Enhancing The Role of Fusion Centers in Cybersecurity

Executive Summary

Fusion centers were created after the 9/11 terrorist attacks to facilitate the type of multijurisdictional information sharing needed to prevent another strike on the homeland. The centers provided a mechanism for state and local governments and the federal government to analyze, share, and disseminate information and intelligence.

In recent years, the growing number and sophistication of threats to the nation's cyber infrastructure have motivated governors to consider adding or expanding cybersecurity capabilities within state fusion centers.

Through fusion centers, states receive classified and unclassified information and intelligence from multiple sources across the nation and combine or "fuse" that information into "products" (for example, law enforcement notices and warnings) that help improve state and national readiness to respond to an attack or threat. Since their inception, fusion centers have become more sophisticated, uniform, and nationally networked. As they have matured and evolved, so have their missions. Originally designed to focus on terrorism, they now address a wider array of threats and hazards, including "accidents; technological events; natural disasters; warfare; and chemical, biological (including pandemic influenza), radiological, nuclear, or explosive events."[1]

Given states' leading role in promoting cybersecurity, using fusion centers as a way to enhance cybersecurity capabilities may be a practical solution to an emerging problem. Actions a governor can take to enhance the role of his or her state fusion center in cybersecurity include:

- Create a shared cybersecurity mission among homeland security, emergency management, IT, and law enforcement.
- Conduct an assessment of the state fusion center's capability to manage a cybersecurity mission.
- Develop a business and operations plan for the state's fusion center.
- Implement an outreach strategy to the private sector to identify existing information-sharing processes.
- Establish clear performance measurements for fusion center activities.

Fusion Centers and Their Role in Cybersecurity

Fusion centers are owned and operated by state and local governments and serve as focal points for state, local, federal, tribal, and territorial partners to receive, analyze, and share threat-related information. Currently, 78 centers exist—53 are owned and operated by states and territories and 25 by major urban areas.[2] Although specifics vary by state, fusion centers are generally staffed by professionals from law enforcement, homeland security, fire services, emergency response, public health, and the private sector.[3]

[1] U.S. Department of Homeland Security, *Federal Continuity Directive 1 (FCD 1): Federal Executive Branch National Continuity Program and Requirements* (Washington, DC: U.S. Department of Homeland Security, 2008), http://www.homelandsecurity.noaa.gov/FCD1.pdf (accessed July 1, 2015).

[2] The 53 state and territorial fusion centers are wholly owned and operated by the state, while the remainder of the fusion centers are located in major urban areas and operated by those jurisdictions, often in partnership with the state government.

[3] Nongovernmental participants include representatives from the public utility, financial, agricultural, and energy sectors.

Fusion centers were created in the wake of 9/11 to facilitate information sharing among public safety agencies to prevent terror incidents, protect citizens, and respond to crises. Fusion centers have focused on areas such as counterterrorism, disaster management, emergency response, protection of critical infrastructure, and drug trafficking. Although organizationally distinct, efforts are underway to better align and encourage mutual support across all of the nation's fusion centers. Those efforts aim to develop strategies to bridge jurisdictional boundaries as well as provide more effective communications about and effective response to the threat environment.

Fusion centers serve as a critical junction for state, federal, and private-sector intelligence collection, analysis, and dissemination. Similar to counterterrorism or disaster response, those centers play a critical role in mitigating and responding to cyber threats, sharing actionable intelligence about the latest attack and threat trends and strategies and enabling preventative action by state information security professionals. In addition, fusion centers can act as a center for coordinating the response to and investigation of cyber crimes and cyber intrusions against state assets and critical infrastructure.

Many fusion centers have begun to develop their cybersecurity capabilities. **Washington** established the Public Regional Information Security Event Management system and established a cyber intelligence analyst position in the state fusion center "to ensure that information on (cyber) threats and reconnaissance activity is shared in real time and across organizational boundaries."[4] In 2013, **New Jersey**'s fusion center, the Regional Operations and Intelligence Center, launched a "cyber fusion cell" to focus on emerging cyber threats to public and private networks.[5]

To better integrate cybersecurity into its state fusion center, **New York** physically relocated the New York State Intelligence Center (NYSIC) to the Center for Internet Security's (CIS) campus near Albany, New York. CIS is a 501(c)(3) nonprofit organization focused on enhancing the cybersecurity readiness and response of public- and private-sector entities. CIS has been designated by the U.S. Department of Homeland Security (DHS) to serve as the national hub for sharing cybersecurity information across states. According to New York Governor Andrew Cuomo, relocating his state's fusion center "will ensure new coordination between government, law enforcement, and public safety resources."[6]

The costs associated with building cybersecurity capabilities depend on a range of factors that vary by fusion center, but the largest cost driver is salaries for cybersecurity professionals. Those professionals are in high demand, and states face challenges across the board when seeking to hire them or contract with private firms that offer cybersecurity expertise.[7] Fusion centers may have anywhere from one part-time staff member to seven full-time-equivalent cybersecurity professionals, with a national goal of averaging three staff members per center. To meet the demands of the cyber threat, fusion centers might have one full-time cybersecurity analyst and a number of all-threat analysts who devote a portion of their time to cyber analysis. As an alternative to hiring, fusion centers can augment their capabilities by developing a cyber internship program or by incorporating analysts from the private sector (and paid by the private sector) into the fusion center. Costs are also associated with

---

[3] Nongovernmental participants include representatives from the public utility, financial, agricultural, and energy sectors.
[4] Office of the Chief Information Officer, Washington State, "The Public Regional Information Security Event Management (PRISEM) System," https://www.ocio.wa.gov/news/prisem (accessed November 10, 2014).
[5] The State of New Jersey Office of Homeland Security & Preparedness, "Cybersecurity," http://www.njhomelandsecurity.gov/cybersecurity (accessed November 10, 2014).
[6] New York State, "Governor Cuomo Announces Partnership with National Center for Internet Security to Strengthen New York's Cyber Security," Press Release, November 18, 2013, http://www.governor.ny.gov/press/11182013-national-center-for-internet-security (accessed July 1, 2015).
[7] Laura Saporito, *The Cybersecurity Workforce: States' Needs and Opportunities* (Washington, DC: National Governors Association Center for Best Practices, 2014), http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1410TheCybersecurityWorkforce.pdf (accessed June 9, 2015).

procuring equipment and services, but such costs tend to be lower than those associated with personnel over the long term.

State law enforcement agencies are also beginning to develop ways to share existing resources and expertise. For example, the Association of State Criminal Investigative Agencies is developing an initiative whereby a state can request assistance from other states to respond in the event of a cyber attack, similar to the process by which a state requests assistance in the event of a natural disaster. Resource sharing may include technical capabilities, analytic surge capacity, intelligence analysis, and information sharing.

Fusion centers also have access to a variety of federally subsidized or discounted training programs, such as the U.S. Secret Service National Computer Forensics Institute, SANS Institute training, the Open Source Practitioners' Course, and the Federal Emergency Management Agency's Cyberterrorism Defense Initiative. Those programs can help ensure that a fusion center's cybersecurity analysts have the necessary technical and analytical skills at a low cost.

Recommendations for Enhancing Fusion Centers

Despite elaborate national efforts to share information about cyber threats (see Appendix on page 6, "National Cybersecurity Information-Sharing Assets"), states are not well equipped to contextualize the information they receive and tailor it to meet their own needs. Fusion centers can perform that essential function by providing critical analyses of the cyber threat intelligence they receive and disseminate. The following recommendations outline actions governors can take to enhance their state fusion center's cybersecurity role.

Create a Shared Cybersecurity Mission Across Homeland Security, Emergency Management, IT, and the State Police

Fusion centers were ostensibly designed to share sensitive information and intelligence among law enforcement and intelligence agencies. In many states, individuals responsible for cybersecurity, such as chief information officers (CIOs), chief information security officers (CISOs), emergency managers (EMs), and homeland security advisors (HSAs), might not have access to the fusion centers, either because they lack the security clearance or are not viewed as having a role. That lack of access bars critical personnel from receiving necessary information and intelligence and impedes a state's ability to combat new and emerging cyber threats.

To remedy that, governors can direct their CIO, CISO, EM, HSAs, and heads of state police to create a shared mission that defines roles and responsibilities for using the state's fusion center to support cybersecurity. **Vermont**, for example, integrated its fusion center into a statewide cybersecurity committee, bringing together the fusion center director, the state's EM, HSA, attorney general, and CISO to manage a shared cybersecurity mission. The committee meets regularly to discuss challenges and ensure that members are aware of each other's missions. That design allows state authorities to evaluate system security, effectively implement new policies, and maintain awareness of the evolving cybersecurity threat environment.

Conduct an Assessment of the State Fusion Center's Capabilities to Manage a Cybersecurity Mission

Governors can order an assessment of their state fusion center's ability to manage a cybersecurity mission. That assessment should identify the actions necessary for implementing the mission. The goal of the assessment is to inventory the state's assets and capabilities and see which ones can be brought to bear in support of a cybersecurity mission within the fusion center.

To achieve that goal, governors can direct their CIO, CISO, and heads of state police jointly to conduct an assessment of the state fusion center's ability to manage a range of cybersecurity information and operations.

Develop a Business and Operations Plan for the State's Fusion Center

An essential step in building cybersecurity capabilities in fusion centers is the development of a business and operations plan that clarifies roles, responsibilities, and procedures, sometimes referred to as a *concept of operations plan.* Such a plan should include estimates of personnel and other costs needed to support the mission. In addition to those basic elements, the plans should address how the state's efforts link to the national network of fusion centers and build on sources of critical information within the state, regionally, and nationally.

Recognizing the importance of developing effective business and operational cyber practices for fusion centers, the Office of the Director of National Intelligence's Program Manager for the Information Sharing Environment (PM-ISE), along with the International Association of Chiefs of Police, the Northern **California** Regional Intelligence Center (NCRIC), DHS, and MSISAC launched a pilot project comprising six fusion centers.[8] Through the project, those fusion centers are identifying best practices for sharing cybersecurity information and intelligence among the federal government; state, local, and territorial governments; and the private sector. The project highlights the importance of establishing a fusion center governance structure with cyber stakeholders and of developing critical policies to integrate cyber into the fusion center's broader mission. The goal is to share those business practices with other fusion centers.[9]

Implement an Outreach Strategy to the Private Sector to Identify Existing Information Processes

The threat of cyber intrusions is only one of many events that could adversely affect critical infrastructure. A majority of critical infrastructure, including cyber assets, resides in the private sector. The private sector has numerous processes in place through which information about threats and attacks is shared. The sector-specific ISACs are one example of such information-sharing processes. To the extent possible, states should work directly with the private sector to take advantage of existing information-sharing processes.

The **Kansas** Threat Integration Center (KSTIC) has effectively integrated private-sector partners, including representatives from the public utility, finance, agriculture, and energy sectors, to share cybersecurity information. The representatives participate in the fusion center on a part-time basis and have access to fusion center intelligence, which they can use to conduct analyses of their own systems to foster greater resilience. That relationship not only benefits the private-sector partners by increasing resiliency but also gives KSTIC and other state authorities insight into current vulnerabilities.

Similarly, NCRIC has developed a trusted relationship with major providers of utility services that face persistent cyber intrusions. Through that partnership, NCRIC aims to place utilities personnel within the fusion center. The arrangement allows for a timely two-way flow of information between the fusion center and the private sector. Such information sharing will allow the company to develop capabilities to improve its internal security and ensure that NCRIC produces actionable threat analysis for other critical infrastructure partners.

Establish Clear Performance Measurements for Fusion Center Activities

A major challenge facing state and local fusion cen-

[8] In addition to NCRIC, the project is working with the **Louisiana** State Analytical and Fusion Exchange, the Kansas City Regional TEW Interagency Analysis Center, **Wisconsin** Statewide Information Center, and NYSIC.

[9] As a component of that effort, NCRIC launched a requirements-setting process that brings together stakeholders from the law enforcement, homeland security, emergency management, and IT communities as well as state, local, and federal officials. Mike Sena, "Fusion Centers and Private Sector Come Together on Cybersecurity," ISE Blog, entry posted October 24, 2013, http://ise.gov/blog/mike-sena/fusion-centers-and-private-sector-come-together-cybersecurity (accessed November 5, 2014).

ters is how they demonstrate their worth. Critics have suggested that they do not produce sufficient value for the money spent on them. As states develop cyber capabilities within fusion centers, they should include performance measurement and communications components through which they can track and share their activities in both classified and unclassified environments. In many cases, the lack of solid performance data means that fusion centers must rely on anecdotal success stories to illustrate their value or risk becoming an easy target for budget cutters.[10]

As fusion centers build their cybersecurity capabilities, they should seek to establish as strong a record of performance as possible. Successful prevention, detection, response, or mitigation of a security breach or other cybersecurity threat should be measured against pre-established criteria. Stronger performance measurements and enhanced understanding of the benefits of cybersecurity capabilities within fusion centers would allow governors and their chief budget officers to better evaluate their mission against their costs.

Moving Ahead

Cyber intrusions against critical cyber infrastructure are one of the most serious threats facing the nation. The increasing frequency and sophistication of such intrusions is leading states to seek greater response capabilities. By implementing this paper's recommendations, governors can effectively use state fusion centers as assets in their efforts to identify and counter cyber intrusions. With fusion centers evolving to focus on all threats rather than strictly counterterrorism, enhancing their cybersecurity capacity is a natural next step. As with any program that relies on public funding, however, state fusion centers will need to be clear about their mission, track their performance, and demonstrate their value.

Timothy Blute
Senior Policy Analyst
Homeland Security and Public Safety Division
NGA Center for Best Practices
202-624-7854

July 2015

Recommended citation format: T.Blute. *Enhancing The Role of Fusion Centers in Cybersecurity* (Washington, D.C.: National Governors Association Center for Best Practices, July 16, 2015).

NGA would like to acknowledge the generous support of the following organizations for this issue brief: Citigroup; CGI Group; Deloitte Consulting LLP; FireEye, Inc.; Hewlett-Packard Company; Intuit Company; McAfee; Motorola Solutions Foundation; Palo Alto Networks, Inc.; Splunk; VMware, Inc.; and WalMart Stores, Inc.

[10] To highlight their role and collaborative efforts, DHS maintains a Web page that highlights a few select fusion center activity success stories from 2007 to 2013. U.S. Department of Homeland Security, "Fusion Center Success Stories," http://www.dhs.gov/fusion-center-success-stories (November 10, 2014).

Appendix. National Cybersecurity Information-Sharing Assets

As governors consider expanding their state fusion center's role in cybersecurity, they should also understand the role of five key national assets: information-sharing and analysis organizations (ISAOs); sector-specific information-sharing and analysis centers (ISACs); the Multi-State Information Sharing & Analysis Center (MSISAC); the Integrated Intelligence Center (IIC); and the National Cybersecurity and Communications Integration Center (NCCIC).

Information Sharing and Analysis Organizations (ISAOs) are organizations created to share and analyze information related to emerging cyber threats and cyber vulnerabilities. They can be categorized on the basis of "sector, subsector, region, or any other affinity."[11] In May 2015, **Virginia** established the first-ever state-specific ISAO.[12]

Sector-specific information sharing and analysis centers (ISACs) are entities created by owner-operators of critical infrastructure to help facilitate information sharing within those sectors.[13] ISACs conduct detailed sector analysis and disseminate information to entities within their sectors, to different sectors, and to government.[14] They provide risk mitigation, incident response, and alert and information sharing.

The Multi-State Information State Analysis Center (MSISAC), a component of CIS, is the ISAC for state, local, tribal, and territorial governments, as designated by DHS.[15] As such, MSISAC, along with DHS, helps collect, share, and analyze cybersecurity information with states.

The Integrated Intelligence Center (IIC), supported by CIS, provides fusion centers with access to a range of cybersecurity intelligence products that DHS and IIC collect and analyze.[16] The goal of IIC is to ensure that actionable information pertaining to cybersecurity is disseminated and shared with fusion centers in a timely fashion.[17]

DHS's National Cybersecurity & Communications Integration Center (NCCIC) provides ongoing cyber situational awareness, incident response, and management to the federal government, intelligence community, and law enforcement. Its mission is "to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the Nation's critical information technology and communications networks."[18] Working in coordination with the MSISAC, NCCIC shares information with states and the private sector about vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

---

[11] Office of the Press Secretary, The White House, "Executive Order—Promoting Private Sector Cybersecurity Information Sharing," Press Release, February 13, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (accessed May 11, 2015).

[12] Governor of Virginia, "Governor McAuliffe Announces State Action to Protect Against Cybersecurity Threats," Press Release, April 20, 2015, https://governor.virginia.gov/newsroom/newsarticle?articleId=8210 (accessed May 11, 2015).

[13] Those sectors include aviation, the defense industrial base, emergency services, electric, financial services, information technology, maritime security, communications, national health, nuclear, oil and gas, public transit, real estate, research and education, supply chain, surface transportation, and water.

[14] National Council of ISACs, "About Us: Information Sharing and Analysis Centers (ISACS)," http://www.isaccouncil.org/aboutus.html (accessed October 28, 2014).

[15] Multi-State Information Sharing & Analysis Center, "Mission & Objectives," http://msisac.cisecurity.org/about (accessed November 5, 2014).

[16] Scott McAllister and William F. Pelgrin, "Fusion Center Access to the CIS/MS-ISAC's Integrated Intelligence Center," Center for Internet Security, http://iic.cisecurity.org/about/JointLettertoFusionCenters.htm (accessed November 5, 2014).

[17] Ibid.

[18] U.S. Department of Homeland Security, "About the National Cybersecurity and Communications Integration Center," http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (accessed November 5, 2014).