Cybersecurity

Overview

With the evolution of technology and new cyber tools, new capabilities have emerged. However with these new technologies cybersecurity threats have increased creating threats to our government and private sector business. The continued cyber-attacks on our critical infrastructure is a threat on our society and continuity of government.

The Council of Governors (COG) approved the *2014 Joint Action Plan for State-Federal Unity of Effort on Cybersecurity (*joint action plan for cyber) on July 10, 2014[1]. The joint action plan is a collaborative effort of the Council and federal partners establishing an understanding to work together within the existing authorities and in cooperation with current resources while recognizing established executive orders.

Prior to the Council's July 2019 plenary meeting, Council governors answered a survey to identify priorities for the CoG's consideration.

Council state staff met with federal partners on 14 June 2019 to discuss the results of the governor's survey and identify collective priorities to be worked for the 2019-2020 Council session. During the June meeting, numerous lines of effort were identified and evaluated, with Duty Status Reform, disaster response, disaster mitigation, increasing eligibility for service, improving stakeholder trust and Cybersecurity being recommended to the Council for consideration.

The Council met July 24, 2019 to review the recommended lines of effort provided by staff and officially established cybersecurity as one of the top three priorities – led by Governor Pritzker of Illinois and Governor DeWine of Ohio, supported by the Department of Homeland Security (DHS)/Cybersecurity Infrastructure Security Agency (CISA) as the federal lead[2] to address the following focus areas:

1) Cyber Capacity and Coordination: Build cyber capacity of state and local partners, and coordination among the private sector, state and federal government.
2) Cyber Prevention: Protect against continuous threat through tactics such as a defined cyber prevention structure, criteria and best practices.
3) Cyber Response: Establish roles and responsibilities for cyber response based on incident.

Council Actions since July 2019 Plenary

States have identified concerns over the complexity of authorities related to cybersecurity dealing with critical infrastructure and the resources available to a state during an event. This is especially true as the lines between homeland security and homeland defense are starting to blur as nation-state actors such as Russia and China[3] attack a state's critical infrastructure. After thoughtful review and deliberation, the Cybersecurity Subcommittee has made the following recommendations:

[1] CoG July 2014 Cyber Joint Action Plan.
[2] Cyber POAM, 24 July 2019.
[3] Critical Infrastructure Protection-Actions Needed to Address Significant Risk Tasking the Electric Grid, *GAO*, August 2019.

- The 2014 Joint Action Plan[4] should remain and enduring foundational document as a charter for the cyber subcommittee and outlining the board agreements by all of the parties while aligning future initiatives under the document as lines of effort.
- The Subcommittee recognizes that today cyber affords our society many new opportunities and initiatives. These new opportunities have also created many challenges to cybersecurity that can create significant and long-term challenges to our society. Because of the numerous changes to affect our nation's security, it is recommended the Cyber Subcommittee remains active until no longer required by future Council of Governors.

The Cybersecurity Subcommittee has identified the following Lines of Effort. A detailed explanation of each Line of Effort can be found below.

- Establish a Cyber Incident Situational Awareness Tool/Information Sharing platform
- Establish a roles and responsibilities matrix to provide a better understanding of authorities and available resources to States.
- Cyber response authorities and capability

[4] CoG July 2014 Cyber Joint Action Plan.

Cybersecurity Roles & Responsibilities Matrix

This section is for state consideration for developing statewide collaboration

A successful approach to cybersecurity requires a whole of government approach in a public private partnership. The Governor should appoint a lead agent tasked to coordinate all state efforts to protect state and local government, critical infrastructure, businesses, and private citizens from cyber threats and attacks. Most importantly, the agent should be tasked with responsibility to grow a statewide partnership among private and public entities, leverage a Cyber Reserve of trained vetted civilians, and a Cyber Range.

Establish Cybersecurity Partnerships

The C3 is a group of individuals drawn from state agencies, local governments, universities, high schools, and business focused on four major lines of effort:

1) Create/enhance the Cyber Reserve as part of the state defense forces nested under The Adjutant General's Department.
2) Curate and share best practices and information with cyber defenders around the state.
3) Use the Cyber Range to support the other three efforts by providing a safe, secure cyber facility to educate and train cyber experts and students, to test cyber networks and programs, and to support cyber in emergency preparedness exercises.
4) Support education and workforce development efforts to grow the number of trained cyber professionals and to ensure these students are well trained and ready to work in the field of cybersecurity.

These four lines of effort interlock and support each other to provide an even stronger effort and involve a whole of government approach, supported by private partners, to improve the state's cyber security posture.

Establish a Cyber Reserve/SDF Capability

The Cyber Reserve is a volunteer force under the direction and supervision of the Adjutant General composed of trained civilians vetted and organized into teams based around the state. The cyber reserve/state defense force will support and protect state and local government, critical infrastructure, and businesses deemed vital by the governor from cyber threats and will help mentor and train new cyber talent. As part of the Organized Militia, when called to state active duty by the Governor, the members of the cyber reserve will be paid by the state and will be available to respond to cyber incidents.

Establish a Cyber Range

The Cyber Range is a secure cyber security test and training environment accessible for competitions, training, and as a testing environment for schools, governments, and businesses. Sites should be placed at locations around the state. The Cyber Range should be capable of serving students throughout the state and is connected to all public institutions of learning through your state's high speed fiber educational network.

Promote Cyber Education and Workforce Development

The C3 and the Department of Education should develop a Cyber Pathway curriculum for its technical pathways program. Additionally, develop a "cyber club in a box" tool kit to assist high schools in the establishment of cyber clubs throughout the state. The C3's Education and Workforce Development

subcommittee should bring together industry and academic experts to ensure educational institutions were teaching the right skills to prepare students to work in the
growing cyber security field and increase the number of individuals training to fill the many vacant positions in the cyber security. Coupled with the Cyber Range, these efforts provide hands on training for cyber security students, allowing them to be ready to go to work on day one after completing their studies.

Promote Secure Cyber Security Information Sharing

Develop trust relationships among public and private entities with an interest in cyber security. Create a "fusion center" for the sharing of cyber security information, threat vectors, and new vulnerabilities. Curate and distribute best practices in network and data security, and promote training in cyber hygiene for users. Ensure all actors are fully aware of the resources available at the local, state and federal level.

Actors and Agencies

Listed below are Actors, Roles and Responsibilities

FEDERAL	
DHS	Department of Homeland Security / Cybersecurity and Infrastructure Security Agency
DHS / US-CERT	United States Computer Emergency Readiness Team
DOJ / FBI	Department of Justice – Federal Bureau of Investigation
COC / NIST	National Institute of Standards and Technology
NICE	National Initiative for Cybersecurity Education
NSF	National Science Foundation
DOD	Department of Defense – Cyber Command
NSA	National Security Agency
NGB	National Guard Bureau
SSA	Secret Service Agency
MS-ISAC	Multi-State Information Sharing and Analysis Center
STATE	
SCSC	State Cyber Security Coordinator
NG	National Guard – The Adjutant General's Department
DAS	Department of Administrative Services
DHE	Department of Education
DPS	Department of Public Safety
LLE	Local Law Enforcement
Fusion Center	Homeland Security – Information Sharing Environment
C3	Cyber Collaboration Committee (A public / private collaboration of interested organizations and individuals to help make the state better at Cybersecurity
CR	Cyber Reserve
AG	Attorney General
CIS	Center for Internet Security
FedVTE	Federal Virtual Training Environment
NICCS	National Initiative for Cybersecurity Careers and Studies
CIO	State Chief Information Officer
CISO	State Chief Information Security Officer

State Cybersecurity Program – Roles & Responsibilities Matrix

Objective	Task	Consult/ Partner with	Agency/Agencies Responsible			Resources
			Federal	State/Local	Private/ Other	
#1: Fortify Current Cyber Postures	Develop or Curate Standards/Best Practices		NIST, NICE, DHS, DOD/NSA, NSF	DAS, Auditor, SCSC, NG, CIO/CISO	C3, MS-IASC, CIS	Cyber Essentials, NIST CSF, CIS Controls
	Outreach, Information, Sharing Cyber Hygiene, Cyber Standards	Trusted Partners	USCERT, DHS	Fusion Center, SCSC, CR CIO/CISO	MS-IASC	HSIN, C3VP
		General Public		SCSC	C3, MS-IASC	
		Students		Dept. of Education	C3, MS-IASC	
	Respond to Protect State and Local Cyber Networks	State Agencies	CISA	DAS, NG, CR, CIO/CISO	Vendors, MS-IASC	NIST CSF, Federal Response Playbooks
		Local Governments	CISA	DAS, NG, CR CIO/CISO through ESF	Vendors, MS-IASC	
		Critical Infrastructure	CISA, SSA	NG, CR	Vendors, MS-IASC	
		Private Citizen	CISA		Vendors, MS-IASC	
		Private Business			Vendors, MS-IASC	
	Investigate cyber attacks	All	FBI	AG, DPS, LLE, CIO/CISO		

State Cybersecurity Program – Roles & Responsibilities Matrix (Cont.)

Objective	Task	Consult/ Partner with	Agency/Agencies Responsible			Resources
			Federal	State/Local	Private/ Other	
#2: Cyber Security Education and Skills development and sustainment	Education Workforce Development (outreach, curriculum development, hands on)	K-12	DOD/NSA, NSF, NICE FedVTE, NICCS	Dept. of Education	C3	FedVTE, NICCS, NICE
		Career Tech			C3	
		Continuing Education/Adult	DOD/NSA, NSF, NICE	DHE, DE	C3	
		Higher ED	DOD/NSA, NSF, NICE	DHE	C3	
	Cyber Range – Education and Training Platform	Support Cyber Curricula	DOD/NSA, NSF, NICE	NG, DHE, DE, DAS, DPS	C3	FedVTE, NICCS, NICE
		Certification				
		Cyber Contests				
		Workforce Development				
#3 Identify Areas to Expand Governance, Policy, Authorities, Programs	Policies and Governance	State CIOs/CISOs Universities, AG	DHS/CISA	SCSC, State Legislatures CIO/CISO	C3	Nationwide Cyber security Review, US-CERT Case studies on Cyber Governance
	Authorities and Identification of Resources	State Legislatures, US Congress, DHS, NSF, NSA, other Grant Awarding bodies				US-CERT SLTT Toolkit, SLTT Government Leadership Agenda

Cyber Services and Resources

Template for POCs for Agencies & Actors

Support / Service	Source	Point of Contact	Contact Info
Standards	Federal: DOC/NIST, DHS/CISA/NICE, DoD/NSA, NSF		
	State/Local:		
	NGO:		
	Private Sector:		
	Critical Infrastructure:		
Best Practices	Federal: DHS/CISA/NICE, DoD/NSA		
	State/Local: DAS, Auditor, SCSC, NG		
	NGO: NGA Center for Best Practices		
	Private Sector:		
	Critical Infrastructure:		
Grants	Federal:		
	State/Local:		
	NGO:		
	Private Sector:		
	Critical Infrastructure:		
Policies and Governance	Federal:		
	State/Local:		
	NGO:		
	Private Sector:		
	Critical Infrastructure:		
Plans	Federal: DHS/CISA, DoD/NSA, DoD/USCYBERCOM		
	State/Local:		
	NGO:		
	Private Sector:		
	Critical Infrastructure:		
Cyber Capabilities Development	Federal: DHS/CISA, DoD/NSA, DoD/USCYBERCOM		
	State/Local: OH		
	NGO:		
	Private Sector:		
	Critical Infrastructure:		

Cyber Incident Situational Awareness Tool

Overview & Goals

The SLTT community needs is common place for situational awareness of cyber incidents, and incident response as necessary. The Council of Governors (CoG) members believe leveraging an existing capability is the best path forward. The Cyber Intelligence Network (CIN) is an existing real-time collaboration tool operated by the Homeland Security Information Network (HSIN). One key benefit of using an existing capability is that HSIN is a known commodity used throughout the country in state's Emergency Management Operation Centers and Fusion Centers.

The CIN is an association of cyber analysts across the country dedicated to responding to cyber incidents, sharing cyber intelligence, and producing analytic products on cyber threats. The CIN's mission is to support the free and rapid exchange of cyber intelligence. Through the CIN, cyber analysts: (1) Share information rapidly, (2) Coordinate and prevent the duplication of efforts, and (3) Connect with each other, so analysts know who their counterparts are nationwide and can rely on them when needed.

The CIN is integrated with the Multi-State Information Sharing & Analysis Center (MS-ISAC) Security Operation Center (SOC) (24/7/365 cybersecurity operations center) which provides real-time network monitoring, threat analysis, early cyber threat warnings and advisories, including enhanced netflow/IPFIX, intrusion detection and intrusion prevention, vulnerability identification, and mitigation and incident response.

- Goal 1: The CoG will adopt and promote the CIN as the states' primary situational awareness and tactical information sharing platform.
- Goal 2: The states will actively participate in CIN as the primary situational and tactical information sharing platform.
- Goal 3: Create a common forum to provide SLTT and Federal with situational awareness of cyber incidents.
- Goal 4: Create an environment for SLTT and Federal analysts to share cyber related intelligence and information

Objectives

- Objective 1: The CoG will promote the use of CIN for the primary situational awareness and tactical information sharing platform.
- Objective 2: Develop a Concept of Operations (CONOPs) for the use of CIN as the states' Cyber Threat Intelligence and Collaboration Platform.
- Objective 3: Review and update Standard Operating Procedures (SOPs) for the use of CIN as the sates' situational awareness and tactical information sharing platform.
- Objective 4: Identify and improve on any deficient issues with CIN, both procedural and technical to meet the needs of the states.

Stakeholders

- Governors' Homeland Security Advisors (HSA's).
- State Fusion Centers.
- DHS/CISA.

- State Chief Information Security Officer (CISO)

Deliverables

- Awareness material (document(s) explaining the 5Ws of the CIN).
- Briefing(s) provided by HSIN and CIN subject matter experts.
- Instructions on how to access CIN.
- Draft CONOPs for the use of CIN as the states' situational awareness and tactical information sharing platform.
- Draft SOPs for use of CIN as the states' situational awareness and tactical information sharing platform.

Timeline

The Playbook finalized and approved by the Council of Governors by the end of February 2020.

Cyber Response Authorities & Capability Overview

During the June 14, 2019 Council staff level working group meeting, a Plan of Action and Milestones (POAM)[5] for Cybersecurity was developed. Within the POAM, states and federal partners identified cyber response as one of the three lines of effort.

The POAM identified the need to establish roles and responsibilities for cyber response based on the incident. This includes prevailing authorities available to a state for cybersecurity and the protection of critical during an incident. Additionally, the subcommittee should evaluate if there is a need for new authorities.

The new and dangerous ability to attack a state entity without fear of retribution, and at little cost or risk[6] makes cybersecurity an extremely attractive attack vector for criminals and nation states. This is one of the reasons the 2018 National Defense Strategy highlight that the "**homeland is no longer a sanctuary**"[7]. This ability to attack, combined with the vulnerability of critical infrastructure to a cyber-attack and importance of this infrastructure to life, safety and normal way of life for the citizens of our states is why the cybersecurity subcommittee finds this topic extremely important.

As outlined by the President's National Infrastructure Advisory Council's (NIAC) report "Transforming the US Cyber Threat Partnership", dated December 12 2019, "**Mr. President, escalating cyber risks to America's critical infrastructures present an existential threat to continuity of government, economic stability, social order, and national security. U.S. companies find themselves on the front lines of a cyber war they are ill-equipped to win against nation-states intent on disrupting or destroying our critical infrastructure. Bold action is needed to prevent the dire consequences of a catastrophic cyber attack on energy, communication, and financial infrastructures. The nation is not sufficiently organized to counter the aggressive tactics used by our adversaries to infiltrate, map, deny, disrupt, and destroy sensitive cyber systems in the private sector."**[8]

Growth of Ransomware & Attacks on Critical Infrastructure

A quick review of today's news, a reader will find many articles concerning ransomware attacks on communities throughout the nation. Many states including Colorado[9], Georgia[10], Louisiana[11], Maryland[12], and Texas[13] to name a few, have received attacks upon all types of critical infrastructure. This critical infrastructure includes department of transportation databases, law enforcement systems, primary education networks, power distribution and water distribution facilities. These attacks are compounded by continued intrusions that occurred upon the elections systems and critical infrastructure in 2016 and 2018. An attack on voting systems occurred in almost every state across the nation[14], creating doubt of the validity of U.S. elections.

---

[5] Cyber POAM, 24 July 2019.
[6] The Cost of Cybercrime; *Accenture Security*; 2019.
[7] The 2018 National Defense Strategy; October 2018.
[8] The President's National Infrastructure Advisory Council; Transforming the US Cyber Threat Partnership, December 12, 2019
[9] SamSam Ransomware Attack Costs $1.5 Million to Colorado Department of Transportation; *Cybersecurity Insiders*, Marcy 2019.
[10] Georgia Charges Iranians in Ransomware Attack on Atlanta, *NPR*, December 5, 2018.
[11] Louisiana's Governor Declared a State of Emergency After a Cybersecurity Attack on Government Servers; *Business Insider*, November 23, 2019.
[12] Cyber Attacks Holding Baltimore Hostage, Threatening $10,000 a Day; *Daily Caller*, May 21, 2019.
[13] Texas Cyber Attack Has Taken 23 Government Agencies Offline, *Forb*es, August 19, 2019.
[14] Russia Targeted Election Systems in All 50 States, Report Finds; *New York Times*, July 25, 2019.

The origins and reason for the attacks are difficult to trace and many times the victim does not know the attack has occurred until the perpetrator notifies the victim of the attack, such as in the case of ransomware or until months later or years later. These brutal attacks have resulted in states developing new authorities to declare a cyber emergency[15] and to assist in mustering the required resources to recover from the attack(s); using the same approach that may be used to recover from a natural disaster such as a fire, flood or a hurricane.

What makes this problem more complex, is critical infrastructure can be owned by different entities such as federal, state, local, tribal and territorial (SLTT) governments or by privately held companies. When you combine these new threats, from different actors to include criminals and nation state actors, along with different owners of the critical infrastructure, approaches to preparedness and response can vary greatly and create significant challenges for responders.

Cybersecurity Challenges: Response

Although the national response model[16,17] identifies DHS/CISA as the agency to protect critical infrastructure and DOD to defend the nation from attack, the plan does not detail a comprehensive strategy and responsibility to support a cyber response. Without clear responsibilities identified at the federal government level, assistance is limited or does not exist based on the severity of the attack, leaving SLTT or a private sector business to defend against these cyber-attacks.[18]

When an attack does occur, typically a state Security Operations Center (SOC) will provide the initial response gathering information about the attack. Based on the severity, size and complexity, the SOC could seek outside assistance.

This assistance can vary based on available resources, but will typically be in the following order:

1) Contracted support from companies specializing in cybersecurity.
2) National Guard response in State Active Duty (SAD) status.
3) DHS/CISA Hunt & Incident Response Team (HIRT).
4) National Guard response under Operational Training Federal Authority (T32).
5) DoD Response (T10 or T32) under the Economy Act.

During a typical cyber event, states will normally provide an initial response by a cybersecurity team within their lead Information Technology/Cybersecurity agencies. Many states have developed a Cyber Annex to their All-Hazards Response Plans that appoint a lead state cybersecurity agency. Based on the severity and uniqueness of the attack, the State Cybersecurity officials could request support from a contracted cybersecurity company that can provide specialized experience and tools. If the scope of the attack is large enough or threatens public safety, the governor can mobilize the National Guard into a State Active Duty (SAD) status to provide additional capacity to the response.

At this point during an elevated response, the state has borne a majority of the response effort, with the exception of coordination with CISA or an Information Sharing and Analysis Center (ISAC) that might be aware of new threats. CISA maintains a Cyber Incident Scoring System[19] to provide an incident-rating scheme based on National Institute of Standards and Technology (NIST) standards. This system

---

[15] Louisiana's Governor Declared a State of Emergency after a Cybersecurity Attack on Government Servers; *Business Insider*, November 23, 2019.
[16] National Strategy, Roles, and Responsibilities Need to be Better Defined and More Effectively Implemented; *GAO*, February 2013.
[17] US Federal Cybersecurity Operations Teams, National Roles and Responsibilities; March 5, 2013.
[18] With U.S. Cyber policy, clear lanes still hard to come by; *Federal Computer Week*, November 25, 2019.
[19] Department of Homeland Security/CISA NCCIC Incident Scoring System.

assigns a numeric rating for each incident to provide a repeatable and consistent mechanism for objectively evaluating the risk of a cybersecurity incident in the national context. This system rates the event based functional impact, observed activity, location of observed activity, actor characterization, information impact, recoverability, cross-sector dependency and potential impact. If the threat is significant and widespread effecting critical infrastructure, it could trigger the deployment of a HIRT from CISA.

The National Guard could be federalized and used under USC Title 32-502(f) at the direction of President or Secretary of Defense to support a homeland defense (HLD) response. In an extreme situation, DHS could request support from DOD through the Economy Act to field more cyber forces from the active duty (Title 10) or the National Guard (Title 32). Unfortunately, the Economy Act process is very slow and may not be the best option during an emergency.

Because of the limited response from the federal government, SLTT and America's companies have no other choice but to combat these cyber-attacks on their own. As outlined by the President's National Infrastructure Advisory Council's **"America's companies are fighting a cyber war against multi-billion-dollar nation-state cyber forces that they cannot win on their own. Incremental steps are no longer sufficient; bold approaches must be taken".**[20]

Cybersecurity Response – Timeline of Next Steps

1) The Departments of Homeland Security and Defense are currently working to define roles and responsibilities at the federal level related to cybersecurity response efforts. DHS and DOD will provide the Council a read out once authorities are established.
2) Federal partners have requested that Council states work to put forward a list of gaps and challenges that require federal assistance or support.
3) The Department of Defense has agreed to provide a briefing to the Council on its feasibility and advisability study as it relates to the National Defense Authorization Act 2019[21] of a cyber civil support team/cyber mission assurance team concept.
4) The National Guard Bureau will provide a briefing concerning three State pilot Cyber Mission Assurance Teams and detail the results and commendations from the pilot program.
5) The Department of Homeland Security /Cybersecurity Infrastructure Agency will provide an overview of the whole of government cyber response plan in the case of a catastrophic cyber event and detail the use of the Economy Act in such an event and the possibility of a cyber "Stafford Act" to support STLL response.

These updates will assist the Cybersecurity Subcommittee in the development of recommendations for next steps in the development of a Cyber Response Plan and resourcing of such actions.

[20] The President's National Infrastructure Advisory Council; Transforming the US Cyber Threat Partnership, December 12, 2019.

[21] John S. McCain National Defense Authorization Act of 2019, Public Law 115-232, Section 1653*; DoD and DHS Report to Congress-Feasibility and Advisability of Establishing a Reserve Component Cyber Civil Support Team for Each State,* 2019.