Kansas Cybersecurity Task Force
Welcome

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

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

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

Kansas

August 2021
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.
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
NGA Resource Center for State Cybersecurity

RESOURCES CENTER FOR STATE CYBERSECURITY

The significant and continued growth of cyber-attacks against the United States makes cybersecurity a critical issue for all governments. States and city governments must address the consequences of the rapidly evolving and expanding international threats now faced by law enforcement agencies, private financial and communications sectors and the general public. NGA is launching a Resource Center for State Cybersecurity to provide governments with resources, tools and recommendations to help craft and implement effective state policies and practices. To inform the work of the Resource Center, NGA is working with leading experts, practitioners, representatives of financial and political agencies and representatives from private industry to develop resources and tools and to provide strategies on state cybersecurity issues.

In January 2021, the NGA Center for Best Practices hosted the Fourth National Summit on State Cybersecurity, in conjunction with Arkansas Governor Asa Hutchinson. Videos from select sessions are available on the NGA’s YouTube channel.

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.
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

- Governance
- 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:

<table>
<thead>
<tr>
<th>What?</th>
<th>Who?</th>
<th>When?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation and Kickoff</td>
<td>Core Team &amp; Home Team</td>
<td>Yes</td>
</tr>
<tr>
<td>Research, Learning Calls, Technical Assistance</td>
<td>Core/Home Team Members as Relevant</td>
<td>Throughout Project Period – as needed basis</td>
</tr>
<tr>
<td>Virtual Check-Ins</td>
<td>Core Team</td>
<td>Throughout Project Period – biweekly basis</td>
</tr>
<tr>
<td>Cohort Convenings (Virtual)</td>
<td>Core Team</td>
<td>Throughout Project Period – monthly basis</td>
</tr>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt; In-State Strategic Planning Workshop (Virtual)</td>
<td>Core Team &amp; Home Team</td>
<td>April – July 2021</td>
</tr>
<tr>
<td>2&lt;sup&gt;nd&lt;/sup&gt; In-State Strategic Planning Workshop (In-Person)</td>
<td>Core Team &amp; Home Team</td>
<td>August – December 2021</td>
</tr>
<tr>
<td>Wrap Up</td>
<td>Core Team</td>
<td>December 2021 – January 2022</td>
</tr>
</tbody>
</table>
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

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

**Figure 1: Cyber Incident Severity Schema**

<table>
<thead>
<tr>
<th>Description</th>
<th>Disaster Level</th>
<th>Cyber Incident Severity</th>
<th>Description</th>
<th>Observed Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extensive amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.</td>
<td>Level 1</td>
<td>Level 5</td>
<td>Emergency</td>
<td>Effect</td>
</tr>
<tr>
<td>Requires escalated coordination among federal and state and local governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.</td>
<td>Level 2</td>
<td>Level 4</td>
<td>Severe</td>
<td>Presence</td>
</tr>
<tr>
<td>Requires coordination among federal and state and local governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.</td>
<td>Level 3</td>
<td>Level 3</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>No event or incident anticipated. This includes routine watch and warning activities.</td>
<td>Level 4</td>
<td>Level 0</td>
<td>Unsubstantiated or inconsequential event</td>
<td></td>
</tr>
</tbody>
</table>

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

---

How have states operationalized this?

**Ex: North Carolina**

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>COLOR</th>
<th>DESCRIPTION / IMPACT</th>
<th>BASELINE CYBER SUPPORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>Black</td>
<td>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.</td>
<td>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.</td>
</tr>
<tr>
<td>Severe</td>
<td>Red</td>
<td>Likely to result in a significant impact to public health or safety, economic security, foreign relations, or civil liberties.</td>
<td>State of Emergency is declared. Full Cyber package which may contain National Guard Defense Cyber Operations, Private Sector and State Cyber resources. Incident reporting by affected party is mandatory.</td>
</tr>
</tbody>
</table>

---

**CYBER DISRUPTION ESCALATION PROTOCOL**

Steady State

Protected by copyright.

© 2018 National Governors Association (NGA)
Responsibilities Associated w/ CDR

Table 1: NCIRP Lines of Effort

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

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
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
- **21-5839.** Unlawful acts concerning computers.

### 48: Militia, Defense and Public Safety
- **48-3701.** Kansas Intelligence Fusion Center Act. 48-3701 through 48-3710,

### 50: Unfair Trade and Consumer Protection
- **50-7a01.** Consumer information; security breach; definitions
- **50-7a02.** Security breach; requirements

### 75: State Departments; Public Officers and Employees
- **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
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

<table>
<thead>
<tr>
<th>School</th>
<th>Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Butler Community College</td>
<td>Cyber Defense Education</td>
</tr>
<tr>
<td>Johnson County Community College</td>
<td>Cyber Defense Education</td>
</tr>
<tr>
<td>Kansas State University</td>
<td>Research</td>
</tr>
<tr>
<td>University of Kansas</td>
<td>Cyber Defense Education, Research</td>
</tr>
<tr>
<td>Wichita State University</td>
<td>Cyber Defense Education</td>
</tr>
</tbody>
</table>
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.
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 bringing in other perspectives
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