Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

Room 029 State Capitol, Denver, CO 80203-1784
Phone: (303) 866-3521 • Fax: (303) 866-3855
lcs.ga@state.co.us • leg.colorado.gov/lcs

Memorandum

April 15, 2020

TO: Interested Persons

FROM: Jean Billingsley, Senior Research Analyst, (303) 866-2357

SUBJECT: State and Local Cybersecurity Collaboration

This memorandum describes how some states find new ways to share cybersecurity knowledge and resources with their local governments to improve the state's overall cybersecurity posture.

Federal Resources

In response to the growing number of cybersecurity threats, the federal government offers cybersecurity information, resources, and funding through agencies such as the Department of Homeland Security (DHS) Multi-State Information Sharing and Analysis Center (MS-ISAC). With over 9,000 members in 182 cities, it is one of the largest cybersecurity resources in the country. The federal Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018 created a federal agency that offers state and local governments expertise in infrastructure security, emergency communications, and risk management. Also, the State and Local Government Cybersecurity Act is a grant program for state and local governments to improve their cybersecurity resiliency measures. Even so, state and local governments may find it challenging to leverage federal resources with their existing resource and budget constraints.

COVID-19 and Cybersecurity Resources

Federal, state, and local governments have banded together to provide cybersecurity guidance and updated information as criminals continue to try to capitalize on cyber vulnerabilities as a result of COVID-19. In response to COVID-19 cyber threats, CISA developed, in collaboration with other federal agencies, state and local governments, and the private sector, an "Essential Critical Infrastructure Workforce" advisory list to assist state and local governments.[1] The recent federal COVID-19 stimulus bill includes grant funding opportunities for implementing cybersecurity initiatives. States have also provided COVID-19 guidance for local governments and citizens by creating dedicated COVID-19 web pages that include cybersecurity recommendations and resources.

[1] https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce

State Resources

Governments are often entrusted with safeguarding sensitive and confidential information for citizens and businesses. A 2019 report from MS-ISAC found a 55 percent increase in reported cybersecurity breaches compared to the previous quarter.[2] As local governments continue to recover and learn from breaches each year, states may be in an ideal position to collaborate with local governments to provide tactical, strategic, and cost-effective resources while still supporting local government autonomy. In 2019, the National Governors Association (NGA) and the National Association of State Chief Information Officers (NASCIO) found that several states were enhancing state and local partnerships. Listed below are collaboration efforts states have implemented to assist their local governments.

Colorado. The Colorado Threat Information Sharing network provides threat information to state agencies and local governments. In October 2019, the Governor's Office of Information Technology published its "Security Guidance and Resources for Local Governments".[3]

Georgia. Since 2018, the Georgia Cyber Center provides cybersecurity training and testing for local governments.

Indiana. The Indiana Cybersecurity Council created a toolkit that includes a statewide cybersecurity plan, incident response template, a training and exercise guide, and additional resources for local emergency managers.

Iowa. The Iowa Office of Information Security offers local governments cybersecurity workshops and services. The state also used 80 percent of its grant from the State Homeland Security Grant Program to fund IT security licensing, hardware, and tools for local governments.

Louisiana. The Information Security Team serves local governments as an escalation point for incident response assistance. Louisiana also seeks opportunities to assist local governments with cybersecurity preparedness, prevention, and detection. The Louisiana Cybersecurity Commission addresses cyber threats and includes an Emergency Support Function group to respond and perform forensic investigations for local incidents.

Michigan. The Chief Information Security Office program plans to establish cyber partners, such as local governments, to share information and resources. Cyber incident responses are provided by the Michigan State Policy Cyber Command Center and a group of volunteer incident responders.

New Hampshire. The state collaborates with local governments in planning for cybersecurity incident response and disaster recovery. It also conducts a statewide cybersecurity workshop focused on local governments to build relationships, collaborate, and share cyber incident resources.

---

[2] "Hot Topic," Department of Homeland Security: CISA, < https://www.cisecurity.org/cybersecurity-threats/ >, accessed on March 30, 2020.
[3] "Security Guidance and Resources for Local Governments," Colorado Governor's Office of Information Technology, < https://drive.google.com/file/d/1E6qVGG-pifDH5R77hwE5Bew-Cb4T3qsT/view >, accessed on April 13, 2020.

New Jersey. The Cybersecurity and Communications Integration Cell provides cybersecurity services to local governments, such as information, incident response, and remediation services. The state provides its local governments cyber products and training, such as an annual cyber symposium and a statewide threat grid at the county level, which includes MS-ISAC funding to monitor all 21 county networks.

North Carolina. The North Carolina Department of Information Technology (NCDIT) provides state resources and services to its local governments. NCDIT also partners with the North Carolina National Guard and North Carolina Emergency Management to help local governments.

Pennsylvania. The Pennsylvania Information Sharing and Analysis Center meets quarterly to collaborate with its local governments. Recent accomplishments include: (1) improving election security; (2) creating a pilot with a cyber-forensic provider; (3) providing training; and (4) reducing overall licensing costs.

Texas. In 2018, the state launched a Managed Security Services program to provide security device management, incident response assistance, and cybersecurity assessment services to local governments. The Texas Department of Information Resources also manages the response to the recent ransomware attacks that ultimately impacted at least twenty Texas local governments.

Wisconsin. Though the state's Cyber Response Teams, cybersecurity assistance is provided to local governments by managing the response to major incidents, analyzing threats, and exchanging critical cybersecurity information. The state also provides 75 percent reimbursement for local training and annual cybersecurity response exercises with its DHS grant funding.

Additional Opportunities

Even with the knowledge and expertise available through federal and state resources, local governments may still find it challenging to attain their cybersecurity goals and acquire resources. A 2018 NASCIO cybersecurity study explains that budget constraints, limited workforce talent, and increased threats continue to impact cybersecurity for state and local governments.[4] Furthermore, unless states and local governments continue to focus on cybersecurity training, the shortages in the cybersecurity workforce may increase. In 2017, ISC2, an international nonprofit security association, reported that the cybersecurity workforce gap is on pace to hit 1.8 million by 2022, a 20 percent increase since 2015.

In January 2019, NASCIO and NGA published a joint report encouraging states and local governments to join cybersecurity forces. According to the report, even though some states are implementing programs to address information sharing and collaboration with local governments, there continues to be a need to improve how governments share and leverage resources. The report explains that obstacles remain with regard to cybersecurity funding and jurisdictional disagreements. Recommendations for states to improve their working relationships with local governments include:

[4] "2018 Cybersecurity Study-States at Risk: Bold Plays for Change," NASCIO, < https://www.nascio.org/resource-center/resources/2018-deloitte-nascio-cybersecurity-study-states-at-risk-bold-plays-for-change/ >, accessed on March 29, 2020.

(1) working with state municipal leagues and county associations; (2) increasing and encouraging communication channels; (3) making local governments aware of the cybersecurity services offered to them; (4) exploring cost savings by including local governments in service contracts; and (5) pooling available resources.

State legislation. Many states have proposed legislation to support local governments and their cybersecurity efforts. Table 1 lists recent state legislation that supports local government cybersecurity improvements.

Table 1
State Cybersecurity Legislation

State	Year/ Status	Description	Bill
Florida	2020 / Pending	Urges DHS to administer cybersecurity grants	FL HM 525
Indiana	2020 /Adopted	Urges a study of potential dangers of cyber hacking and ransomware attacks on state and local governments	IN HR 42
Louisiana	2020 / Adopted	Provides for mandatory training in cybersecurity awareness for state and local employees, officials, and contractors	LA H 633
Maryland	2020 / Pending	Establishes a cybersecurity response team and requires certain funds to be dispersed to local jurisdictions	MD H 996
New Jersey	2020 / Pending	Concerns information security standards and guidelines for state and local governments	NJ A 1396
New York	2020 / Pending	Establishes civilian cybersecurity reserve forces within the state militia to protect election systems, businesses, and citizens from cyberattacks	NY A 8776
New York	2020 / Pending	Creates a cybersecurity enhancement fund to be used for upgrading cybersecurity in local governments	NY S 7246
North Carolina	2019 / Enacted	Makes technical changes, including state agency cybersecurity reporting to include local government incidents	HB 217
Ohio	2019 / Enacted	Provides funding for cybersecurity initiatives, including providing cyber training and education to students and government employees	OH H 166
Texas	2019 / Enacted	Revises provisions related to cybersecurity training for certain state and local government employees and state contractors	TX H 3834
Virginia	2020 / Adopted	Requests a study of susceptibility, preparedness, and tools for the state and local governments to respond to ransomware attacks	VA HJR 64

Source: National Conference of State Legislatures.