States Confront the Cyber Challenge

Memo on State Cybersecurity Centers

Overview

Since 2015, seven states have publicly established or announced the creation of a state "cybersecurity center," tasked with implementing key cybersecurity policies.[1] Unlike state information technology (IT) security offices, these centers are tasked with responsibilities that extend beyond defending state networks. Based on their current roles and responsibilities, these centers can be divided into three categories: (1) integration centers that focus on information sharing and incident response; (2) centers with a workforce and education focus; and (3) centers with policy making authority. Although these centers are in various stages of implementing their priorities, other states should review why and how these centers were organized, and their sustainability, if they are considering creating their own center.

Integration Centers

Integration centers focus largely on information sharing among state, local, private, and federal partners to assist in preventing, and at times mitigating or responding to, cybersecurity incidents.

New Jersey

One of the more well-known cyber centers is the **New Jersey** Cybersecurity and Communications Integration Cell (NJCCIC), established in May 2015 by executive order. The NJCCIC's mission is to act as the "central 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."[1] To fulfill this mission, the NJCCIC is authorized to:

- Coordinate information sharing related to cybersecurity risks, warnings, and incidents, and to provide support for cybersecurity incidents and cyber crime investigations;
- Provide information and recommend best practices concerning cybersecurity and resilience measures to public and private entities; and

[1] Not included in this examination are efforts underway in Idaho. Idaho recently passed legislation to create the "Cybercore Integration Center and the Collaborative Computing Center" at the Idaho National Laboratory to serve as an education and training facility for cybersecurity research. This center was excluded due its apparent federal focus.

- Serve as an information sharing and analysis organization (ISAO)[2] and coordinate with federal agencies, public and private sector entities.[2]

The actors responsible for implementing these responsibilities include the state's office of homeland security and preparedness (OHSP)—where the NJCCIC resides—the attorney general's office; state police; office of information technology; and any other local, federal, or private sector partner that the Director of OHSP deems necessary.[3]

California

In the fall of 2015, the **California** Cybersecurity Integration Center (Cal-CSIC) was established by executive order to "to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks."[4] Like the NJCCIC, the Cal-CSIC coordinates information sharing among local, state, federal, tribal, and private partners. Specifically, the Cal-CSIC is tasked with:

- Providing warnings of cyber attacks to government agencies and other partners;
- Coordinating information sharing among entities and sharing of recommended best practices;
- Assessing risks to critical infrastructure and information technology (IT) networks;
- Prioritizing cyber threats and supporting public and private sector partners in protecting their vulnerable infrastructure and IT networks; and
- Supporting cybersecurity assessments, audits, and accountability programs that are required by state law to protect the IT networks of state agencies and departments.[5]

In addition to the actors identified in the NJCCIC, the Cal-CSIC also includes the state's health and human services agency, the utilities emergency association, universities, and community colleges. Lastly, the Cal-CSIC will create a cyber incident response team (CIRT) that leads cyber threat detection, reporting, and response, as well assists in cyber crime investigations.[6]

New Hampshire

The **New Hampshire** Cybersecurity Integration (NH-CIC) was created by executive order in October 2016. It will coordinate cybersecurity monitoring, share information, perform threat analyses, and promote situational awareness among executive branch agencies and departments.[7] According to meeting minutes, the NH-CIC will maintain an active role in responding to security events by:

- Coordinating the prevention and mitigation of cyber threats to the state;
- Pursing whole-of-state operation integration through information sharing;
- Breaking down technological and institutional barriers that impede information exchange, situational awareness, and understanding of threats and their impact;
- Sustaining readiness to respond to all cyber incidents;

[2] An ISAO is any entity or collaboration created or employed by public or private-sector organizations, for the purposes of: (1) gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability; (2) communicating or disclosing critical cyber and related information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to cyber systems; and (3) voluntarily disseminating critical cyber and related information to its members; federal, state, and local governments; or any other entities that may be of assistance in carrying out the purposes previously specified.

- Serving stakeholders as a statewide "center of excellence"; and
- Protecting the privacy and critical data of New Hampshire citizens.[8]

The state's department of information technology will establish and maintain the NH-CIC, but it will be located within the state's division of homeland security and emergency management. To facilitate the fulfillment of its mission, the executive order requires that (1) all known or suspected cyber incidents within state agencies or within any vendor acting as an agent of the state to be reported to the NH-CIC and (2) for all agencies to appoint an employee to lead all agency security matters.[9]

Distinctions

Although these three integration centers have many commonalities, they each possess unique qualities. First, New Jersey leverages the NJCCIC to assist in evaluating the state's cybersecurity performance based on the NJCCIC's activities. For instance, cyber analyses will be evaluated by the volume of alerts and reports published by NJCCIC; public-private partnerships will be assessed by the number of new members registered with the NJCCIC; and cybersecurity awareness will be measured by the number of briefings and webinars.[10] Other states may wish to use their integration centers in a similar way. For example, a state may evaluate its incident response efforts by assessing how many hours were worked on an incident, reviewing reports for adherence to policies, and determining if the incident is a recurrence of a previous incident.[11]

The Cal-CSIC is the lone integration center developing a statewide cybersecurity strategy to "strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's workforce of cybersecurity professionals, and expand cybersecurity awareness and public education."[3, 12] Other states may want to consider a similar approach as an integration center may be best suited to understand the state's threats and vulnerabilities, and its ability to prevent threats from materializing. This knowledge could then be used to form the baseline of a cybersecurity strategy.

Lastly, the NH-CIC has a unique governance structure called the executive oversight committee. This committee's broad goal is to manage operations and implementation of the strategic plan and overall governance of the center. The body is unique in that it comprises a wide range of departments, such as employment security, environmental services, revenue administration, transportation, and the office of professional licensure and certification.[13] Such a diverse body I designed to overcome divisions and institutional barriers that hinder information sharing across stakeholders in the public and private sectors.

Workforce and Education Centers

These cybersecurity centers have similar roles to the integration centers described above, but they have additional duties related to cybersecurity education and workforce development.

<u>Colorado</u>

The National Cybersecurity Center (NCC) in **Colorado**, legislatively enacted in 2016 as a nonprofit organization, consists of three "pillars," with one pillar focusing specifically on incident response. Like the integration centers, the NCC's Rapid Response Center (RRC) is composed of law enforcement entities, military organizations, and emergency management and homeland

[3] Although California is the only integration center to create a statewide cybersecurity strategy, other state cyber centers are also tasked with creating a statewide cybersecurity strategy.

security agencies. The RRC assists NCC members when they are victims of an incident, encourages interstate information sharing, supports intelligence and law enforcement operations, and conducts training and exercises, among other things. [14]

The other two pillars of the NCC have mandates that extend beyond incident response. The Cyber Research, Education, and Training Center (CRETC) develops and provides workforce education and training programs for the nation's public and private sector employees. A few of its objectives include coordinating with the U.S. Department of Homeland Security and the National Security Agency to certify cyber courses; collaborating with community colleges to develop transferable cybersecurity curricula; creating a public policy think tank; and establishing education, training, and "academic symposia" for government leaders.[15] The third pillar, the Cyber Institute, will be a dedicated national facility to share real-time information on cyber trends, security, best practices, and education resources.

Georgia

Georgia's Cyber Innovation and Training Center (Center) seeks to "promote modernization in cybersecurity technology for private and public industries through unique education, training, research, and practical applications."[16] To facilitate this goal, the Center will establish a cyber range, a pseudo network allowing for red team/blue team exercises, for businesses and universities. Regarding the former, the Center stands out from other states due to acting as an incubator for start-up companies. With the range, the Center also intends on:

- Allowing professionals to practice incident response plans;
- Establishing the Georgia Cybersecurity Academy to provide cybersecurity awareness, training, and education for information security officers;
- Providing security awareness, training and education, professional development, and cyber workforce development;
- Educating and training local human resource professionals to fill workforce deficiencies;
- Providing the ability to rapidly test and evaluate various security architecture; and
- Performing exercises to verify government and business readiness.[17]

Distinction: The Economic Cost

Operational costs for the integration centers in New Jersey, California, and New Hampshire could not be found. By contrast, Colorado and Georgia have appropriated funds to develop their centers. Specifically, Colorado appropriated roughly eight million dollars to launch the NCC, while Georgia allocated roughly $50 million to create the Center. The Colorado legislation enacting the NCC does not contain line item spending,[18] but Georgia provides spending detail for their center. Georgia's higher costs derive from the planned construction of a $41.5 million, 150,000 square foot facility, which will contain a cyber range and a sensitive compartmented information facility (SCIF).[19] The remaining funds will cover staffing; operating costs; and planning and design, utilities, and marketing.[20] These figures indicate that the Georgia Center will cost roughly seven to nine million dollars a year to operate, until it is fully leased.[21] Other states should take into consideration the economic cost of creating these types of centers and ask themselves:

- Will legislators have the appetite to continue to appropriate funds for the center?
- Will a new gubernatorial administration still prioritize cybersecurity and provide sufficient funds to the center?
- How will the center measure its return on investment? and
- What legal status makes the most economical sense: state entity, non-profit, or public-private model?

Centers with Policy Making Authority

Oregon and **Nevada** currently have pending legislation that would create their own cybersecurity centers. Unlike the previous centers, Oregon's and Nevada's centers would have more active roles in defending the state's networks from cyber threats and, as a result, have authority to enforce their standards and policies.[4]

Oregon

The Oregon Cybersecurity Center of Excellence (CCE) would be the focal point for cybersecurity policies in the state. In addition to performing functions similar to the centers in the previous two categories, such as serving as the state's ISAO and developing the cybersecurity workforce in the state,[5] the CCE would also play a more formal role in securing the state. For example, the CCE would review critical infrastructure's IT security to assess if the current policies are sufficient enough to prevent breaches and to develop plans to recover from threats.[22] The CCE would also create a process to conduct risk-based assessments for state agencies; develop cybersecurity recommendations for state agencies; recommend content and timelines for conducting cybersecurity awareness training for state employees; and establish data breach reporting, among other things.[23]

The structure of the CCE further underscores Oregon's whole-of-state approach. While the CCE would reside in the office of the state CIO, members of the center include the state's department of justice; the office of the secretary of state; department of consumer and business services; the higher education coordinating commission; the employment department; and the Oregon Business Development Department, among others.[6]

Nevada

Although Nevada's new Office of Cyber Defense Coordination (OCD) is technically an office, Gov. Brian Sandoval has referenced it as a center and charged it with duties similar to other state centers.[24] Like Oregon, OCD has a broad mission to "serve as the strategic planning, facilitating, and coordinating office for cybersecurity policy and planning in the state." [25] OCD will emulate roles similar to state information security offices by reviewing information systems of state agencies; identifying risks posed to those systems; and developing standards and guidelines for securing those systems. Other responsibilities include developing a disruption response plan; coordinating and initiating cybercrime investigations; creating a statewide strategy; establishing a CIRT; and coordinating a training and awareness program. Gov. Brian Sandoval has proposed to allocate $3.5 million to establish OCD, which would create four new positions to staff the office.[26]

Distinctions: Authority

---

[4] Oregon and Nevada are two of five states that were selected to be in NGA's *Policy Academy on Enhancing State Cybersecurity*. Through this project vehicle, NGA has consulted Oregon and Nevada in devising their respective centers.

[5] Roles and responsibilities include: coordinating information sharing related to cybersecurity risks, warnings, and incidents; providing cybersecurity incident response and cybercrime investigations support; recommending best practices for resiliency measures; drafting and updating a cybersecurity strategy and disruption response plan; and detailing steps the state should take to increase resiliency of its operations in preparation of and during the response to a cyber disruption event.

[6] These are all non-voting members. Voting members include representatives from cyber related industries in Oregon, a representative from post-secondary institutions, and one representative from law enforcement.

The commonality that distinguishes Oregon and Nevada from the rest of the states is their proposed ability to enforce their policies and standards. Yet, how they can enforce their authority differs.

Oregon's current legislation does not appropriate any funds to the CCE, but instead creates the "Oregon Cybersecurity Fund," from which dollars will be "continuously appropriated to the office of the [CIO] for the operation of the [CCE] consistent with the Oregon Cybersecurity Strategy and Cyber Disruption Response Plan."[27] Furthermore, the funds will be used for cyber education, workforce training, assessments and vulnerability testing, disruption and incident response, risk-based remediation measures, and other measures.[28] The CCE's authority to allocate funding—based on strategies that it designs—therefore empowers its leadership to exercise tremendous influence over cybersecurity spending throughout Oregon.

In Nevada, the OCD is granted authority to enforce standards it develops by:

- Coordinating performance audits and assessments of information systems to determine adherence to regulations, standards, etc.;
- Providing recommendations to state agencies and the Division of Enterprise Information Technology Services regarding the security of information systems; and
- Adopting any regulations necessary to carry out the provisions of this bill.

These are just two mechanisms that other states may wish to include in their centers to empower them.

Conclusion

Identifying the roles, responsibilities, and differences of these six centers is a useful exercise to examine how some states are addressing core cybersecurity challenges, such as information sharing and workforce development. Yet, there are unanswered questions that are beyond the scope of this memo that states and practitioners should ask themselves. Is a state center economically sustainable? Does the center duplicate activities within the state or at the national level, or does it truly address a gap in the state? Can existing offices, such as the state's IT security office or fusion center, fulfill a center's activities by changing existing statutes? Can a state negotiate a memorandum of understanding with a neighboring state's center and share resources? What authority should the center possess to enforce its policies?

These centers have or will undoubtedly provide unique benefits to their states; but states wishing to create centers should work with one another on how they can create centers that complement one another rather than duplicate current efforts.

Please e-mail Michael Garcia, Policy Analyst, Homeland Security and Public Safety Division, at mgarcia@nga.org *with any questions.*

[1] New Jersey Governor's Office. (2015). Executive Order No. 178. Retrieved from http://nj.gov/infobank/circular/eocc178.pdf.
[2] New Jersey Governor's Office. (2015). Executive Order No. 178. Retrieved from http://nj.gov/infobank/circular/eocc178.pdf.
[3] New Jersey Governor's Office. (2015). Executive Order No. 178. Retrieved from http://nj.gov/infobank/circular/eocc178.pdf.
[4]Office of Governor Edmund G. Brown Jr. (2015). Governor Brown Signs Executive Order to Bolster Cybersecurity. Retrieved from https://www.gov.ca.gov/news.php?id=19083.
[5] Office of Governor Edmund G. Brown Jr. (2015). Governor Brown Signs Executive Order to Bolster Cybersecurity. Retrieved from https://www.gov.ca.gov/news.php?id=19083.
[6] Office of Governor Edmund G. Brown Jr. (2015). Governor Brown Signs Executive Order to Bolster Cybersecurity. Retrieved from https://www.gov.ca.gov/news.php?id=19083.
[7] State of New Hampshire Office of the Governor. (2016). An Order Establishing the New Hampshire Cybersecurity Integration Center and Executive Oversight Committee. Retrieved from http://sos.nh.gov/WorkArea/DownloadAsset.aspx?id=8589963332.
[8] State of New Hampshire Department of Information Technology. (2016). Meeting Summary. Retrieved from https://www.nh.gov/doit/it-council/documents/20161028-minutes.pdf.
[9] State of New Hampshire Office of the Governor. (2016). An Order Establishing the New Hampshire Cybersecurity Integration Center and Executive Oversight Committee. Retrieved from http://sos.nh.gov/WorkArea/DownloadAsset.aspx?id=8589963332.
[10] New Jersey Office of Management and Budget. (2016). Fiscal Year 2017: The State of New Jersey Detailed Budget. Retrieved from http://www.nj.gov/treasury/omb/publications/17budget/pdf/FY17BudgetBook.pdf (p. D-247).
[11] National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.
[12] Office of Governor Edmund G. Brown Jr. (2015). Governor Brown Signs Executive Order to Bolster Cybersecurity. Retrieved from https://www.gov.ca.gov/news.php?id=19083.
[13] State of New Hampshire Office of the Governor. (2016). An Order Establishing the New Hampshire Cybersecurity Integration Center and Executive Oversight Committee. Retrieved from http://sos.nh.gov/WorkArea/DownloadAsset.aspx?id=8589963332.
[14]Colorado General Assembly. (2016). House Bill 16-1453. Retrieved from http://www.leg.state.co.us/clics/clics2016a/csl.nsf/fsbillcont2/0528CBE6CA4319BD87257F3A007B1CEF/$FILE/1453_signed.pdf.
[15] Colorado General Assembly. (2016). House Bill 16-1453. Retrieved from http://www.leg.state.co.us/clics/clics2016a/csl.nsf/fsbillcont2/0528CBE6CA4319BD87257F3A007B1CEF/$FILE/1453_signed.pdf.
[16] State of Georgia. (2016). Georgia Cyber Innovation and Training Center. Retrieved from https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia Cyber Innovation and Training Center.pdf.
[17] State of Georgia. (2016). Georgia Cyber Innovation and Training Center. Retrieved from https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia Cyber Innovation and Training Center.pdf.
[18] Colorado General Assembly. (2016). House Bill 16-1453. Retrieved from http://www.leg.state.co.us/clics/clics2016a/csl.nsf/fsbillcont2/0528CBE6CA4319BD87257F3A007B1CEF/$FILE/1453_signed.pdf.
[19] State of Georgia. (2016). Georgia Cyber Innovation and Training Center. Retrieved from https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia Cyber Innovation and Training Center.pdf.
[20] State of Georgia. (2016). Georgia Cyber Innovation and Training Center. Retrieved from https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia Cyber Innovation and Training Center.pdf.
[21] State of Georgia. (2016). Georgia Cyber Innovation and Training Center. Retrieved from https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia Cyber Innovation and Training Center.pdf.
[22] Oregon State Legislature. (2017). Senate Bill 90. Retrieved from https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB0090/A-Engrossed.
[23] Oregon State Legislature. (2017). Senate Bill 90. Retrieved from https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB0090/A-Engrossed.
[24] Williams, Jake. (2017). "States Call for Collaboration with Federal Government on Cybersecurity." Fedscoop. Retrieved from. https://www.fedscoop.com/national-governors-association-call-for-federal-cybersecurity-collaboration/.
[25] Nevada Legislature. (2017). "Assembly Bill No. 471." Retrieved from https://www.leg.state.nv.us/Session/79th2017/Reports/history.cfm?ID=1067.
[26] State of Nevada: Governor's Finance Office. (2017). "Executive Budget 2017-2019." P. 2411-2412. Retrieved from http://budget.nv.gov/uploadedFiles/budgetnvgov/content/StateBudget/2018-2019/FY2017-2019_GovExecBudgetBook-

Online.pdf
[27] Oregon State Legislature. (2017). Senate Bill 90. Retrieved from https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB0090/A-Engrossed.
[28] Oregon State Legislature. (2017). Senate Bill 90. Retrieved from https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB0090/A-Engrossed.