Kansas Cybersecurity Task Force

Welcome

- Executive Order 21-25
- Establishing the Governor’s Cybersecurity Task Force

Governor’s Remarks

To listen to Governor Laura Kelly’s remarks, please visit the video available at www.youtube.com/watch?v=iecDnEmKnss. Governor Kelly’s remarks begin at the 4:25 mark.

Members and Introductions

State Chief Information Technology Officer or designee: Secretary Dr. DeAngela Burns-Wallace	State Chief Information Security Officer or designee: Jeff Maxon, Topeka	The Adjutant General of the Kansas National Guard or designee: Col. David Hewlett, Wichita	The Attorney General or designee: Jay Emler, Lindsborg	The Secretary of State or designee: Kevin Comstock, Topeka
Representative from the Kansas Department of Emergency Management: Jonathan York, Topeka	Director of Kansas Criminal Justice Information System: David Marshall, Topeka	Director of the Kansas Intelligence Fusion Center: William (Bill) Glynn, Topeka	Representative from a municipal governments: Mike Mayta, Wichita	Representative from the Regents institution: John Godfrey, Shawnee
Representative from critical infrastructure: Charles King, Overland Park	Representative from critical infrastructure: John Berghuis, Salina	Representative from the Joint Committee on Information Technology: Representative Kyle Hoffman, Coldwater	Representative from the Joint Committee on Information Technology: Senator Jeff Pittman, Leavenworth	Representative of county governments: Doug Peters, Garden City, Finney County

Charges

Facilitate	Identify	Identify	Develop	Develop	Recommend	Recommend
Facilitate cross-industry and cross-government collaboration to share best practices and mitigate cybersecurity risks related to critical infrastructure and protected systems;	Identify opportunities to improve the overall cyber security posture across all levels of government within Kansas;	Identify partnerships and avenues to maximize and leverage existing cybersecurity resources within the state;	Develop a framework for coordinated information sharing, response, simulation, testing, and mutual assistance between the government and private sectors;	Develop a coordinated and collaborative State of Kansas Cyber Response Plan;	Recommend appropriate and cost-effective safeguards to reduce, eliminate, or recover from identified threats to data;	Recommend resources and possible methods to accomplish the recommendations identified above;

Deliverables

EO WAS SIGNED JULY 13TH

WITHIN 90 DAYS OF THE DATE OF THIS ORDER, SUBMIT TO THE GOVERNOR AN INITIAL REPORT DETAILING RECOMMENDATIONS AND PROPOSALS FOR THE TASK FORCE'S FUTURE WORK.

FIRST DELIVERABLES ARE DUE FRIDAY OCTOBER 8TH , 2021

BY DECEMBER 5TH, 2021, THE TASK FORCE SHALL SUBMIT A COMPREHENSIVE REPORT AND RECOMMENDATIONS TO THE GOVERNOR.

NATIONAL GOVERNORS ASSOCIATION

NGA Policy Academy to Advance Whole-of-State Cybersecurity

Kansas

August 2021

The National Governors Association

Over 100 years of serving our nation's governors

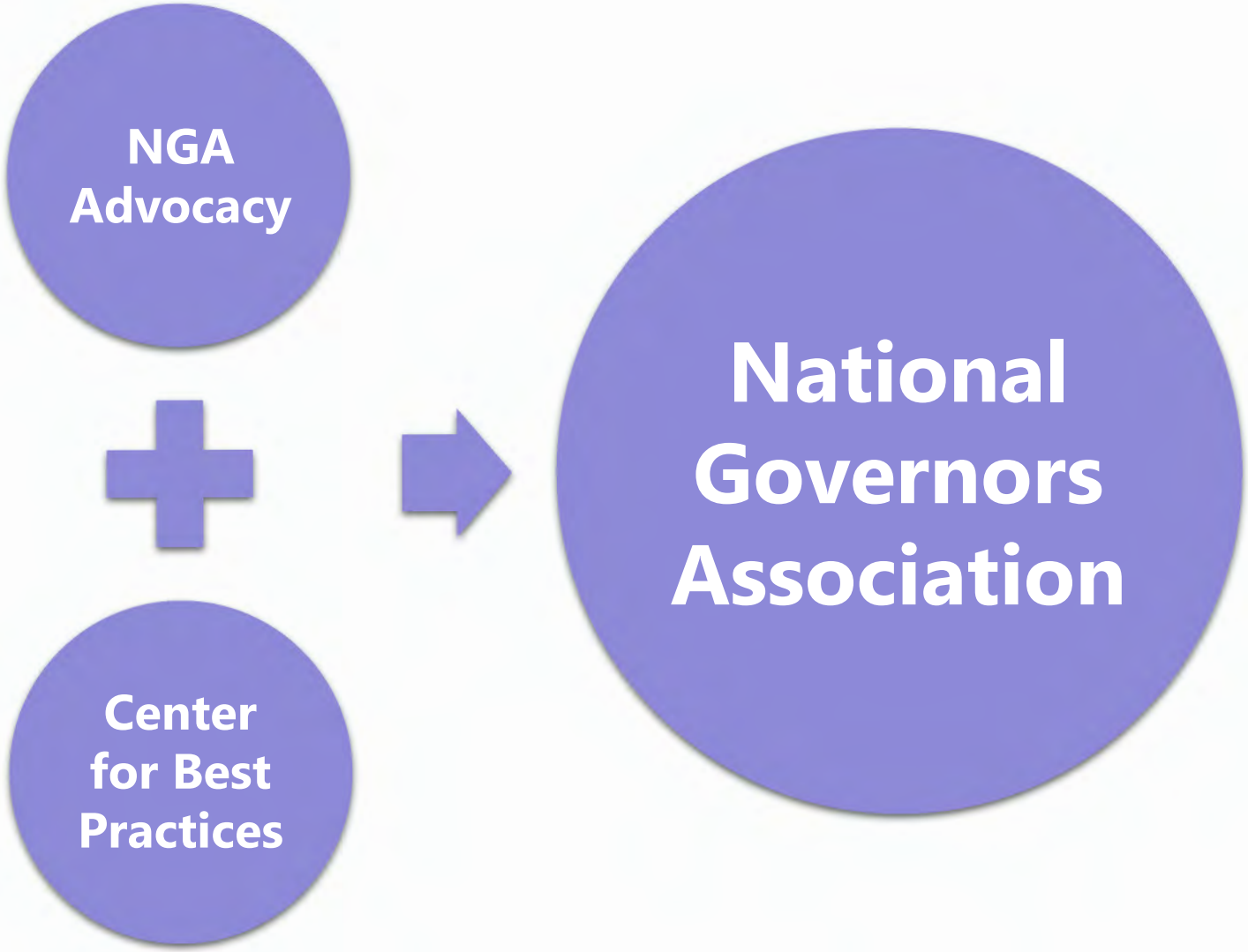
Founded in 1908, the National Governors Association (NGA) is the nonpartisan organization of the nation's 55 governors. Through NGA, governors share best practices, address issues of national and state interest and share innovative solutions that improve state government and support the principles of federalism.

NATIONAL GOVERNORS ASSOCIATION

The National Governors Association

Organization

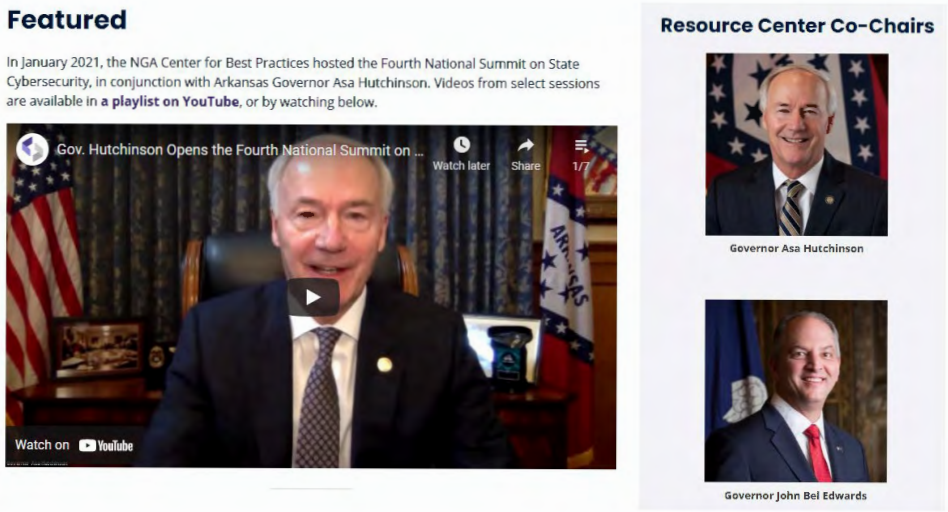
The NGA Center for Best Practices is a 501(c)(3) and part of our larger organization.



The Center for Best Practices Program Areas

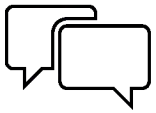
NATIONAL GOVERNORS ASSOCIATION

NGA Resource Center for State Cybersecurity

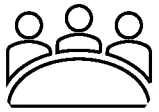


https://www.nga.org/statecyber/

How We Work With States



Policy Academies: Over a year long engagement, the program supports governor-appointed teams in developing and implementing strategic plans designed to address critical state policy challenges.



Policy Institutes and Workshops: The program hosts an annual policy institute for governors' criminal justice policy advisors and other workshops on specific topics to bring governors' staff together with subject-matter experts to exchange ideas and identify best practices.

Conference Calls and Webinars: The program regularly hosts conference calls and webinars to highlight new and emerging issues and provide a forum for peer-to-peer exchange.

Publications: Practical materials to inform governors' offices about available policy options to address pressing public criminal justice and public safety issues.

Technical Assistance: Staff can provide tailored assistance to governors' offices upon request. Assistance can come in a variety of forms, including brief confidential memos addressing a specific policy question, comments on draft legislation or regulations as related to best practices, consultations on a policy development process or access to outside experts.

NATIONAL GOVERNORS ASSOCIATION

What is a Policy Academy Anyways?

- Definition: Year-long engagement with NGA to provide in-depth technical assistance.
- States selected on competitive process.
  - Most competitive to date!

Application: Priority Areas

Critical Infrastructure Cybersecurity

State-Local Partnerships

Workforce Development

State Innovations

NGA's 2021 Policy Academy to Advance Whole-of-State Cybersecurity

Governance

Workforce Development

State-Local Partnerships

Policy Academy Benefits:

- Subject Matter Expertise
- Neutral, Third-Party Facilitation
- Provides Impetus for Action
- “Pilot State” – Outcomes Serve as a National Model

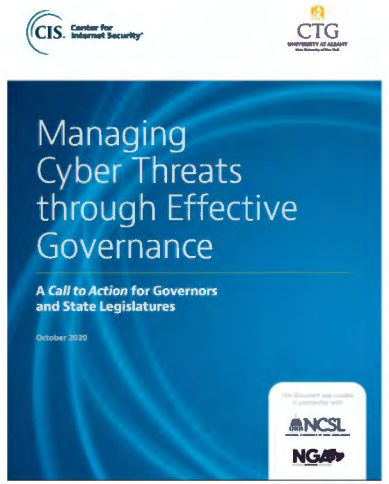
Policy Academy Activities :

What?	Who?	When?
Preparation and Kickoff	Core Team & Home Team	✓
Research, Learning Calls, Technical Assistance	Core/Home Team Members as Relevant	Throughout Project Period – as needed basis
Virtual Check-Ins	Core Team	Throughout Project Period – biweekly basis
Cohort Convenings (Virtual)	Core Team	Throughout Project Period – monthly basis
1st In-State Strategic Planning Workshop (Virtual)	Core Team & Home Team	April – July 2021
2nd In-State Strategic Planning Workshop (In-Person)	Core Team & Home Team	August – December 2021
Wrap Up	Core Team	December 2021 – January 2022

Cybersecurity Governance

- Definition: the processes by which decisions are made about cybersecurity risk.
- No "One-Size-Fits All" Approach
- Limited Academic/Scientific Research

DHS-NASCIO Cybersecurity Governance Case Studies

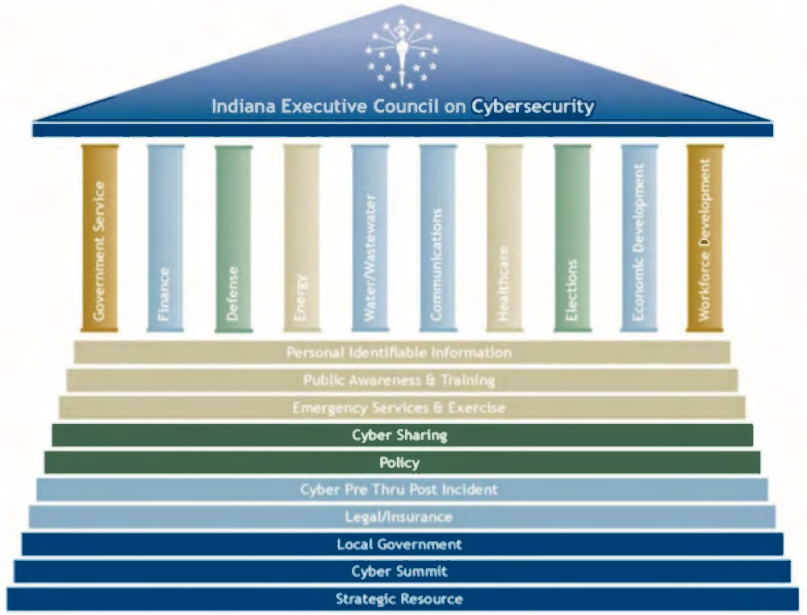


CIS White Paper on Managing Cyber Threats Through Effective Governance

Cybersecurity Governance: State Examples

Louisiana Cybersecurity Commission

Indiana Executive Council on Cybersecurity

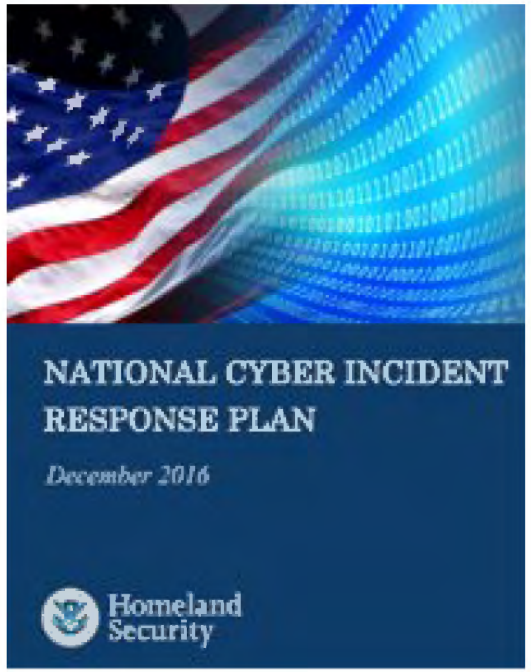


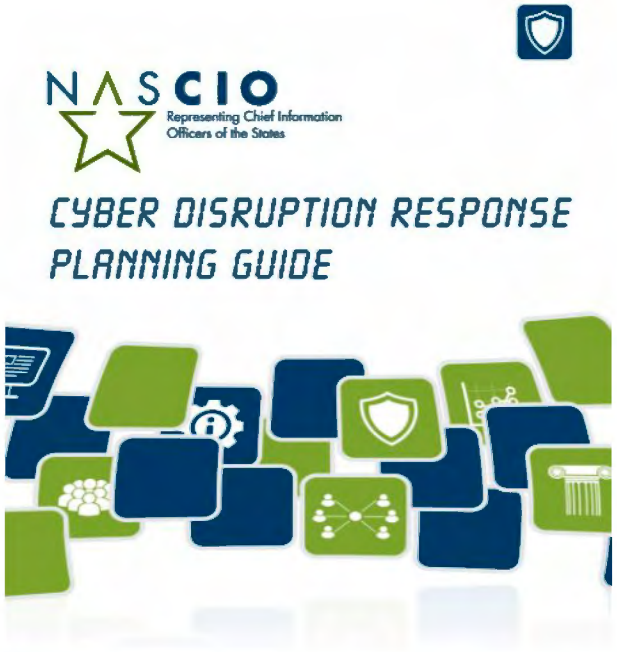
Cybersecurity Governance: State Examples

Cal Cybersecurity Taskforce & CAL CSIC

New Jersey CCIC

Cyber Disruption Response Planning





NGA MEMO: State Cyber Disruption Response Plans

DHS National Cyber Incident Response Plan (NCIRP) & PPD-41

NASCIO GUIDE: Cyber Disruption Response Planning Guide

Threat Matrices/Escalation Protocol

Figure 1: Cyber Incident Severity Schema

Description	Disaster Level	Cyber Incident Severity	Description	Observed Actions
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.	Effect
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.	Presence
		Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	Engagement
		Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.	
No event or incident anticipated. This includes routine watch and warning activities.	Level 4	Level 0	Unsubstantiated or inconsequential event.	Steady State

Source: Presidential Policy Directive 41, United States Cyber Incident Coordination.

DHS National Cyber Incident Response Plan (NCIRP) & PPD-41

How have states operationalized this?
Ex: **North Carolina**

CYBER DISRUPTION ESCALATION PROTOCOL			
LEVEL	**COLOR**	**DESCRIPTION / IMPACT**	**BASELINE CYBER SUPPORT**
Emergency	Black	Poses an imminent threat to the provision of wide-scale critical infrastructure services, State government stability, or the lives of North Carolina residents.	State of Emergency is declared. Full Cyber package which may contain National Guard, Private Sector, State and Federal Cyber resources. EMAC support may be requested. Incident reporting by affected party is mandatory.
Severe	Red	Likely to result in a significant impact to public health or safety, economic security, foreign relations, or civil liberties. Involvement of any actual, suspected, or potential breach of bulk Restricted or Confidential Data.	State of Emergency is declared. Full Cyber package which may contain National Guard Defensive Cyber Operations, Private Sector and State Cyber resources. Incident reporting by affected party is mandatory.

Responsibilities Associated w/ CDR

Table 1: NCIRP Lines of Effort[13]

Threat response	Asset response	Intelligence support	Affected entity response
• Investigative, forensic, analytical and mitigation activities. • Interdiction of a threat actor. • Providing attribution.	• Furnishing technical support to affected entities. • Mitigating vulnerabilities, identifying additional at-risk entities. • Assessing affected entities' risk to the same or similar vulnerabilities.	• Activities to better understand the cyber incident and existing targeted diplomatic, economic or military capabilities to respond. • Sharing threat and mitigation information with other potentially affected entities or responders.	• Maintaining business or operational continuity. • Mitigating potential health and safety impacts. • Addressing adverse financial impacts. • Protecting privacy • Managing liability risk; complying with legal and regulatory requirements (including disclosure and notification). • Engaging in communications with employees or other affected individuals. • Managing external affairs.

1. **Threat**
2. **Asset**
3. **Intel**
4. **Entity**

NGA Memo on State Cyber Disruption Response Plans: https://www.nga.org/wp-content/uploads/2019/04/IssueBrief_MG.pdf

Lessons Learned from AARs

COLORADO SAMSAM ATTACK ON CDOT

- March 2018
- Implemented ICS
- Activated National Guard
- EMAC request for cyber personnel
- Public AAR

LOUISIANA SCHOOL DISTRICT RANSOMWARE

- July 2019
- First instance of declaration for a local entity
- Activated National Guard
- Used private sector volunteers
- Coordinated through GOHSEP

Contact

John Guerriero
Acting Program Director
Cybersecurity Program
Jguerriero@nga.org

Questions?

Kansas Cybersecurity Landscape

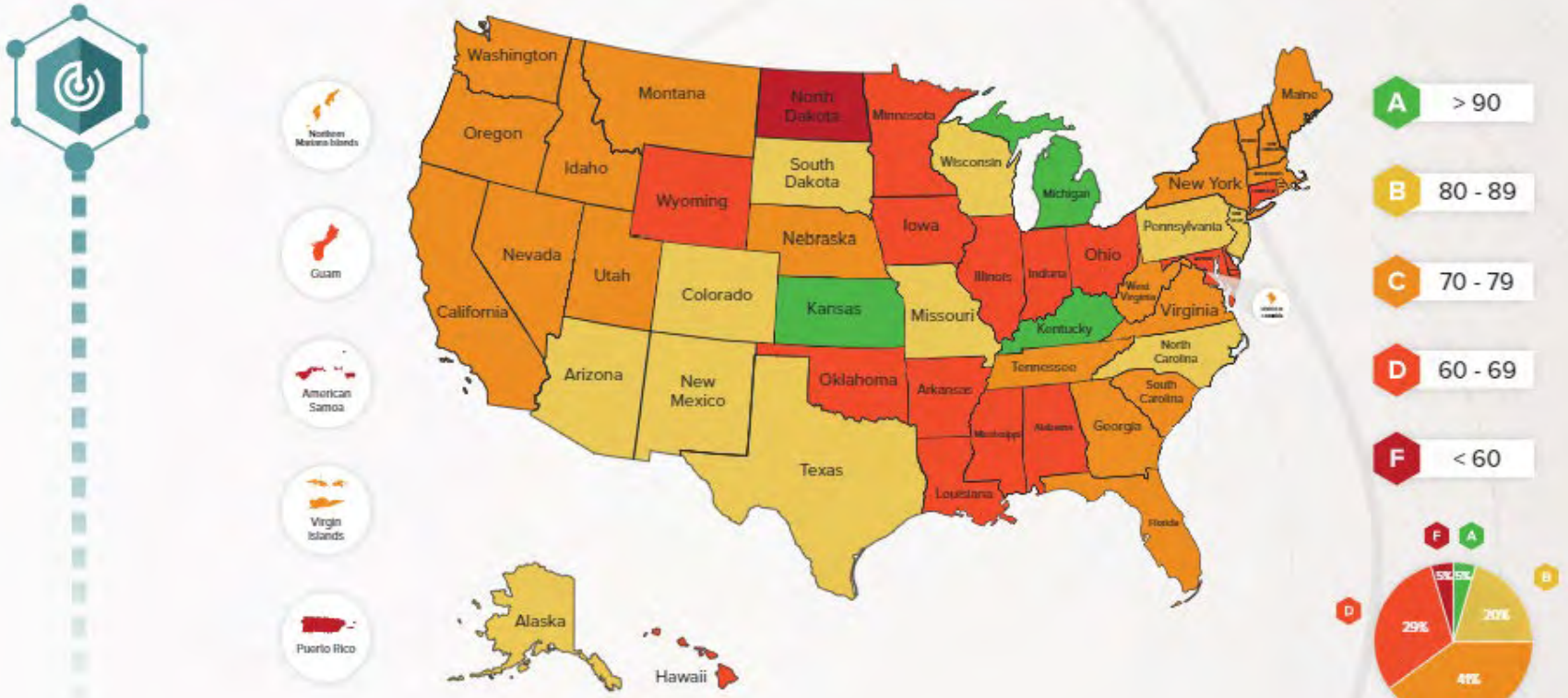
Webroot Riskiest State Surveys

- 2018: 41st
- 2019: 44th
- 2020: 20th

SecurityScorecard

State of the States

SecurityScorecard reviews overall cybersecurity posture, including election-related infrastructure, of all 56 U.S. states and territories



Kansas Cybersecurity Legislation

21: Crimes and Punishment	48: Militia, Defense and Public Safety	50: Unfair Trade and Consumer Protection	75: State Departments; Public Officers and Employees
• 21-5839. Unlawful acts concerning computers.	• 48-3701. Kansas Intelligence Fusion Center Act. 48-3701 through 48-3710,.	• 50-7a01. Consumer information; security breach; definitions50-50-7a02. Security breach; requirements	• 75-7236. Kansas cybersecurity act. K.S.A. 75-7236 through 75-7243

Kansas Information Security Office

- Established in 2018
- Supports executive branch information security programs
- Protects state enterprise network
- Collaborate with external partners to enhance security posture
- Assist agencies in preparing for and responding to cyber incidents

Kansas Bureau of Investigation

- Established a cyber crimes unit in 2019
- Respond to and pursue criminal cases for various cyber events
- Collaborate with federal partners

Kansas Division of Emergency Management

- Maintains and Manages the Kansas Response Plan
- Kansas Response Plan provides policy and guidance for emergency management
- Describes procedures for responding to an emergency
- Contains procedures for various types of incident

Kansas Intelligence Fusion Center

Partnership between the Attorney General's Office and Adjutant General's Department

Intelligence analysis and sharing

Partners with critical infrastructure and public entities

Kansas National Guard

- Defensive Cyber Operations Element
- 184th Cyberspace Operations Group
  - 299th Network Operations Security Squadron
  - 177th Information Aggressor Squadron (Red Team)
  - 127th Cyberspace Operations Squadron (Blue Team)

Critical Infrastructure in Kansas

Cybersecurity Programs in Kansas

- Butler Community College
- Fort Hayes State University
- Friends University
- Johnson County Community College
- Kansas City Kansas Community College
- Kansas State University
- University of Kansas
- University of Saint Mary
- Wichita State University

NSA/DHS Centers Academic Excellence

School	Designation
Butler Community College	Cyber Defense Education
Johnson County Community College	Cyber Defense Education
Kansas State University	Research
University of Kansas	Cyber Defense Education, Research
Wichita State University	Cyber Defense Education

Higher Education Research

- University of Kansas is one of the six Science of Security Lablets funded by the NSA Research Directorate to conduct foundational research in cybersecurity
- Kansas State University Center for Information and System Assurance conducts fundamental and applied research in information assurance and computer security

Wichita State University

ennovar

CSFRG
CYBER SECURITY & FORENSICS RESEARCH GROUP
AT WICHITA STATE UNIVERSITY

WSU Ennovar Technology Solutions

- Applied learning model
  - Cybersecurity
  - Development
  - Technical Support

Kansas Department of Commerce

Identified professional and technical services as a target sector for accelerated growth in Kansas

Provided Grant in 2020 to examine opportunities for economic growth from cybersecurity in Kansas

Cybersecurity Job Market

Total cybersecurity job openings: 2,535

Estimated employed cybersecurity workforce: 6,543

Workforce supply to demand ratio: 2.6

Average Salary $75,000

Developing the Bigger Picture

- High level overview from the state perspective
- Gap in visibility of cross industry collaboration
- Gap in visibility of cross government collaboration at varying levels
- Power of task force is to build that multi-level visibility by brining in other perspectives

Summary

A lot of cybersecurity efforts and progress in Kansas

Significant cybersecurity opportunity

Attack frequency and sophistication are increasing

Varying disruptions and impacts from cyber attacks

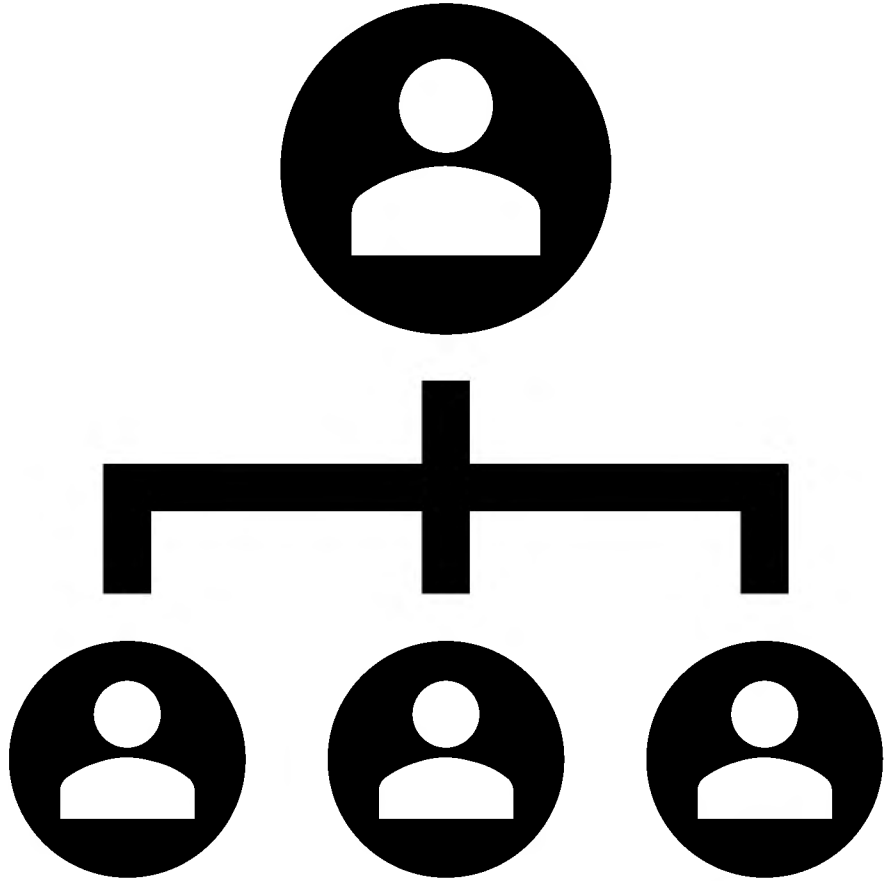
How do we bring together all of our efforts to ensure Kansas is secure and resilient?

Think Strategically

- Think "Whole-of-State"
- Recommendations should be actionable
- Propose resources needed to execute on recommendations

Format of Task Force

- Co Chairs
- Four subcommittees
- Chair for each subcommittee

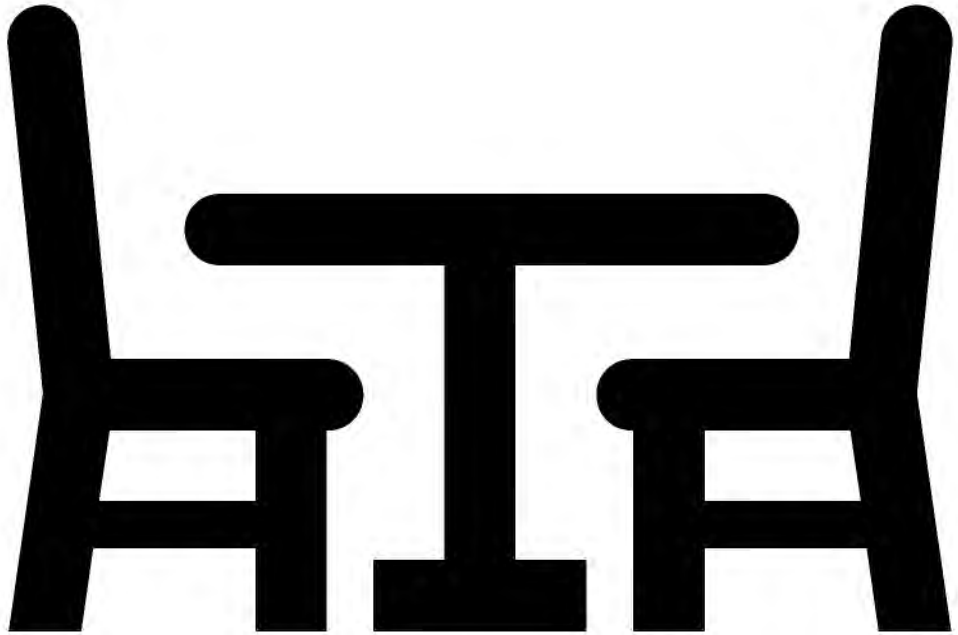


Subcommittee Responsibilities

- Establish regular working cadence
- First recommendations due to Task Force by Monday Sept 27th for compilation and drafting of report

Chairs

- Mike Mayta: CIO, City of Wichita
- Jeff Maxon: CISO, State of Kansas



Subcommittees

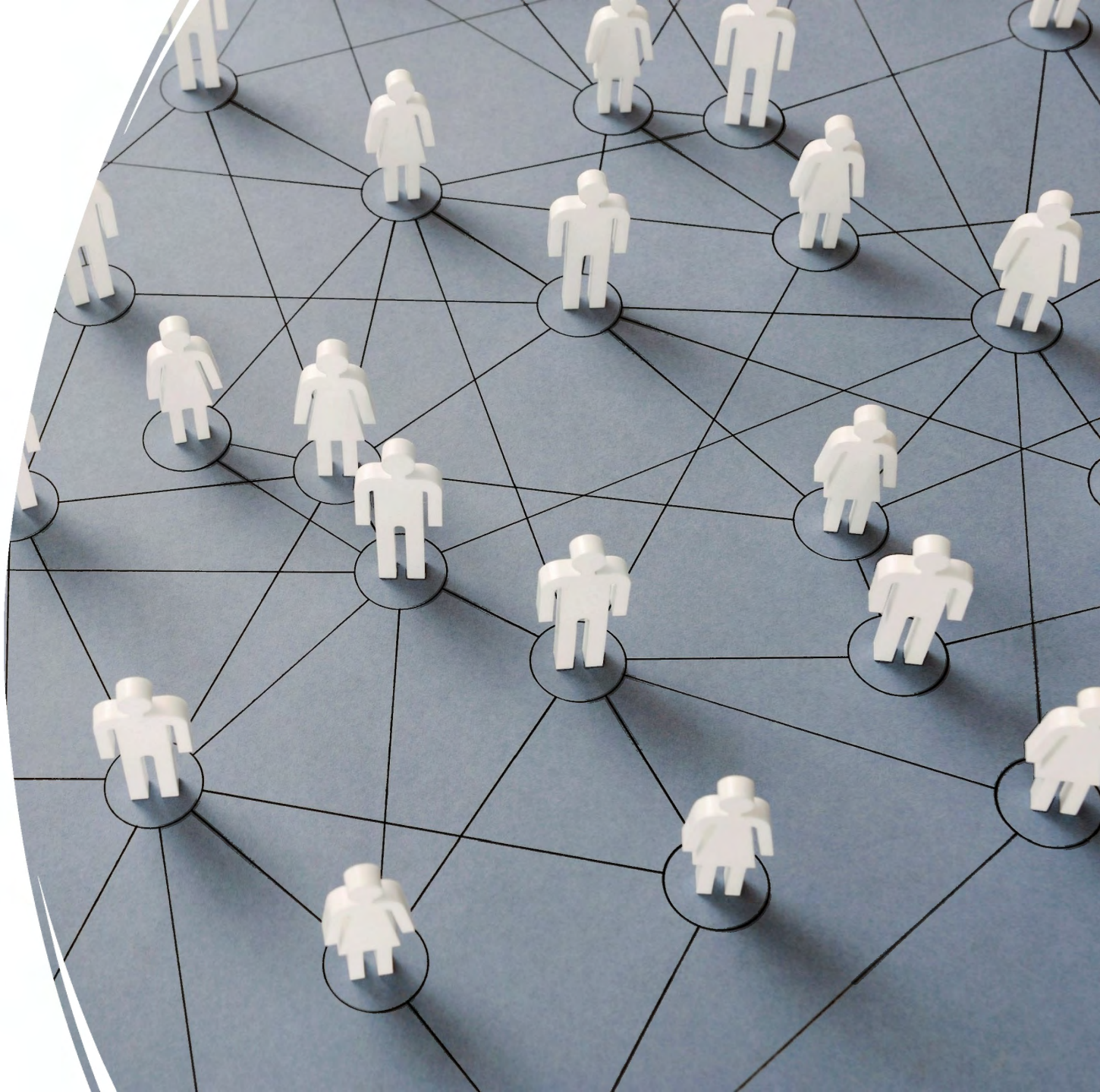
- Strategic Visioning and Planning
- Statewide Coordination and Collaboration
- Cyber Incident and Disruption Response
- Workforce Development and Education

Strategic Vision and Planning

- **Goal**: Identify key needs and develop components for a holistic statewide strategic plan for advancing cybersecurity in the State of Kansas

Statewide Coordination and Collaboration

- **Goal:** Identify, facilitate, and make recommendations to develop successful cross-government and cross-industry collaboration and coordination efforts to further cybersecurity within the State of Kansas



Cyber Incident and Disruption Response

- **Goal:** Identify key resources and components needed for a coordinated and collaborative cybersecurity response annex to the Kansas Response Plan

Workforce Development and Education

- **Goal:** Identify and make recommendations on ways to grow Kansas's cybersecurity workforce, educational and economic opportunities

Next Steps

- Subcommittee Assignments
- Selection of subcommittee chairs
- Scheduling of subcommittee meetings

Administrative Details

- KOMA and KORA
- SharePoint will serve as a repository for research and documents
- Points of Contact:
  - Allie Denning: allie.denning@ks.gov
  - Samir Arif: samir.arif@ks.gov

Closing Remarks