the state's CIO, Chief Risk Officer, and the Deputy Director of State Operation to develop and roll out a statewide Cyber Risk Management Initiative in cooperation with all state agencies. This program is the result of the creation of the new Chief Risk Office position—and the strong leadership of the current appointee—and of a pilot project that was spearheaded by the Governor's Office in 2014 with five state agencies. The goal of the pilot program was to assess how these agencies were managing their cybersecurity risk, what measures they had in place to protect their cyber assets, and whether they were aware of the existing security standards and policies. The program was successful for those agencies in answering those questions, and helped raise awareness about existing standards and the responsibility that each agency has in protecting its own information. This collaborative effort between the Governor's Office, the state's CIO, CISO, and Chief Risk Officer was a success, and as a result it has cemented the relationship and power structure moving forward.

In addition, ITS released its first State IT Strategic Plan in 2014. Although the Plan primarily focuses on innovation and ways to modernize the state's infrastructure, it also discusses the ITS Enterprise Information Security Strategic Plan, which is a comprehensive information security management framework based on business and risk management objectives and leverages industry standards and best practices. The security program's objectives include aligning policy, business, and technology approaches to effectively manage risks, building partnerships to further cyber education, increasing information sharing, and maintaining a skilled cyber workforce, layered controls, and effective monitoring.[76]

Finally, the state devised specific report cards designed for state agencies to conduct self-assessments and measure their compliance against specific security standards. The results are then combined to offer an aggregate overview of the state's cyber risks and better inform policies to improve the cybersecurity posture of the state based on that analysis.

Incident Response

New York has a well-established Cyber Incident Response plan that is both regularly updated and exercised.[77] The plan outlines a clear incident response and notification process, identifies specific stakeholders' roles and responsibilities within the state, and includes additional security standards and requirements for all state entities. According to the plan, the state CISO provides overall incident response coordination, and all state government entities are required to have predefined agency incident response teams at the ready, and to notify the EISO Cyber Incident Response Team (CIRT) of any cyber incident which may have a significant or severe impact on operations or security, or which involves digital forensics, to ensure proper incident response procedures, coordination, and oversight.[78]

In addition, the EISO Cyber Security Operations Center (CSOC) helps resolve incidents, collects statewide information on vulnerabilities and attacks, fosters collaboration and information sharing, and coordinates

[74] Author's interview with William Pelgrin, June 12, 2015.

[75] Author's interview with Peter Bloniarz, Acting CISO and Executive Director and Senior Policy Advisor to the Governor's Cyber Security Advisory Board, June 30, 2015.

[76] NY Office of Information Technology Services, "New York State IT Strategic Plan 2014-2017," 21, https://www.its.ny.gov/sites/default/files/documents/StrategicPlan_FINAL.pdf.

[77] NY Office of Information Technology Services, "New York State Information Technology Standard: Cyber Incident Response," March 20, 2015, http://www.its.ny.gov/sites/default/files/documents/cyber_incident_response_standard.pdf.

[78] NY Office of Information Technology Services, "Incident Reporting," https://www.its.ny.gov/incident-reporting.

some of the training activities for state agencies. Other external entities, including MS-ISAC, Internet Service Provides (ISPs), security vendors, and the FBI, may provide additional assistance with incident response, analysis, and investigation. The development structure of the CSOS is being further refined in collaboration with partners at IBM.

Finally, the state has put forward a proposal to enhance the role of the New York's National Guard and establish a Cyber Protection Team to target cybersecurity threats to the region's infrastructure and networks. This team would integrate both the New York and New Jersey Army National Guards as a cyber-resource capable of responding jointly to threats anywhere in either state.[79]

E-crime and Law Enforcement

Law enforcement plays an essential role in understanding the physical and cyber threats to the state. New York has been able to develop an effective partnership between the FBI, the local DHS investigative branch, as well as State and Local Police. When a cyber incident occurs, EISO CIRT engages—as appropriate—law enforcement, the FBI, and other interested parties. Moreover, law enforcement is able to work cooperatively with security intelligence officials from a variety of federal, state, and local agencies through the New York State Intelligence Center, and effectively and efficiently assess, prioritize, defend against, and respond to both cyber and physical threats.

On the e-crime side, the updated NYS Data Breach Notification Law sets a clear course of action for businesses to follow in the event of a data breach, including the requirement to report any such breach to the Department of State, the New York State Division of State Police, and the New York Attorney General.[80]

Information Sharing

Efforts to build trust and awareness for info-sharing date back to the late 90s, when the state first Chief Cyber Security Officer, William Pelgrin, initiated the first public-private partnership—a non-attribution, safe-haven—to provide private and public sector organizations with a trustworthy venue and transparent way to share important information and intelligence on the most pressing cyber threats. This informal partnership became the Cybersecurity Threat Intelligence Coordinating Group (CTICC), which includes members from healthcare, financial institutions, utilities, aviation, and other critical infrastructure. The group of professionals continues to meet monthly in collaboration with members of EISO, the New York State Police, and the intelligence office to facilitate valuable situational awareness and discuss interrelationships between physical and cybersecurity activities.[81]

Moreover, the creation of the New York Cyber Security Advisory Board coincided with the relocation of the New York State Intelligence Center (NYSIC)—a combined physical and cyber infrastructure security operations center—within the Center for Internet Security (CIS), a non-profit organization dedicated to enhancing cybersecurity readiness and response of the public and private sectors.[82] The center houses security intelligence experts from a variety of federal, state, and local agencies, including the Division of Military and Naval Affairs, New York State Police, and NYS Department of Homeland and Emergency Services. Putting the state's primary cybersecurity protection agency, originally created as an all-crimes fusion center, under the same roof as a leading non-profit organization (home also to the MSISAC) is a great example of a hybrid partnership that is allowing these two organizations to more effectively collect, analyze, and share cyber threat information in real-time, as well as providing a venue for state intelligence

[79] Eric Anderson, "National Guard to Provide Cybersecurity," *Times Union*, November 17, 2014, http://www.timesunion.com/business/article/National-Guard-to-provide-cybersecurity-5899638.php.

[80] New York Department of State, "Data Breach Reporting Form and Compliance Guidance for Businesses," http://www.dos.ny.gov/consumerprotection/security_breach/data_security_breach.htm.

[81] MS-ISAC, "Cyber Threat Intelligence Coordinating Group," https://msisac.cisecurity.org/partners/cticg.cfm.

[82] Official Website of the State of New York, "Governor Cuomo Announces Partnership with National Center for Internet Security to Strengthen New York's Cyber Security," Press Release, November 18, 2013, https://www.governor.ny.gov/news/governor-cuomo-announces-partnership-national-center-internet-security-strengthen-new-yorks.

officials to coordinate efforts with federal authorities to defend against and respond to cyber incidents. The NYSIC provides also cyber warnings and analysis to promote information sharing throughout all levels of government.

Cyber R&D, Education, and Capacity Building

EISO is committed to increasing cyber awareness and hygiene around the state and partners regularly with local think tanks, educational institutions, and national government agencies to provide educational resources to the wider public. EISO, for example, co-hosts the Annual New York State Cyber Security Conference—a major conference for cybersecurity education—with the NYS Forum Inc. and the University at Albany's School of Business and College of Computing and Information. It also joined forces with the Center for Internet Security and the Governors Homeland Security Advisors Council to help support and promote the National Campaign for Cyber Hygiene—a multi-year effort to create a nationwide movement towards measurable and sustainable improvements in cybersecurity.[83]

Most recently, New York launched a series of industry-specific cybersecurity roundtables around the state to "disseminate timely information about cybersecurity, learn the challenges that various sector face, and build partnerships between businesses and academia for workforce development and R&D."[84]

In addition, the state houses some of the leading research universities in the country and eight NSA/DHS National Centers of Excellence in Information Assurance Education, including the Polytechnic University, Syracuse University, and the U.S. Military Academy at West Point.

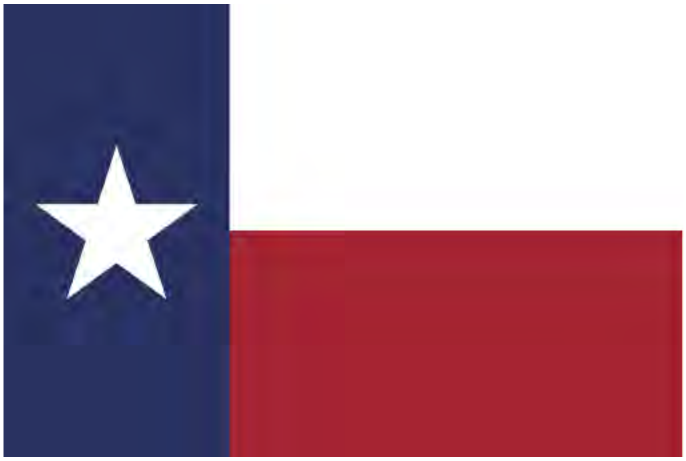
Finally, a new cross-sector Cybersecurity Workforce Alliance (CWA) launched by iQ4 in collaboration with SIFMA, the City University of NY (CUNY), NYU and various financial institutions intends to

> connect industry and education; establish virtual curricula that align cybersecurity skills, competencies, and traits of ideal college hires to industry needs; provide ways to assess students online learning; and help scale the college student workforce to improve the pipeline of cybersecurity professionals. Although the pilot program started at CUNY, NYU/Poly, and John Jay University, the CWA plans to expand its efforts to other states.[85]

[83] NY Office of Information Technology Services Enterprise Information Security Office, "Cyber Hygiene," http://www.its.ny.gov/cyber-hygiene.

[84] Author's interview with Peter Bloniarz, July 10, 2015.

[85] Author's interview with Teresa Durocher, Vice President, Information Security, Citizens Banks, June 19, 2015.



Texas

Total Population: 26,956,958
Current Governor: Greg Abbott

In 2011, the Texas Legislature authorized the creation of the Texas Cybersecurity, Education, and Economic Development Council (TCEEDC) to provide recommendations to the state leadership on how to improve the state's critical cyber infrastructure and accelerate the growth of the cybersecurity industry in the state. The Council, composed of representatives from government, academia, and industry, made several ambitious recommendations in 2012 and established a framework for statewide action on cybesecurity. Although not all of their recommendations have been implemented—at least, not as originally framed—they have helped streamline cybersecurity best practices across the state, have encouraged investments in cybersecurity programs, and have promoted collaboration and entrepreneurship within Texas' cyber environment.[86] At the conclusion of its two-year extended term, the TCEEDC is expected to prepare a status report regarding the implementation of the recommendations and the state of cybersecurity efforts in Texas.

State Cybersecurity Strategic Plan & Competent Authority

When the Council published its first report in 2012, there was not a single lead office for cybersecurity coordination of policy and response in Texas. The Council, however, recognized that the Texas Department of Information Resources (DIR) had established a strong information security program for state agencies and was capable of taking on a greater leadership role in cybersecurity, and therefore recommended that the DIR's duties and powers be expanded to enhance its efforts in leading implementation of state infrastructure improvement activities and improving the state's posture against cybersecurity incidents.[87] Since then, DIR has been granted broader authority and responsibility to oversee cybersecurity initiatives for state agencies and to promote cybersecurity awareness and training for the wider public.

The executive director of DIR was tasked with continuing the work of the Council through September 1, 2015 and designating a Cybersecurity Coordinator. While the Council had originally recommended that the state level coordinator for cybersecurity be positioned within the Governor's office to ensure that the individual had the authority "to provide a strategic direction to bring government and business leaders together as partners

[86] Author's interview with Robert Butler, Chairman of the Texas Cybersecurity, Education and Economic Council, June 2015.
[87] Texas Cybersecurity, Education, and Economic Development Council, "Building a More Secure and Prosperous Texas," December 1, 2012: 5

in securing the state's infrastructures,"[88] the position has been assigned to the state CISO, which resides at DIR. As DIR Interim Executive Director and state acting CIO, Todd Kimbriel, explains:

> This dual-hat position allows him to have centralized control and oversees both the management of statewide security programs and the coordination of Texas public-sector cybersecurity efforts. He has the authority to establish standards through the updated Texas Administrative Code and ensure that state agencies are compliant with those requirements, although Texas' distributed form of government allows them to determine how to implement those standards.[89]

As Cybersecurity Coordinator, the CISO is also responsible for bringing together both public and private sector organizations to develop and encourage wider adoption of cybersecurity best practices to protect critical state infrastructure and sensitive information. He also drives education and skill-building efforts to produce a skilled cybersecurity workforce within the state.

The DIR not only provides various security services to state agencies and higher education institutions (which allows it to be a completely self-funded agency), but it also educates agencies about security threats and prevention strategies, negotiates favorable contracts for security services and tools, and has developed a standardized, statewide Cybersecurity Framework. As current state CISO, Eddie Block, explains,

> There are several components to the Texas Cybersecurity Framework, including a revised Texas Administrative Code 202.[90] TAC 202 is the information security rule to which all Texas state agencies and institutions of higher education must adhere. Incorporated by reference in TAC 202 is a Security Control Standards Catalog, which specifies the minimum information security requirements for these organizations and is based on the NIST 800-53 Rev. 4, with some modifications for Texas.[91]

Additionally, each agency and institution of higher education is required to submit a security plan to DIR every even-numbered year and include best practices developed by the department. To facilitate that reporting, DIR has developed an objective framework with 40 controls that aligns with the NIST Cybersecurity Framework. All these efforts add up to a more structured cybersecurity governance model for the state that allows Texas to adapt and grow as needed.[92]

Finally, DIR Network Security Operation Center (NSOC) recently published its first annual threat report as part of an ongoing effort to increase communications with the over 100 government entities it serves and provide updates on the security posture of the state's shared network.[93] This report offers an aggregate overview of the cyber threats to Texas and details many of the services offered through NSOC.

Incident Response

DIR has a well-exercised incident response plan and has transformed the incident reporting process to allow up-to-the-minute, on-site reporting. Although the plan is typically not published publically, it offers a clear course of action for state agencies and institution of higher education to follow in case of a cyber incident. The plan is currently under review.

[88] Ibid: 1.

[89] Author's interview with Todd Kimbriel, DIR Interim Executive Director and state acting CIO, June 2015.

[90] Office of the Secretary of State, "Texas Administrative Code," http://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=1&pt=10&ch=202.

[91] Texas Department of Information Resources, "Security Control Standards Catalog, version 1.2," April 3, 2015. See also author's interview with Eddie Block, Texas State CISO, July 18, 2015.

[92] Colin Wood, "Texas CISO Brian Engle Departs for Cybersecurity Nonprofit," *Government Technology*, February 3, 2015, http://www.govtech.com/state/Texas-CISO-Brian-Engle-Departs-for-Cybersecurity-Nonprofit.html.

[93] Texas Department of Information Resources, "2014 DIR NSOC Annual Threat Report," May 2015.

According to TAC 202, each state organization is required to provide timely reporting (preferably within 24 hours) of cyber incidents to DIR which, depending on the threat or level of risk to the State, could be considered emergency reporting. In addition, DIR is developing a Governance, Risk, and Compliance (GRC) portal for agencies to go beyond reporting raw security incident data and instead to provide real-time and actionable analysis, compare statistics for incident management and response, and manage the investigation process.[94] As Block points out, "by incorporating risk assessment, security plans to mitigate risk, threat information, and incident data in a single system, we hope to give agencies better analytics and give DIR a single pane of glass view of the state of the state."[95]

E-crime and Law Enforcement

There have been discussions with the Texas Emergency Management Agency, DPS, and other key state agencies to enhance law enforcement efforts in cybersecurity, but this is still a work in progress. When a cyber incident occurs, DIR engages—as appropriate—different law enforcement entities to assess, investigate, and eventually prosecute cyber crimes.

Information Sharing

Although there is not a formal information sharing mechanism in place or an established industry forum for industry to participate with state government for enhancing cybersecurity and sharing information in real-time, DIR maintains a 24/7 security alert and response system through its voluntary open data portal and collaborates regularly with the MS-ISAC. Additionally, the GRC portal, available to all state agencies and institutions of higher education, will offer them a place to track security incidents and privacy violations in real time, compare incident activities among similar organizations, and manage their information security programs. Recent legislation has also created a new position within DIR, a Chief Data Officer, who reports directly to the state CIO and helps solicit voluntary information sharing.

Cyber R&D, Education, and Capacity Building

Texas has various clusters of academic institutions, public and private sector entities located in and around major metropolitan areas and military installations that provide great examples of collaboration, innovation, and achievement in cybersecurity. The City of San Antonio, for example, cooperates actively with the Chamber of Commerce, local businesses, the military community, colleges and universities, and independent school districts to increase cybersecurity education, awareness, and workforce development by leveraging opportunities and assets in the area. Moreover, Texas has twelve NSA/DHS Centers of Academic Excellence in Information Sharing, including Texas A&M University, Rice University, and University of Dallas. Many of these centers have been able to use state funds to then leverage significant federal and other non-state funds back into their universities to grow and develop their cybersecurity programs.[96]

In addition, DIR has launched an education program—the Texas InfoSec Academy—specifically designed to train security professionals within the state, including information security officers and state agency workers, which leverages private sector experts to provide comprehensive cybersecurity classes and certifications.

The Cybersecurity Coordinator has also been tasked with "establishing and leading a Texas Business Council to support public-private partnerships, align competencies, and create mutually reinforcing incentives for both companies and universities" to create jobs and develop the right talent pool of cybersecurity professionals.[97]

Finally, DHS has recently awarded an $11 million grant to the University of Texas at San Antonio to serve as the standards-setting body for the new Information Sharing and Analysis Organizations (ISAOs). These new

[94] Texas Department of Information Resources, "The Archer GRC Portal," http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=136.

[95] Author's interview with Eddie Block.

[96] Texas Cybersecurity, Education, and Economic Development Council, "Building a More Secure and Prosperous Texas," 17.

[97] Author's interview with Robert Butler, June 3, 2015.

entities that are being stood up by various states around the country are intended to facilitate cyber threat sharing and collaboration between the private sector and the government. As Andy Ozment, DHS Assistant Secretary of Cybersecurity and Communications stated:

> The University of Texas at San Antonio will work with existing information sharing organizations, owners and operators of critical infrastructure, federal agencies, and other public and private sector stakeholders to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs.[98]

[98] Katie Bo Williams, "DHS awards $11M to set cyber-sharing standards," *The Hill*, September 4, 2015, http://thehill.com/policy/cybersecurity/252766-dhs-awards-11m-to-set-cyber-sharing-standards.

Virginia

Total Population: 8,326,289
Current Governor: Terry McAuliffe

Virginia has a long history of integrated leadership, coordination, and collaboration between public and private sector organizations and higher education institutions, which have made the state a leader in innovation and technology, and more recently in cybersecurity. Its proximity to the federal government—the wellspring of cybersecurity policy, funding, and technology—and its business-friendly policies have attracted both private and federal technology investments and helped building its cybersecurity industry.[99] In 2014, Virginia Governor Terry McAuliffe established the Virginia Cyber Security Commission to identify high-risk cybersecurity issues facing the Commonwealth of Virginia, provide suggestions for more secure network plans and procedures, offer response strategies and best practices for the State, promote cyber hygiene, help facilitate the presentation of cutting-edge science and technologies in the cybersecurity realm, implement state cyber assessments, and contribute to the overall cyber-safety of Virginia as a whole.[100] As Karen Jackson, Virginia Secretary of Technology and co-chair of the Commission, stated "the Commission did not wait for their full report to be published to take action, and has already been able to make an impact and get some of their recommendations implemented by identifying important bills and pushing the Virginia Legislature to pass them."[101]

State Cybersecurity Strategic Plan & Competent Authority

Although there is not a unique entity responsible for cybersecurity in the state, different agencies are tasked with enforcing security standards, ensuring that policies are implemented, collecting compliance metrics, protecting electronic assets, responding to cyber attacks, and providing cybersecurity education and awareness. Virginia Code empowers the Commonwealth's CIO, under the direction of the Secretary of Technology, to govern cybersecurity efforts of state owned systems through the creation and promulgation of information security policies, procedures, and standards.[102] The CIO oversees the Virginia Information

[99] Office of Virginia's Secretary of Technology, "Virginia's Innovation Ecosystem: The Trusted Leader in Growing Cyber Security Solutions," 3.

[100] Virginia Office of the Governor, "McAuliffe Names Members of Virginia Cyber Security Commission," Press Release, May 16, 2014, https://governor.virginia.gov/newsroom/newsarticle?articleId=4817.

[101] Author's interview with Karen Jackson, Virginia Secretary of Technology and co-chair of the Virginia Cyber Security Commission, June 2015.

[102] Office of Virginia's Secretary of Technology, "Virginia's Innovation Ecosystem," 6.

Technologies Agency (VITA), the Commonwealth's consolidated information technology organization responsible for the governance, operation, and security of the state's cyber infrastructure.[103] Four additional entities within VITA share cyber-related responsibilities and activities:

- The Commonwealth Security & Risk Management (CSRM) Directorate, tasked with protecting citizen data and providing a safe, secure technology environment to enable state agencies to accomplish their respective missions. In order to do so, the Directorate offers a wide variety of tools and processes, including detailed information security policies, standards, and guidelines, designated to secure state agencies' data and systems.

- The Information Technology Advisory, responsible for advising the CIO and the Secretary of Technology on the planning, budgeting, acquiring, using, disposing, managing, and administering of information technology and to appoint a health information technology standards advisory committee in the Commonwealth.

- The Information Security Officer's Advisory Group, which holds monthly meetings for state and local government people interested in information security.

- The Commonwealth Information Security Council makes recommendations on the strategic direction of the state's information security and privacy-related initiatives and "provides a forum to discuss, assess, and propose pending legislation, regulation and/or requirements that have the potential to impact the commonwealth or individual agency information security practices, thereby enabling the commonwealth to take proactive steps to address such mandates."[104] All information security officers, information technology auditors, and other information security interested parties of government entities can participate in the Council's meetings.

As Zaki Barzinji, Deputy Director of Intergovernmental Affairs for Governor McAuliffe, explained,

> One of the recommendations of the Virginia Cyber Security Commission is to tighten and centralize the responsibility for the cybersecurity posture of the Commonwealth, and ensure that each state agency is responsible for the protection of its own data, instead of only relying on VITA to protect their cyber assets.[105]

As a result of these recommendations, the Governor recently issued an executive order requiring a strategic plan to address data security across the state government.[106] The executive directive requires VITA to review the state's risk management stance and provide recommendations for strengthening and modernizing state agencies' cybersecurity profiles. The order calls for VITA to conduct agency audits and present status reports to the Governor and the Secretary of Technology and Finance in 2016.

Finally, Virginia was the first state to adopt the NIST Framework for Improving Critical Infrastructure Cybersecurity, which was adapted to the specific needs of the state and implemented by VITA's CSRM "to enhance the systematic process for identifying, assessing, prioritizing, and communicating cybersecurity risks;

[103] Virginia Information Technologies Agency, "About VITA," http://www.vita.virginia.gov/about/.

[104] Virginia Information Technologies Agency, "Commonwealth Information Security Council Charter," October 15, 2012, http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/Information_Security_Council/CISC_%20Charter_102012.pdf.

[105] Author's interview with Zaki Barzinji, Deputy Director of Intergovernmental Affairs for Governor McAuliffe, July 2, 2015.

[106] Virginia Office of the Governor, "Governor McAuliffe Signs Executive Directive to Strengthen Cybersecurity Protocol," Press Release, August 31, 2015, https://governor.virginia.gov/newsroom/newsarticle?articleId=12544.

efforts to address risks; and steps needed to reduce risks as part of the state's broader priorities."[107] Virginia has also begun to explore how the Framework could be leveraged to enhance cybersecurity capabilities of critical infrastructure, and groups such as the Virginia Cyber Security Commission plan to further investigate how it can improve the overall state's cybersecurity posture.

Incident Response

While "all executive branch agencies including institutions of higher education are required to report information security incidents to VITA, except for the University of Virginia, Virginia Polytechnic Institute and State University, and the College of William and Mary)," the Secretary of Public Safety and Homeland Security is generally responsible for all-hazards incident response, depending on the nature of the incident.[108] VITA's website provides additional guidance on reporting this type of incidents, including an information security incident reporting template.

In addition to VITA's incident response capabilities for Commonwealth systems, the Virginia National Guard (VANG) has explored ways in which their capabilities could be leveraged for pre-incident preparation, response, and post-incident recovery. In June 2014, VANG established the Virginia Cyber Response Working Group whose mission was to establish and understand the specific role and capabilities of VANG in supporting cyber incident response through facilitated discussions with federal, state, and local agency stakeholders. The Working Group has since taken a broader perspective of the state's role in cyber incident response and has made significant progress in this area.

Under the direction of the Office of the Secretary of Public Safety and Homeland Security, the Working Group drafted the first ever Cyber Security Hazard Specific Annex of the Commonwealth of Virginia Emergency Operations Plan (COVEOP). Included in the effort were representatives from VANG, Virginia State Police (VSP), Virginia Fusion Center (VFC), VITA, and the Virginia Department of Emergency Management (VDEM). The Annex is a product of the Working Group's efforts to define the state's role in responding to cyber incidents that affect its critical infrastructure outside of the scope of the Commonwealth's networks.

The Annex was recently reviewed during the first Virginia Cyber Guard Prelude table top exercise which brought together over seventy stakeholders from federal, state, local, and private sector organizations to discuss how the state would respond to a sophisticated cyber attack impacting critical infrastructure systems from multiple sectors. Currently, the exercise planning team is in the process of finalizing the Prelude's After Action Report (AAR), which details several action items to be addressed over the ensuing twelve months, including revisions to the draft Annex.

E-crime and Law Enforcement

In 1991, the Virginia Attorney General established a Computer Crime Section to carry out multiple duties, including investigating and prosecuting crimes under the Virginia Computer Crimes Act, such as computer fraud, computer trespass, spamming, phishing, identity theft, and child exploitation. This entity also helps with law enforcement in computer crime cases, as well as trains law enforcement in computer security matters. It also assists in drafting legislation within cyber crime, and has testified before Congress in relevant cases.[109]

In 2009, the VSP formed the High Tech Crimes Division (HTCD) within the Bureau of Criminal Investigation (BCI). The HTCD engages the use of leading technologies to proactively provide specialized law enforcement services in response to the needs of local, state, and federal law enforcement agencies, and the Commonwealth's citizens, including planning and training to promote a competent, positive, and productive

[107] Virginia Information Technologies Agency, "2013 Commonwealth of Virginia Information Security Report," http://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/Security/2013_COVA_IS_Annual_Report.pdf.

[108] Virginia Information Technologies Agency, "Guidance on Reporting Information Security Incidents," http://www.vita.virginia.gov/security/default.aspx?id=317.

[109] Virginia Office of the Attorney General, "About the Office of the Attorney General's Computer Crime Section," http://ag.virginia.gov/CCSWeb2/index.php/home/about-the-computer-crime-section.

workforce who perform their duties with the highest degree of professionalism.[110] The HTCD is split into four specialties: the Northern Virginia/District of Columbia Internet Crimes Against Children (ICAC), the Computer Evidence Recovery Section (CERS), the High Tech Crimes Section (HTCS), and the Technical Support Section (TSS). The HTCD is the primary state authority in charge of investigating and conducting forensics analysis of computer crimes.

The Commission has a specific Cyber Crime Working Group that has been reviewing state statutes that govern cyber crimes, and recommended legislation to update the definition of what constitute a "cyber crime" and to improve law enforcement's capabilities in investigating such crimes. Members of the VSP HTCD are included in this working group.

Information Sharing

In 2015, Governor McAuliffe announced the development of the Virginia Information Sharing Analysis Organization (ISAO), which includes collaboration between the VSP, Secretary of Public Safety and Homeland Security, the Secretary of Technology, and VITA.[111] The ISAO, a first-of-its-kind central point of contact for both the federal government and state agencies, bolsters information sharing related to cybersecurity threats and attacks, and makes relevant information more effective and reliable.

The Virginia Fusion Center (VFC) operates as a focal point within the Commonwealth of Virginia for the collection, receipt, analysis, and dissemination of timely threat intelligence between the federal government and state, local, and private sector partners. In particular, the VFC has developed a cyber capability utilizing a civilian analyst and a sworn special agent dedicated full-time to cyber activities. These personnel identify and track known and emergent cyber threats to the Commonwealth and contributes to the statewide awareness, detection, analysis, and response to such threats through the dissemination of timely and actionable cyber threat intelligence. The VFC also provides analytical case support on criminal investigations with a cyber nexus, cybersecurity training and awareness, and increased cyber resiliency through exercise and assessment.[112] The VFC cyber capability is an identified asset for the Commonwealth to be leveraged for the newly developed ISAO.

Cyber R&D, Education, and Capacity Building

Virginia has been able to successfully leverage partnerships with local companies and universities to promote innovation, technology, and cybersecurity solutions, and attract significant federal investments for its leading research and development institutions. Former Governor Bob McDonnell signed the Virginia Higher Education Opportunity Act in 2011, which served to place more emphasis on STEM education in Virginia's colleges and universities. Moreover, Virginia has four NSA/DHS Centers of Academic Excellence in Information Sharing, including George Mason University, University of Virginia, and James Madison University, which is also a SFS participating institution. Virginia Community College System provides additional workforce training and certification to individuals pursuing careers in cybersecurity.

In 2013, Virginia established a Cyber Security Partnership (CSP) to enact a trusted and dependable community of public and private sector cyber professionals. The CSP leverages the collective experience and knowledge of such members, promotes mutually beneficial information sharing, and fosters professional development.[113] Former Governor Bob McDonnell had also launched a public-private partnership in 2013—Semper Secure—designed to extend the Commonwealth of Virginia's and the Greater Washington, D.C., metro region's leadership in cybersecurity.[114]

[110] Secretary of Public Safety and Homeland Security, "Cyber Security," https://pshs.virginia.gov/homeland-security/cyber-security/.
[111] Virginia Office of the Governor, "Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats," Press Release, April 20, 2015, https://governor.virginia.gov/newsroom/newsarticle?articleId=8210.
[112] Secretary of Public Safety and Homeland Security, "Cyber Security."
[113] "The Virginia Cyber Security Partnership (CSP)," https://www.infragard.org/sites/default/files/cyber_security_partnership.pdf.
[114] "Governor Bob McDonnell Announces Virginia Cyber Security Partnership," *Dark Reading*, April 4, 2013, http://www.darkreading.com/risk/governor-bob-mcdonnell-announces-virginia-cyber-security-partnership/d/d-id/1139472?.

Washington

Total Population: 7,061,530
Current Governor: Jay Inslee

For the past several years, Washington State has been at the forefront of cybersecurity protection and preparedness. Recognizing the need for the state to have a holistic response to the challenges of a significant cyber event, Washington state officials launched a “bottom-up” cybersecurity planning effort in early 2012—part of a statewide Cybersecurity Program—to prepare for any type of major cyber incident occurring or directly impacting the citizens of Washington.[115] The Washington State Military Department, including the Washington State Emergency Management Division (EMD) and the Washington National Guard, play a key role in this effort and have worked tirelessly to develop policies and frameworks to better prepare the state for cyber emergencies. In addition to having an overarching cybersecurity strategy based on a community effort and a comprehensive incident response plan, the state has appointed a senior emergency manager to serve as Cyber Security Manager, and is actively promoting research, analysis, and sharing of cybersecurity information and best practices across private and public sectors.

State Cybersecurity Strategic Plan & Competent Authority

In a recent high-level document addressed to DHS Deputy Secretary, Alejandro Mayorkas, Washington State’s Governor, Jay Inslee, articulated the state’s unified approach and overall strategy—or, as they call it, “Community Cybersecurity.”[116] The Governor’s letter detailed many of the state cybersecurity strategy’s objectives, including: strengthening state’s networks for public safety and commerce; fostering regional collaboration between public, private, and tribal partners; promoting research, analysis, and sharing of cybersecurity information and best practices; developing a cybersecurity workforce; and ensuring unity of effort to enhance protection of critical infrastructure. And in March 2015, the State of Washington published a Cyber Emergency Response Annex—the Washington Significant Cyber Incident Annex (WSCIA)—to the Comprehensive Emergency Management Plan (CEMP).[117] This Annex is part of the Cybersecurity Program, created within the Emergency Management Division with the goal of “fully integrating cybersecurity into statewide emergency planning, training, preparation, and response procedures” to address the growing scope

[115] Major General Bret Daugherty, “Challenges in Cybersecurity,” Proceedings from the *Esri National Security Summit*, (San Diego, July 12, 2014), http://proceedings.esri.com/library/userconf/nss14/papers/nss-15.pdf.

[116] State of Washington Office of the Governor, *Letter to The Honorable Alejandro Mayorkas, U.S. Department of Homeland Security Deputy Secretary*, August 19, 2015.

[117] Washington Military Department, “Washington State Significant Cyber Incident Annex to the Washington State Comprehensive Emergency Management Plan,” March 2015, http://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.

and sophistication of cyber threats to the state.[118] This statewide, interagency, public/private/tribal endeavor brings together key partners from the National Guard, multiple state agencies, utilities, private sector critical infrastructure operators and IT companies, and even the rural community service providers. The program was the result of the work of an innovative state multi-agency Cyber Integrated Project Team (IPT) that works collaboratively to advance the cybersecurity for the state. The manager of the program serves as the state's cybersecurity policy leader and strategist for emergency management. In addition to developing and expanding internal procedures, the Cybersecurity Program promotes extensive outreach with the private and public sectors to further state emergency preparedness. Additionally, cybersecurity has been incorporated into the State Preparedness Report and the Threat and Hazard Identification and Risk Assessment (THIRA) and local universities conduct regular research on cyber threats for the Hazard Identification and Vulnerability Assessment (HIVA).

Finally, the Governor designated The Adjutant General (TAG) and Homeland Security Advisor for the state of Washington as the competent authority and "Senior Official to represent the state for response to a significant cybersecurity incident, both within the state and at the federal level" and the Military Department as "the Primary Agency for external communication with the Department of Homeland Security for significant cybersecurity incident exercises."[119] As Matt Modarelli, the state's current EMD Cyber Security Manager, explains, his position "reports to the Director of Emergency Management, under the direction of the state Homeland Security Advisor and the Governor."[120] In his unique role, he conducts extensive outreach, collaboration, and integrated planning and exercise activities with the private and public sectors in furtherance of statewide cyber incident preparedness. Additionally, he oversees enterprise-level program development of the state's first-ever cyber emergency response plan and serves as chairman of multiple private and public sector integrated project teams.

Incident Response

As mentioned above, Washington has recently adopted a thorough incident response Annex, WSCIA, that complements the Comprehensive Emergency Management Plan (CEMP) and provides guidance on how the state should respond to major cyber incidents occurring at the state, local, and tribal or private sector levels.[121] Indeed, cybersecurity has been updated as a core capability in all phases of emergency management planning and the Annex has been distributed statewide to help encourage cybersecurity preparedness and unity of effort. The State Emergency Operations Center (SEOC) is the competent authority responsible for developing and maintaining the common operational picture for emergency management initiatives and coordinating state and national cyber response efforts. The Cyber Unified Coordination Group (UCG), which includes representatives from the federal, state, and local governmental agencies, academia, and the private sector, assists in response activities by providing additional resources, authorities, and information.

The Cybersecurity Annex was built on the foundations of the National Response Framework (NRF) and the Draft National Cyber Incident Response Plan (NCIRP), and is intended to facilitate both the rapid internal state-level and national incident coordination needed to defend against the full spectrum of cyber threats. The WSCIA ties various policies and doctrines together into a single tailored, strategic, cyber specific plan designed to assist with operational execution, planning, and preparedness activities, and to guide recovery efforts. In addition, the plan describes the roles and responsibilities that different stakeholders in the state have and the clear course of action to follow in case of a significant cyber incident, including ensuring that the Governor's Office and SEOC receive timely updates on the status of response activities. While the WSCIA already offers a comprehensive framework for coordination and execution among federal, state, local, tribal, and territorial governments, the private sector, and operators of critical infrastructure, communities and emergency managers are also encouraged to refer to documents like the NIST Framework to develop individual agency or organizational cyber incident response plans. Moreover, the state carries out

[118] Washington Emergency Management Division, "Cybersecurity Program," http://mil.wa.gov/emergency-management-division/cyber-security-program.

[119] State of Washington Office of the Attorney General, *Letter to Major General Bret Daugherty, The Adjutant General*, July 29, 2015.

[120] Author's interview with Matthew R. Modarelli, Washington State' Emergency Management Division Cyber Security Manager, September 9, 2015.

[121] Washington Military Department, "Washington State Significant Cyber Incident Annex ."

regular state-level cybersecurity exercises, including a state cabinet level tabletop exercise, as part of the Cybersecurity Program. In every case, these exercises involve public and private sector participation at both the policy and execution levels.

Moreover, Washington was one of the first states to tap into its National Guard for help in coordinating cybersecurity response and activities. Indeed, the state began using the National Guard in a cybersecurity capacity when they realized that many of its soldiers, who are full-time employees and part-time soldiers, worked in cyber-related roles for tech companies based in Washington, such as Google, Boeing, Microsoft, Cisco, and Verizon.[122] Today, four Washington National Guards units are used in a cybersecurity capacity and can be deployed in "red teams" exercises to evaluate the strengths of the state's digital networks and the effectiveness of existing cyber emergency plans.

E-crime and Law Enforcement

State law enforcement and criminal justice agencies partner routinely to interdict, investigate, and prosecute cyber crimes. In particular, the Washington State Patrol (WSP) is responsible for investigating cyber crimes committed on state property, against state agencies, and against state assets. Its High Tech Crimes Unit (HTCU)—a full time computer forensics team—is entirely dedicated to investigating this type of crimes and may also be activated at the request of local law enforcement agencies. During a significant cyber incident, WSP coordinates the initiation of cyber crime investigations with appropriate state and local law enforcement agencies and support from federal partners, and the HTCU ensures that the Cyber UCG and SEOC are aware of which law enforcement agencies are engaged.

Moreover, Washington State's Attorney General, Bob Ferguson, has taken actions to protect consumers who have been victim of data breaches by introducing legislation in 2105 to prevent identity theft. The legislation, recently passed by both the state House and Senate, strengthens Washington's data breach notification law by eliminating the blanket exemption for encrypted data; requiring consumers to be notified as soon as possible and no later than 45 days from when a breach is discovered; and requiring businesses, non-profits or public agencies to notify the Attorney General within 45 days of a breach, and to provide consumers with basic information they can use to help secure or recover their identities.[123]

Efforts to combat cyber crime and resolve consumer issues date back to the early 2000s, when Washington State launched various innovative initiatives designed to help law enforcement investigate and prosecute illicit cyber activities. These included a partnership of local, state, and federal law enforcement agencies—the Computer Law Enforcement of Washington initiative (CLEW)—to provide around-the-clock law enforcement response to high-tech crime complaints, and share expertise, resources and training; an online clearinghouse to help people avoid online fraud and crime; and a high tech strike team of attorneys and investigators entirely focused on high-tech crimes.[124]

Information Sharing

The WSCIA recognizes that effectively understanding risks in cyberspace requires different state entities to collaborate on a daily basis to share information and identify threats, vulnerabilities, and potential consequences. Although Washington does not have a dedicated integration and information sharing hub, it encourages cybersecurity partners in the state to take advantage of national efforts, such as the MS-ISAC and the NCCIC, to build a more robust common operational picture of cyber threats to the state and facilitate cyber incident response activities. As mention above, SEOC is also responsible for communicating significant cyber incident-related information and situational awareness to its partners in the state, the Governor's Office, NCCIC, and the Washington Homeland Security Advisor (HSA). Additionally, Washington is an

[122] "National Guard Unites Help States Ward Off Attacks," *Homeland Security News Wire*, February 3, 2014, http://www.homelandsecuritynewswire.com/dr20140203-national-guard-units-help-states-ward-off-cyberattacks.
[123] State of Washington Office of the Attorney General, "AG's Data Breach Notification Bill Unanimously Approved in Senate," April 13, 2015, http://www.atg.wa.gov/news/news-releases/ag-s-data-breach-notification-bill-unanimously-approved-senate.
[124] Lori Enos, "Washington State Gets Tough on Cybercrime," E-*Commerce Times*, May 1, 2000, http://www.ecommercetimes.com/story/3182.html.

active member of the Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) group—a regional organization similar to the ISAC model but focused on information sharing and analysis between members, which include federal law enforcement (FBI, Secret Service), state, local, and tribal governments, and many private-sector companies in Washington State. CIRCAS members share information on threats observed on member networks, and have a standing agreement to assist with analysis and response for those events that exceed the response capability of a member organization. The state also takes advantage of other regional monitoring programs, such as the Public Regional Information Security Event Management (PRISEM) system, that can supply situational awareness regarding the threat surface of the region, and provide a common operating picture across the participating public, energy, and health-sector organizations.

Finally, the Washington State Fusion Center (WSFC) facilitates information sharing using the Homeland Security Information Network (a national secure and trusted web-based portal for information sharing and collaboration) cybersecurity alerts, and provides a number of classified and unclassified network feeds that can greatly enhance situational awareness and incident response coordination. During a cyber incident, WSFC may also host the Cyber UCG and generate specific cyber alerts to notify federal, state, regional, local, tribal, and private sector partners with early warning indicators and potential actionable intelligence measures.

Cyber R&D, Education, and Capacity Building

In addition to providing a framework of reference for cybersecurity preparedness and response, the state's Cybersecurity Program works closely with the Washington State Emergency Management Training program and other jurisdictions across the state to plan and deliver multiple training events and seminars aimed at raising cybersecurity awareness of emergency managers across the state.

The Washington Department of Commerce works actively to ensure that the state is considered a prime location for IT and cybersecurity-related public and private investments that meet this growing industry need. Additionally, the state is taking steps to build on private sector relationships with companies like Microsoft and Internet Identity to maximize the talented employees already working in this space and to attract additional cybersecurity professionals to the state. The state is also partnering with various institutions of higher education, like the University of Washington and Whatcom Community College, to develop a pipeline of cybersecurity talents, and with private companies, like Snohomish PUD and Pacific Northwest National Laboratories, to coalesce the best and brightest to the field.

Moreover, different universities in the state have launched cybersecurity programs and research centers. Washington State University of Tacoma, for example, created a Center for Information Assurance and Cybersecurity (CAIC), which fosters a unique collaboration between information science, computer science, economics, electrical engineering, and law—all critical aspects of the study of cybersecurity.[125] Washington also has three NSA/DHS Centers of Academic Excellence in Information Sharing.

[125] Washington State University of Tacoma, "Center for Information Assurance and Cybersecurity," http://depts.washington.edu/ciac/node/15.

Conclusions

No state is cyber ready.

As states continue to embrace the benefits that ICTs bring to their economy and society, they must also consider the negative implications of illegal and illicit cyber activities that are threatening the security and economic wellbeing of their communities and devise comprehensive strategies to address those threats.

The federal government has actively worked to develop standards, policies, and regulations to enhance cybersecurity across the nation, increase its situational awareness, fight cyber crime, lower cyber risks, improve resilience, and promote information sharing. Cybersecurity, however, cannot be tackled at the federal level alone and states cannot wait for the federal government to provide all responses and solutions before taking actions. States have a responsibility to shoulder their part of the burden and must work to secure their critical infrastructure and cyber assets. And while these responsibilities are shared with other stakeholders, including critical infrastructure operators, IT security specialists, law enforcement officials, financial institutions, and even international organizations, states still play a fundamental role in creating the legal and policy frameworks that will allow their regions to harness the economic power of ICTs, foster innovation and job creation, and ensure that their citizens can rely on safe and secure Internet connectivity.[126] Several states in the United States have started to address cybersecurity issues and a handful of them have positioned themselves as leaders in this field by devising innovative solutions to improve cyber resilience and promote cybersecurity workforce development and business opportunities.

These states are exercising their responsibility through both government action by leveraging policies, plans, laws, regulations, and standards, and by providing the right set of incentives and assistance for other stakeholders. Such actions come in different forms: adopting a cybersecurity strategic plan and secondary legislation; identifying a competent authority responsible for the strategy's execution and policy compliance; implementing legal and policy reforms; developing detailed incident response plans; creating integration and information sharing hubs to facilitate the exchange of actionable intelligence between state agencies and critical industries; equipping state employees with the education and training necessary to understand their specific roles and responsibilities in protecting citizens information and maintaining the highest ethical standards; providing funds and tax credits to grow their cybersecurity industry; and partnering with academic and research institutions to promote cyber R&D, innovation, and education across the state. Although the specific organizational structures and composition of different partnerships may vary, and not every state may have the same needs and resources, these initiatives provide practical ways for states to take inventory of their cyber assets and devise strategies, policies, and activities to protect the value of their digital investments, lower cyber risks, and increase resilience.

While the CRI methodology offers a credible, actionable, and flexible tool to objectively assess the gaps between states' current cybersecurity posture and the cyber capabilities needed to protect their cyber infrastructure and digital investments, the initiatives highlighted throughout this report provide models for other states and jurisdictions to follow and offer a useful set of best practices and activities at the state-level to put recommended actions into practice.

[126] European Union Institute for Security Studies, "Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development," *Report no. 21,* December 2014: 12.

SALVE REGINA UNIVERSITY

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Claiborne Pell's legacy, the Center promotes American engagement in the world, effective government at home, and civic particpation by all Americans.

www.pellcenter.org