DECEMBER 2021

Kansas Cybersecurity Task Force Final Report

Report to

Governor Laura Kelly

[THIS PAGE WAS INTENTIONALLY LEFT BLANK]

FROM THE CO-CHAIRS

FORWARD

This Cybersecurity Task Force report and its recommendations to advance a whole-of-state approach to cybersecurity are the culmination of hours of discussion between multiple cybersecurity stakeholders throughout Kansas. While we believe the Task Forces has developed some great recommendations, we recognize that these recommendations are just the beginning of a larger opportunity and continuing effort. We hope these recommendations are actionable and can serve as a valuable guide or starting point to facilitate future efforts to develop a whole-of-state approach to cybersecurity for Kansas.

Thanks to all the Task Force members for contributing their valuable time and expertise to this effort. We could not have accomplished what we did without your help and dedication. We also want to thank all individuals and organizations that presented and contributed to the Task Force. The input was incredibly valuable in steering and assisting the Task Force in developing recommendations that can benefit Kansas.

We also want to thank John Guerriero and Steven Fugelsang with the National Governors Association (NGA). Their assistance in providing us with a national context as well as introducing us to peers from around the country allowed start from a great foundation of best practices and lessons learned.

A special thank you goes to the individuals that assisted and supported the Task Force. Without their efforts, we would not have been successful in completing the Task Force Charges. Thank you to Allie Denning, Samir Arif, and Cheryl Cadue from the Department of Administration Public Affairs Office. In addition, we also want to thank Sara Kahn for assisting the Task Force. These individuals ensured that the Task Force was prepared for each meeting and coordinated with the guest speakers.

Lastly, we would like to thank Governor Laura Kelly for allowing us the opportunity to serve on this Task Force. We found it to be a rewarding experience and we believe the recommendations set up Kansas for success in the cybersecurity space.

Mike Mayta
Co-Chair

Jeff Maxon
Co-Chair

EXECUTIVE SUMMARY

As public and private organizations become more reliant on information technology and organizations become more interconnected, we also see a proliferation in cybersecurity attacks and their lasting impact. Cybersecurity attacks are often perceived to be the responsibility of information technology and cybersecurity experts and continuing to frame cybersecurity as 'their' responsibility only exacerbates the problem.

In 2019, Ponemon Institute conducted a survey, sponsored by Keeper Security, of approximately 2,000 small to medium-sized businesses, including public sector participants, from multiple countries and found that approximately 66% percent had suffered some form of a cyberattack within the past 12 months. In addition, 63% suffered a data breach. The report also indicated that the average cost of the compromise was $1.24 million while the overall average cost of business disruption was $1.9 million.[1] In addition, the Federal Bureau of Investigation (FBI) Internet Crimes Complaint Center (IC3) reports a significant rise of cybercrime-related complaints over the past five years as well as a consistent rise in total financial losses.[2]

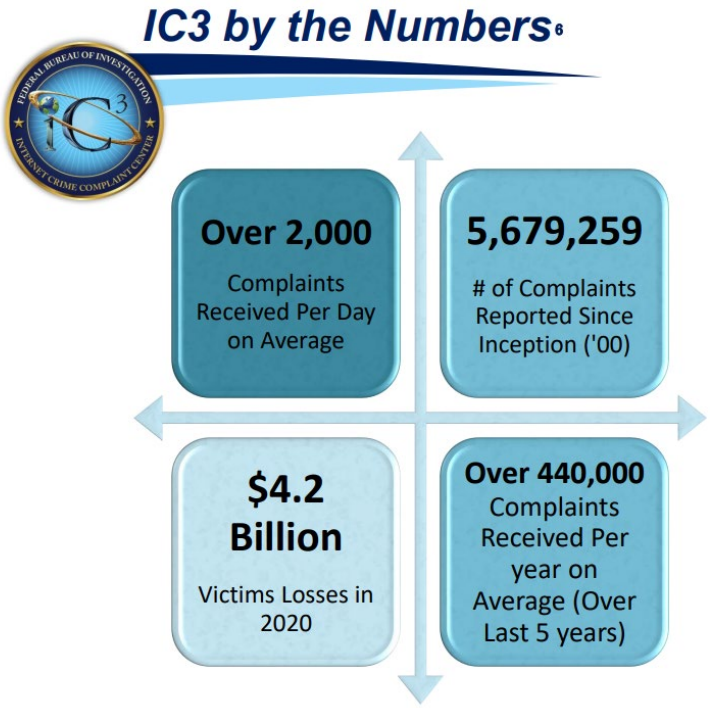

Figure 1: FBI IC3 Statistics from 2020 Internet Crime Report

While we grapple with the challenge of reframing the conversation around cybersecurity and how we all have a common responsibility in mitigating risk, we also face an ever-growing shortage of skilled cybersecurity professionals. Though the gap exists in both the public and private sectors, the public sector falls behind even more as it struggles to compete with the salaries of its private sector counterparts.

[1] https://www.cisco.com/c/dam/en/us/products/collateral/security/ponemon-report-smb.pdf
[2] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

With these challenges in mind, the Governor's Cybersecurity Task Force identified 41 recommendations to include in its final report with 17 of those recommendations being defined as critical priorities. Recommendations defined by the Task Force as critical are seen as critical to the implementation of other recommendations or, if there are limited resources, as musts to be implemented to have the greatest impact.

The 17 critical recommendations are:

1. Identify a short-term cybersecurity governance model to continue the work of this task force.
2. Identify a long-term sustainable cybersecurity governance model to support a whole-of-state approach.
3. A strategy must be developed to direct and guide efforts to build a whole-of-state approach to cybersecurity.
4. Conduct a state assessment or landscape analysis of the current cybersecurity capabilities and posture of Kansas.
5. Conduct a state assessment or landscape analysis of the current computer science and cybersecurity workforce development and education capabilities in and available to Kansas.
6. Begin building and establishing formal relationships and consistent, standard communication with local governments, K-12 education, higher education, critical infrastructure and other partners.
7. Create a cybersecurity position such as a Cyber Navigator or Cyber Liaison in state government to focus on communicating, coordinating, and collaborating with public and private cybersecurity partners.
8. Create and conduct an annual cybersecurity conference and other regularly scheduled events for public and private partners.
9. Identify the appropriate agencies and stakeholders who could form a cyber advisory body that would support and develop a cyber incident and disruption response plan and push the work to completion.
10. A cyber incident and disruption response plan should be created and maintained as part of an annex in the current State of Kansas Response Plan with the appropriate roles and associated responsibilities filled by stakeholders.
11. Ensure there are mechanisms for annual testing and exercising any cyber incident and disruption response plan with partners throughout the state.
12. Create language in statute to better allow public entities like the Division of Emergency Management, Adjutant General's Department, Kansas Information Security Office, and others such as municipalities, to provide mutual cybersecurity assistance to other public entities, critical infrastructure and education as needed.
13. Assess all existing state information technology and cybersecurity contracts and identify existing gaps in cybersecurity services and solutions. Develop a multi-vendor master cybersecurity contract that includes needed cybersecurity services and cybersecurity solutions and tools.
14. Ensure all State of Kansas cybersecurity contracts and other applicable technology contracts are open to political subdivisions.
15. Develop and deploy security awareness training resources and make them broadly available. Continue to encourage organizations to have information system users routinely complete cybersecurity awareness training if not already required.
16. Establish partnerships with higher education institutions to begin developing a talent pipeline through work-based learning opportunities.
17. Identify salary differences between public and private jobs and see if and where the public sector can raise wages to be more competitive.

ABOUT THE TASK FORCE

The following is a list of the Task Force members appointed by Governor Laura Kelly. Governor Kelly appointed 15 members to the Task Force from across Kansas representing a broad array of perspectives, backgrounds, and experiences.

CO-CHAIRS

Mike Mayta | Wichita | Chief Information Officer, City of Wichita

Jeff Maxon | Topeka | Chief Information Security Officer, State of Kansas

MEMBERS

Dr. DeAngela Burns-Wallace | Topeka **|** Chief Information Technology Officer, State of Kansas

Col. David Hewlett | Wichita **|** Designee of the Adjutant General of the Kansas National Guard

Jay Emler | Lindsborg **|** Designee of the Attorney General

Kevin Comstock | Topeka **|** Designee of the Secretary of State

Jonathan York | Topeka **|** Response and Recovery Branch Director, Kansas Division of Emergency Management

David Marshall | Topeka **|** Director, Kansas Criminal Justice Information Systems (KCJIS) Committee

John Godfrey | Shawnee **|** Chief Information Security Officer, University of Kansas Medical Center, Representative from Regents Institutions

Charles King | Overland Park | Senior Vice President and Chief Technology Officer, Evergy, Representative from Critical Infrastructure

John Berghuis | Salina **|** VP and Chief Information Officer, Salina Regional Health Center, Representative from Critical Infrastructure

Representative Kyle Hoffman | Coldwater **|** Representative from Joint Committee on Information Technology

Senator Jeff Pittman | Leavenworth **|** Representative from Joint Committee on Information Technology

William "Bill" Glynn | Topeka **|** Director, Kansas Intelligence Fusion Center

BACKGROUND

During the past several years, the United States has seen an increase in major cyberattacks that had significant impacts on organizations and everyday life. These cyberattacks are becoming increasingly more sophisticated and disruptive. Recognizing the impact of these cyberattacks, Governor Laura Kelly signed Executive Order No. 21-25 to establish the Governor's Cybersecurity Task Force ("the Task Force") on July 13, 2021.

The Task Force membership consisted of subject matter experts from various stakeholder organizations. Members represented multiple viewpoints consisting of state government, local government, academia, private sector, and critical infrastructure. The Task Force was charged with identifying and developing actionable recommendations to approach cybersecurity with a whole-of-state concept. This concept is viewed as an effective approach to reduce the overall cybersecurity risk to Kansas.

The Task Force's key charges were to facilitate cross-industry and cross-government collaboration, identify key cybersecurity partnerships, develop a framework for collaboration, and develop recommendations around a coordinated cyber response plan. The Task Force was broken into four subcommittees to address the varying charges. These four subcommittees are:

1. Strategic Vision and Planning
2. Statewide Coordination and Collaboration
3. Cyber Disruption and Incident Response
4. Workforce Development and Education

The Task Force and various subcommittees met on a biweekly basis since August of 2021. The Task Force produced an interim report that contained forty-five (45) recommendations and was delivered to the Governor on October 5, 2021. The Task Force produced a final report and delivered it to the Governor's Office on December 6, 2021.

Stakeholders and subject matter experts from Kansas and across the nation contributed valuable information to assist in making informed recommendations. These stakeholders presented background information on their cybersecurity efforts, their views on the current landscape, and ways they can contribute to advancing a whole-of-state approach. Additionally, many of the stakeholders provided suggestions they felt might be appropriate recommendations.

Our partnership with the National Governors Association (NGA) has been instrumental in the progress of this effort. By aligning this effort with the selection of Kansas to participate in the annual Policy Academy to Advance the Whole-of-State Cybersecurity, we were able to identify a significant number of recommendations by leveraging the work NGA has already completed in other states. NGA was able to provide an objective view of other efforts states have undertaken to help tackle the same problem and challenges Kansas is faced with.

THE TASK FORCE'S WORK

The Task Force was charged to identify actionable recommendations to approach the complex cybersecurity challenges and problems that the State faces. Based on the charges of the Task Force outlined in Executive Order 21-25 the Task Force formed four subcommittees to address the various charges. Each subcommittee had an established goal that their recommendations are striving to achieve. The Task Force and subcommittees met on alternating weeks starting in August and ending on December 1, 2021.

Subcommittees

Strategic Vision and Planning (SVP)

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

Cyber Incident and Disruption Response (CIDR)

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

Statewide Coordination and Collaboration (SCC)

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

Workforce Development and Education (WDE)

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

UNDERSTANDING THE PROBLEM

Organizations, both public and private, are almost wholly dependent on information technology and data. Information technology is critical for organizations to conduct their business operations. Business operations can range from providing electricity, checking out food at the grocery store, providing healthcare, providing citizen services, and everything in-between. The Covid-19 pandemic has further driven society to become more digitally connected. Organizations had to enable remote work capabilities and provide more digital services. In order to operate, organizations must ensure their data maintains confidentiality, maintains integrity, and is readily available. Malicious actors are aggressively exploiting our reliance on technology with very real and very damaging consequences. Organizations face a constant threat from these malicious cyber actors to include cybercriminals and nation-states. Cybersecurity has become a major business risk to organizations and Kansas citizens.

In recent years, cyberattacks have devastated organizations worldwide. In 2017, we saw the destructive NotPetya cyberattack cause an estimated $10 Billion in damages[3]. There have been several cyberattacks that have disrupted both local and state government operations for the better part of a month. School districts and hospitals have been the target of cyberattacks causing disruptions in education and healthcare services. Additionally, there have been numerous data breaches that have led to the theft of hundreds of millions of records of personally identifiable information. There have also been numerous ransomware attacks that have held organizations hostage. Finally, we have seen sophisticated cyber-espionage campaigns that have taken the better part of a year to orchestrate and execute.

Compounding the risks posed by the various cyber threats, there is a significant shortage of qualified cybersecurity professionals globally and in the United States. According to the International Information System Security Certification Consortium (ISC)[2], which is a non-profit cybersecurity certification and training organization, in 2019 they estimated that the cybersecurity workforce gap was approximately half a million skilled professionals in the United States. The cybersecurity workforce gap is defined as the estimated existing cybersecurity job demand and the assessed capacity to fill that demand. In 2020, there was a decrease in the cybersecurity workforce gap. The current cybersecurity workforce gap in the United States is still approximately 350,000[4]. While this represents significant positive progress to close the gap, a major gap remains. Public sector organizations have trouble competing with the private sector for these valuable and scarce resources.

Organizations are becoming increasingly more connected and digitally dependent on one another. An example of this can be seen in the interconnected nature of the energy grid where outages in one provider's space can cause a ripple effect across the system. When a cyberattack affects one entity it will likely have effects on others. Identity theft from one system could lead to fraudulent activity in another. In larger forms, a major network compromise or cyberattack in one organization's environment could lead to a major compromise in another. The major underlying challenges include inconsistent approaches and prioritization of cybersecurity across Kansas and even the country. In addition, the lack of cross organization and cross government coordination and

[3] https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/
[4] https://www.isc2.org/Research/Workforce-Study

cooperation leads to a “fend for ourselves” mentality. When tackling the common cybersecurity challenges, we have a collective interest to work together.

Cybersecurity is becoming a greater priority for organizations. As organizations continue to struggle to detect, respond to, and recover from cybersecurity attacks, efforts must be made to address these challenges in concerted or whole-of-state ways. Working across organizational boundaries is critical for success and protecting Kansas citizens.

CYBERSECURITY EFFORTS IN KANSAS

While the cybersecurity challenges that organizations face continue to increase, there is some good news in Kansas. Over the past several years there have been multiple cybersecurity efforts taking place throughout Kansas that are having a positive impact. The Task Force heard from many of these stakeholders and learned about their efforts during Task Force and subcommittee meetings. These efforts range from non-profit organizations providing scholarship opportunities all the way to State Government efforts.

Higher education in Kansas is making significant strides in cybersecurity and computer science education. Most of the four-year institutions in Kansas offer some form of cybersecurity courses. Six institutions offer cybersecurity degrees. In addition, four four-year institutions have received Department of Homeland Security (DHS) and National Security Agency (NSA) designation as centers of academic excellence for cybersecurity education or cybersecurity research. Many of the two-year institutions are now offering courses in cybersecurity and computer science. Three of the two-year institutions are offering associates in degrees in cybersecurity. Two of the two-year schools have also received the DHS/NSA designation of a center of academic excellence. Finally, several State of Kansas scholarship programs exists, like the Kansas Promise Act Scholarship, which focuses on providing financial assistance to individuals pursuing certain degrees.

Within the State of Kansas government, there have been several efforts focused on cybersecurity over the past couple of years. Efforts include the passage of the Kansas Intelligence Fusion Center Act in 2017 which formally established the Kansas Intelligence Fusion Center (KIFC). The KIFC has demonstrated a successful partnership and joint effort between the executive branch and elected office that includes a cybersecurity focus. KIFC operations also include assisting critical infrastructure with an expanded understanding of threats to their networks. The Kansas Cybersecurity Act in 2018, established the Kansas Information Security Office (KISO) and the position of the State Chief Information Security Officer (CISO). In 2019 the State updated the state cybersecurity standards. Also, in 2019, the Kansas Bureau of Investigation (KBI) created a cybercrime division. The Kansas National Guard over the past several years has continually grown its cybersecurity focused skill sets. The establishment of the 184th Cyberspace Operations Group within the Kansas Air National Guard has created a significant concentration of cybersecurity professionals within Kansas.

Non-profit organizations are contributing greatly to developing the next generation of cybersecurity professionals. Several non-profit efforts include providing scholarships to students looking to pursue cybersecurity or other technical degrees. Other non-profit clubs exist that support and encourage science, technology, engineering, and mathematics (STEM) activities.

Lastly, the Federal Government is spending significant resources through the DHS Critical Infrastructure Security Agency (CISA) into state, local, and critical infrastructure. CISA brings several cybersecurity services to organizations at no cost. Also, they are developing their outreach capabilities by looking to assign a dedicated cybersecurity liaison for Kansas.

The major challenge has been coordinating and aligning these efforts in a unified approach that provides the greatest value. This is where a whole-of-state approach to cybersecurity is critical for Kansas.

WHOLE-OF-STATE CYBERSECURITY

Organizations within Kansas and even nationally have similar objectives in protecting their data and delivering services. Cyber threats are not bound to an organization and geopolitical boundaries. Cyber threats are increasing in sophistication. Adding to the cyber threats is the cybersecurity workforce shortage. Recognizing that the threats and challenges impact all levels of government, education, critical infrastructure, and the private sector, many states are beginning to approach cybersecurity with a new approach. The intrinsic ties that the organizations, particularly in the government space, have with one another and a common or collective responsibility to provide citizen services is leading states to a whole-of-state approach to cybersecurity. The enormity and the complexity of the cybersecurity landscape can only be tackled when working together to achieve a common objective.

Whole-of-state cybersecurity leverages the combining of resources and expertise across the state to maximize capabilities to overcome the threats and challenges affecting organizations within the state. In addition, leveraging the national level resources, such as those offered by DHS available to the State, Local, Tribal, and Territorial (SLTT) entities. The National Association of State Chief Information Officers (NASCIO) and the NGA developed a publication "Stronger Together: State and Local Cybersecurity Collaboration"[5] that advocates for states to approach cybersecurity with a whole-of-state approach.

One of the key tenants of whole-of-state cybersecurity is collaboration, relationship building, and partnership building. This was a recurring theme from almost all the presenters and experts that spoke to the Task Force and subcommittees.

INTERIM REPORT

The Task Force delivered the Interim Report[6] to the Governor on October 5, 2021. The first report contained forty-five (45) initial recommendations to advance whole-of-state cybersecurity in Kansas. Recommendations were initially broken down into near-term and long-term recommendations and organized by the subcommittee that presented the recommendation. These recommendations represent the Task Force's initial effort to produce recommendations. After the delivery of the interim report, the Task Force continued to develop new recommendations and further refine the existing recommendations.

[5] https://www.nga.org/wp-content/uploads/2020/01/NASCIO_NGAStatesLocalCollaboration.pdf
[6] https://governor.kansas.gov/wp-content/uploads/2021/10/10_28_21_Cybersecurity-Task-Force-Interim-Report.pdf

FINAL RECOMMENDATIONS

As the Task Force continued to meet, certain themes around the recommendations began to become apparent. The recommendations in this final report are organized by those themes.

During the last few subcommittee meetings, Task Force members identified several priority recommendations. Priority recommendations were either assigned a critical or a high priority designation. Critical recommendations are critical to the implementation of other recommendations or if there are limited resources, these would be the absolute musts to be implemented to have the greatest impact. High-priority recommendations will have significant impacts on efforts to advance whole-of-state cybersecurity in Kansas.

While the Task Force developed multiple recommendations to advance a whole-of-state approach to cybersecurity, it is only the beginning. Work must be done to develop an approach and establish a way to execute and implement the recommendations.

Recommendations follow the format below:

Recommendation
CATEGORY.NUMBER TIME TO IMPLEMENT GOAL (NEAR/LONG) | PRIORITY (CRITICAL/HIGH)
PRIMARY STAKEHOLDERS INVOLVED IN IMPLEMENTION OF RECOMMENDATION
Description and context of the recommendation.

Definition of Terms:

Time to implement goal:

NEAR:	Recommendation could likely be implemented within six (6) months of initiation
LONG:	Recommendation may take longer than six (6) months to implement

Priority:

CRITICAL:	Recommendations that are critical to the implementation of other recommendations or if there are limited resources, these would be the absolute musts to be implemented to have the greatest impact
HIGH:	Recommendations that will have significant impacts to efforts to advance whole-of-state cybersecurity in Kanas.

Primary Stakeholders Involved in Implementation of Recommendation:

STATE/AGENCY: State of Kansas Departments, Agencies, Boards, Offices, or Commissions
LOCAL: Counties and Cities
LEGISLATIVE: Legislature
CRITICAL INFRASTRUCTURE: Organizations in the 16 sectors defined by PPD-21
HIGHER EDUCATION: Higher education institutions
K-12: K-12 School Districts and Schools
PRIVATE SECTOR: Commercial entities or not for profit organizations that support cybersecurity efforts

Cybersecurity Governance and Strategy (CGS)

Identify a short-term cybersecurity governance model to continue the work of this task force.

CGS.1 NEAR | CRITICAL

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, PRIVATE INDUSTRY

Continue the Task Force for one year, giving time for the whole-of-state formal cybersecurity governance to be developed for Kansas and ratified by the Legislature in statute. This Task Force is critical to continue driving, coordinating, and organizing a whole-of-state approach. (Appendix A)

Identify a long-term sustainable cybersecurity governance model to support a whole-of-state approach.

CGS.2 LONG | CRITICAL

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE INDUSTRY

A long-term governance structured approach should include a legislatively established working group under the auspices of the Adjutant General and the Kansas Homeland Security Office or developing a joint group co-governed by the Adjutant General and the Chief Information Technology Officer (CITO) and KISO or Department of Administration. This body should have the authority to develop an umbrella function guiding a whole-of-state approach to sharing of information, collaboration, memorandums of understanding, and incident coordination across the state of Kansas with governments, critical infrastructure, businesses, and citizens. For a whole-of-state cybersecurity effort to be effective, ownership and accountability must be formally established. In some cases, funding must also be established for the various efforts. By establishing ownership and accountability, efforts are more likely to be successfully completed. (Appendix A)

A strategy must be developed to direct and guide efforts to build a whole-of-state approach to cybersecurity.

CGS.3 NEAR | CRITICAL

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE INDUSTRY

Strategies are imperative to guide and direct organizations to meet their goals and objectives. These strategies will help and guide the individuals, groups, and organizations that come together to develop a whole-of-state approach to cybersecurity. The Strategic Vision and Planning subcommittee outlined proposed goals and strategies based on observations of the other subcommittees. (Appendix A)

Resource Analysis (RA)

Conduct a state assessment or landscape analysis of the current cybersecurity capabilities and posture of Kansas.

RA.1 NEAR | HIGH/CRITICAL

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE SECTOR

An inventory or assessment of cybersecurity capabilities and posture within Kansas and across stakeholders should help identify current capabilities, resources, partnerships, and needs. This will help with identification of roles, responsibilities, and capabilities that exist within the state. Communicating the inventory ensures stakeholders know what resources may be available to them to improve their cybersecurity posture and respond to cybersecurity incidents.

Conduct a state assessment or landscape analysis of the current computer science and cybersecurity workforce development and education capabilities in and available to Kansas.

RA.2 NEAR | HIGH/CRITICAL

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE SECTOR

An inventory of workforce development partners, current programs, and mapped industries and jobs available will provide Kansas with a bigger picture of what is happening, what can be scaled, and where gaps exist. Similarly, an inventory of what's happening in both higher education and K-12 education, educational resources available, programs offered, and a mapping of the types of degrees being produced from higher education to meet workforce demand will prepare Kansas to build upon existing efforts that work well and filling any gaps. We must identify how to pull these entities together, share the resources, leverage the information, tell the story, and assess for next steps of action. These tools and resources can come from entities external to Kansas, but that are being used in the Kansas landscape.

Outreach and Coordination (OC)

Begin building and establishing formal relationships and consistent, standard communication with local governments, K-12 education, higher education, critical infrastructure, and other partners.

OC.1 NEAR | CRITICAL

STATE/AGENCY, LOCAL, HIGHER EDUCATION, K-12 EDUCATION, CRITICAL INFRASTRUCTURE

Building and establishing formal relationships and networking avenues with various stakeholders are imperative for the success of a whole-of-state approach. Proactively engaging with stakeholders early and often is essential to sharing cybersecurity education and information.

Create a cybersecurity position such as a Cyber Navigator or Cyber Liaison in state government to focus on communicating, coordinating, and collaborating with public and private cybersecurity partners.

OC.2 NEAR | CRITICAL

STATE/AGENCY

Coordination and collaboration are key to approaching cybersecurity in a whole-of-state approach. By having a dedicated individual or several individuals to perform outreach and collaborate with various stakeholders, we can build and maintain relationships that continuously advance cybersecurity and raise awareness. These collaborations also open the door to more grant opportunities in the long-term, including potential grant opportunities. The success of this position and its related activity will depend upon the influence, autonomy, and authority that this role has for executing a whole-of-state approach. Other states are effectively leveraging similar positions.

Create and conduct an annual cybersecurity conference and other regularly scheduled events for public and private partners.

OC.3 NEAR | CRITICAL

STATE/AGENCY

The annual cybersecurity conference is a critical platform for developing communities of practice, sharing of best practices and approaches, deepening the conversations around cybersecurity throughout the State, and providing direct or hands-on actions and artifacts that can be taken and deployed immediately. Shareholders will further network, learn about other capabilities and resources throughout the State, and identify gaps that can be addressed through other State cyber processes. This event should be hybrid to ensure accessibility, access, and participation.

Partner with organizations including, but not limited to, the League of Kansas Municipalities (LKM), the Kansas Association of Counties (KAC), Kansas Research and Education Network (KanREN), and Kansas Corporation Commission (KCC) to reach broader audiences to raise cybersecurity awareness, share available resources, and to strengthen trust with stakeholders.

OC.4 LONG | HIGH

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE INDUSTRY

Engaging and working with groups and associations that support or advocate for various sectors can allow for a conduit or distribution program for cybersecurity messaging and alerts, allowing for a broader

reach to stakeholders. In addition, their aggregate awareness of issues across their organizations can provide valuable insight into cybersecurity challenges. There is not a one-size approach to this distribution program. The structure and framework of communication must be defined to match information with the capabilities and interests of the different entities. Direct communication would still be handled by the partner organizations.

Develop and deploy a continuous education campaign to share and promote best practices and raise awareness that cybersecurity is a business risk to the continuity of government and related critical infrastructure.

OC.5 LONG | HIGH

STATE/AGENCY, LEGISLATIVE, LOCAL, HIGHER EDUCATION, K-12 EDUCATION, CRITICAL INFRASTRUCTURE, PRIVATE INDUSTRY

Cybersecurity issues affect more than just information technology. Attacks and disruptions can delay or halt business operations. Awareness of cybersecurity as a business risk and that everyone has a role to play in ensuring continuity of business is critical. Consideration of special programming during October, due to cybersecurity awareness month, should be considered. Lean on using best practices published by the federal government and disseminate them to stakeholders throughout Kansas.

Identify an individual or group to specifically manage cybersecurity grants.

OC.6 NEAR

STATE/AGENCY

An individual or group needs to be appointed or hired to specifically manage cybersecurity grants. This individual or group will focus on helping organizations identify and apply for cybersecurity grant opportunities such as the Homeland Security Grant Program and other emerging grant programs. This individual or group can properly vet applications to ensure they meet the cybersecurity requirements of various grants, and they would also be responsible for communicating out the cybersecurity grant opportunities to various stakeholders. Exploring and leveraging grants is a critical strategic component of funding a whole-of-state approach to cybersecurity.

Identify state and regional opportunities where the whole-of-state approach can create engagements and find alignment around cybersecurity.

OC.7 LONG

STATE/AGENCY, LOCAL, HIGHER EDUCATION, CRITICAL INFRASTRUCTURE

Utilize existing efforts like the National Crossroads Initiative for National Security to align with and bolster cybersecurity efforts. Aligning with them on work, messaging, and techniques improves both the State and regional cybersecurity posture and encourages economic development. Creating engagements and alignment also creates opportunities to be more competitive in applying for grants and other funding opportunities.

Cyber Incident and Disruption Response Plan Development and Maintenance (CIDR)

Identify the appropriate agencies and stakeholders who could form a cyber advisory body that would support and develop a cyber incident and disruption response plan and push the work to completion.

CIDR.1 NEAR | CRITICAL

STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE

Cyber incidents require specialized skillsets for effective response. Additional cross-functional stakeholders that have not traditionally been involved in emergency management and response will need to be identified and brought together to begin to collaborate and develop an incident response plan. In gathering information and lessons learned from other states who have developed incident and disruption response plans, they indicated bringing together similar advisory structures was instrumental to enable development of their plans. Their input has consistently indicated that their initial plans represented a starting point which then continued to evolve and mature.

A cyber incident and disruption response plan should be created and maintained as part of an annex in the current State of Kansas Response Plan with the appropriate roles and associated responsibilities filled by stakeholders.

CIDR.2 NEAR | CRITICAL

STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE

The Kansas emergency management and response framework enables multiple options for incorporating a statewide cyber incident and disruption response plan, with the recommendation being that it be developed as an incident-specific annex in the Kansas Response Plan. Incorporating the incident-specific annex into the Kansas Response Plan with clearly identified and assigned roles will ensure that it is properly maintained, exercised, and communicated. Clearly identified roles and responsibilities of stakeholders also ensures a strategic communication and chain-of-command response is followed, minimizing confusion and overlap of efforts. This would be a cybersecurity incident annex in the Kansas Response Plan and later incorporated into the Kansas Planning Standards for inclusion in local emergency operations plans, which are created at the county level of government across the state. Defining local level roles when developing the standards will be done through the planning standards. The Kansas Response Plan takes effect when an incident reaches the level that requires a state of disaster emergency by the Governor. Initially, this plan would be managed in a centralized fashion by the Kansas Division of Emergency Management (KDEM), with a long-term goal of counties across the state to each independently follow and develop an incident-specific annex for cybersecurity in their local emergency operations plans. Maintenance of the plan will be modeled on KDEM's response plan maintenance.

Encourage all public entities to subscribe to the Multi-state Information Sharing and Analysis Center (MS-ISAC) to have access to the numerous services they provide at no cost.

CIDR.3 NEAR | HIGH

STATE/AGENCY, LOCAL, K-12

MS-ISAC offers a significant number of services at no cost to public sector entities. Services from MS-ISAC include cyber threat intelligence, cyber alerts, access to the Center for Internet Security resources, incident response services, and numerous others. By encouraging public sector entities to subscribe to the MS-ISAC, organizations have additional tools to increase their cybersecurity posture with little investment.

Incident Response Exercises and Training (IRET)

Ensure there are mechanisms for annual testing and exercising any cyber incident and disruption response plan with partners throughout the state.

IRET.1 LONG | CRITICAL

STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE

Testing and exercising the incident and disruption response plan on an annual basis is critical. Much like testing organization Continuity of Operations Plans (COOP), testing the incident and disruption response plan allows organizations to practice and improve their plans. CISA has training exercises available for utilization. Some training is general while other training is much more focused. CISA can facilitate and provide after action-reports at no cost.

Ensure that any cyber incident and disruption response plan has a formal process for recurring reviews, updates, and exercises.

IRET.2 LONG | HIGH

STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE

Evaluating and modifying a cyber incident and disruption response plan is critical. Incorporating lessons learned from exercises and real-world events continually improves the plan to become more efficient and effective.

Ensure there is a continuous training and awareness component around the cyber incident and disruption response plan.

IRET.3 LONG | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION, CRITICAL INFRASTRUCTURE

In a similar effort to Continuity of Operations Plans training and other emergency management training, steps should be taken to train and educate stakeholders on the cyber incident and disruption response plan. Additional training and awareness should focus on available resources and various roles and responsibilities of stakeholders and assisting organizations. Training organizations on the incident and disruption response plan allows them to better incorporate the plans into their organization, know about available resources and raise awareness of the importance of the plan.

Incident Notification and Response (INR)

Create language in statute to better allow public entities like the Division of Emergency Management, Adjutant General's Department, Kansas Information Security Office, and others such as municipalities, to provide mutual cybersecurity assistance to other public entities, critical infrastructure, and education as needed.

INR.1 LONG | CRITICAL

LEGISLATIVE

One of the major hesitancies for state agencies and other political subdivisions to provide cybersecurity assistance to other government entities or critical infrastructure is the liability for potential damages. Cybersecurity activities, whether assessments or incident response, have the potential to create negative impacts on an organization's physical network. By creating language to protect them from liability, organizations will be able to provide additional support more openly to other entities.

Ensure that all cyber incident reporting or requests for help to the State have protection mechanisms to maintain confidentiality and not hinder the response.

INR.2 LONG | HIGH

STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE, LEGISLATIVE

To encourage reporting or requests for help and not hamper response, protection mechanisms should be in place to protect the confidentiality of organizations if they reach out for assistance. In many instances, some organizations may not want to report incidents or make requests for help if they feel they may be made public. This may require a review of current policies around information sharing.

Within the proposed role-based incident response plan, include a cyber triage intake process or a central notification system for communication of cyber incidents.

INR.3 LONG | HIGH

STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE

In the event of an incident, city, county, State government, and other entities have a central point of contact to report incidents. When stakeholders in an incident are identified, a process can be leveraged to send a text or email blast of information for triage and impact analysis. A triage call sheet can help the initial point of contact collect the pertinent information and then decide who is most appropriate to receive it for follow-up or additional information. Initially, the cyber disruption and incident response process and associated triage would be centrally managed by KDEM, and then coordinated with state agency stakeholders based on knowledge and experience.

Establish a framework of substantive agreements including, but not limited to, memorandums of understanding (MOUs) and statements of work (SOWs) templates, and relationships with entities in advance of an event to remove risk to those entities.

INR.4 LONG | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION, CRITICAL INFRASTRUCTURE

By establishing agreements or having templates available like MOUs and SOWs between organizations ahead of time, allows organizations to respond quicker to cybersecurity incidents and not have to wait for agreements to be drafted from scratch. It also provides education, awareness, and understanding to the participating organizations of the roles and responsibilities of organizations in supporting those incidents.

Explore opportunities to deploy MS-ISAC Albert Intrusion Detection System Sensors to the counties.

INR.5 LONG | HIGH

STATE/AGENCY, LOCAL

MS-ISAC Albert Sensors are Intrusion Detection Systems (IDS) managed, maintained, and monitored by MS-ISAC's 24X7 security operations center. Albert Sensors can operate in a non-intrusive manner and much of the setup is handled by MS-ISAC. By deploying sensors to all counties, we can ensure that there is some level of monitoring of county networks for malicious activity. MS-ISAC notifies the appropriate parties when they identify malicious traffic. In addition, this activity can be aggregated to provide better situational awareness within the state. Albert Sensors are only available to public entities. There are initiation fees and cost associated with Albert Sensors. Many states have taken a variety of approaches through grants and other funds to widely deploy Albert Sensors.

Cybersecurity Supply Chain and Procurement (CSCP)

Assess all existing state information technology and cybersecurity contracts and identify existing gaps in cybersecurity services and solutions. Develop a multi-vendor master cybersecurity contract that includes needed cybersecurity services and cybersecurity solutions and tools.

CSCP.1 NEAR | CRITICAL

STATE/AGENCY

Having a multi-vendor master cybersecurity contract that covers cybersecurity services and cybersecurity solutions and tools have multiple benefits. By consolidating these into a master contract, it allows organizations to easily locate needed cybersecurity services and solutions, reduces the RFP effort by only needing to release one RFP, and allows for a resource that can be readily compiled and shared with organizations. In addition, the State of Kansas can perform the initial vetting of vendors. By having multiple vendors on contract for a variety of services, it ensures that organizations can rapidly locate a vendor if needed in a timely manner without having to submit a specific RFP. This provides a much larger scale which in turn provides a quicker response. A master contract may also serve as a reference point for smaller private industry organizations.

Ensure all State of Kansas cybersecurity contracts and other applicable technology contracts are open to political subdivisions.

CSCP.2 NEAR | CRITICAL

STATE/AGENCY

By opening all state cybersecurity contracts, where possible, to political subdivisions has multiple benefits. First, it will allow the state to negotiate lower rates. Secondly, it allows political subdivisions to leverage those lower rates based on the economies of scale and allows them to maximize their cybersecurity dollars. In addition, by opening all cybersecurity contracts to political subdivisions, the State can free up the scarce resources at a local level that would have been spent by local entities to develop their own requests for proposals to identify similar services. It also provides downstream benefits such as common training and support. In addition, a catalog of these contracts should be created, made available, and communicated.

Develop and deploy model cybersecurity contract language that can serve as a guide and be modified as needed for incorporation into all information technology contracts that involve organizational data.

CSCP.3 NEAR | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION, CRITICAL INFRASTRUCTURE

Organizations are heavily reliant upon vendors and contractors to help manage and deliver IT goods, services, and solutions. All organizations benefit from having customer-centric cybersecurity contract language and guidance. This ensures that data and IT services meet certain cybersecurity requirements while assuring due diligence and due care from the providers.

Develop and deploy guidance around cybersecurity Supply Chain Risk Management Best Practices.

CSCP.4 LONG

STATE/AGENCY, LOCAL, HIGHER EDUCATION, CRITICAL INFRASTRUCTURE

Organizations are heavily reliant upon vendors and contractors to help manage and deliver IT goods, services, and solutions. Organizations should be made aware of the risks that the supply chain presents to organizations. By developing material that can be widely shared and easily consumed would help many organizations.

Identify ways to pool cybersecurity funding to build on economies of scale and reduce duplicate efforts.

CSCP.5 NEAR

STATE/AGENCY, LOCAL, HIGHER EDUCATION, CRITICAL INFRASTRUCTURE

The pooling of resources, funding, in particular, can be mutually beneficial to organizations as they access services and tools to enhance their cybersecurity posture. Organizations could procure services, such as security and vulnerability assessments, individually at a higher rate or pool their funding and procure multiple services or tools at a reduced rate. By coordinating cybersecurity spending and leveraging economies of scale, organizations may be able to procure more services than if they procure them individually.

Cybersecurity Awareness Training (CAT)

Develop and deploy security awareness training resources and make them broadly available. Continue to encourage organizations to have information system users routinely complete cybersecurity awareness training if not already required.

CAT.1 LONG | CRITICAL

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE INDUSTRY

Disruptive cyberattacks have impacted all types of organizations. Basic activities such as checking email and browsing the internet can create risk for government organizations at all levels. In addition, there are multiple points of interaction between various government entities where one impacted organization can affect others. Cybersecurity awareness training to build cybersecurity-aware employees is one of the most important lines of defense against cyberattacks. Providing education to the public and private sector on available resources to assist with training their employees and special programming in October for Cybersecurity Awareness Month should be considered.

Explore if critical infrastructure roles that require a license or certification from the State could include cyber training as part of their licensing or certification or continuing education process.

CAT.2 LONG | HIGH

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE

To help individuals more fully understand cybersecurity concerns when connected to other parties, could the State of Kansas include cybersecurity training as part of any licensing or certification an employee is required to get from the State for a role, e.g. water quality engineers, nurses, architects, etc. This could also include cybersecurity awareness training being recognized as a continuing education credit.

Staff Development Training (SDT)

Develop a training program with partners, such as Universities, for existing public sector employees to address cybersecurity and information technology training.

SDT.1 LONG | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION

Information technology and cybersecurity professionals require constant training to further their skills and introduce them to new technologies. Training is invaluable to developing proficient cybersecurity professionals. Models such as the partnership with KU for the Public Management Program, Law Enforcement Training Center, or the KDEM emergency management training program can serve as model programs for training public sector IT and cybersecurity professionals. These programs can be used to upskill employees by teaching them additional skills. To bridge the workforce gap, training programs can also reskill employees to transition them into IT and cybersecurity roles.

Explore the development of a public/private cyber range that includes partnerships with our higher education institutions to provide staff and students training and development opportunities.

SDT.2 NEAR

STATE/AGENCY, LOCAL, HIGHER EDUCATION

The development of a cyber range that benefits both public and private sector entities and higher education institutions can provide a unique training environment for organizations to develop their cyber defense skills. There are multiple avenues to explore. In addition, there may be partnerships opportunities already developed by the Kansas Department of Commerce.

Talent Pipeline Development (TPD)

Establish partnerships with higher education institutions to begin developing a talent pipeline through work-based learning opportunities.

TPD.1 NEAR | CRITICAL

STATE/AGENCY, LOCAL, HIGHER EDUCATION

Many of the higher education institutions in Kansas have both computer science programs and cybersecurity programs. Building partnerships between organizations and educational institutions can benefit both the schools and organizations trying to build talent pipelines to fill critical positions with qualified staff. This relationship would be mutually beneficial as recruiting opportunities for educational institutions and employers. Apprenticeships, partnerships, and internships may serve to overcome some of the challenges in exposing college students to enterprise environments before entering the workforce. Looking at the long-term objectives of this recommendation, building these partnerships will help build the talent pipeline and impact the retention issues facing all sectors public and private.

Create a registry or industry matching service to connect potential interns and job seekers with organizations offering work-based learning opportunities.

TPD.2 LONG

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE INDUSTRY

A registry or industry matching service where public and private organizations can list internships and job opportunities will benefit the State, especially smaller, local governments and regions. For areas that lack the capacity or expertise to support interns, a registry can provide resources of coordination, connection, and support. A registry of this type should live within the Kansas workforce development system.

Develop work-based learning opportunities through public and private partners to provide hands-on learning for students and continued learning and training for existing staff.

TPD.3 LONG

STATE/AGENCY, LEGISLATIVE, LOCAL, CRITICAL INFRASTRUCTURE, HIGHER EDUCATION, K-12 EDUCATION, PRIVATE SECTOR

Developing work-based learning opportunities provides students, both in high school and college, an opportunity for real-world training and experience they can leverage upon graduation. Work-based learning opportunities also provide additional training opportunities for employees to continue their learning and development.

Partner with commercial and non-profit training programs to build the talent pipeline by tapping into the adult workforce, including transitioning soldiers, to reskill, retrain, and retool them to step into cybersecurity roles.

TPD.4 LONG

STATE/AGENCY, LOCAL, HIGHER EDUCATION, PRIVATE SECTOR

Many adults in the workforce are poised to retrain, reskill, and retool their skillset allowing them to step into cybersecurity roles organizations are struggling to fill. Transitioning soldiers are a prime audience to benefit from this opportunity. With Fort Riley, Fort Leavenworth, and McConnell Air Force Base throughout the State, Kansas can engage with and train soldiers 6 months before they transition out of service. This fills a workforce gap as well as keeps people in Kansas.

Early Education (EE)

Develop and support efforts to train more K-12 teachers on how to teach computer science or cybersecurity concepts. Additionally, develop and support efforts to boost K-12 retention of teachers already teaching computer science or cybersecurity concepts.

EE.1 LONG | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION, K-12

Investing in teachers early on and through continued professional development, gives them the skills to introduce and teach computer science and cybersecurity concepts to K-12 students. Additionally, investing in teachers provides a more immediate return on investment as they can begin teaching the concepts right away. To support educators, connect them to summer externships and camps like the University of Kansas GenCyber Camp to help them develop their own skills while creating and adapting curriculum for their classrooms.

Develop and support efforts to engage K-12 students early and often regarding computer science and cybersecurity.

EE.2 LONG | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION, K-12

Encouraging and exposing K-12 students to computer science or cybersecurity enhances the possibility that they pursue these career paths in the future. Exposing them to computer science classes or clubs that focus on computer science and cybersecurity are key components. Many of the Kansas universities are developing curriculum to train teachers in the area of computer science.

Recruitment and Retention (RR)

Identify salary differences between public and private jobs and see if and where the public sector can raise wages to be more competitive.

RR.1 LONG | CRITICAL

LOCAL, STATE/AGENCY, HIGHER EDUCATION

Cybersecurity jobs are in incredibly high demand as there is a significant shortage of professionals both globally and nationally. By increasing salaries to be more competitive with the private industry, the public sector can attempt to fill their personnel gaps. An analysis of the jobs and salaries across the state can be conducted as part of a state assessment or landscape analysis. Promoting the information found can encourage conversations with students and families to consider cybersecurity as a career.

Identify possible state-level scholarship opportunities that mirror the Federal Government's Scholarship for Service program.

RR.2 LONG | HIGH

STATE/AGENCY, LOCAL, HIGHER EDUCATION

The scholarship for service program pays for an individual's degree while requiring them to complete government service for a certain number of years after graduation. A whole-of-state specific approach that requires individuals to work for the state, county, or city government could help fill some of the existing staffing shortages, especially in rural and underserved areas. The state has several similar programs for roles such as nurses and teachers.[7]

Using the NIST National Initiative for Cybersecurity Education (NICE) framework (cybersecurity workforce framework), work with the public sector to compartmentalize work with the right job titles and descriptions.

RR.4 LONG

STATE/AGENCY, LOCAL, HIGHER EDUCATION

The NIST NICE framework establishes common tasks, knowledge, skills, and abilities that apply to cybersecurity positions. This framework is used by many organizations in the private sector for their cybersecurity positions. Aligning public sector cybersecurity roles and descriptions to the NICE framework and private sector entities' position descriptions enhances hiring and recruiting, develops career progression paths for employees, and develops education and certification paths. Reclassify and align current public sector job responsibilities and align from a salary standpoint where able.

[7] https://www.kansasregents.org/scholarships_and_grants

FEDERAL FUNDING OPPORTUNITIES

There are several Federal funding opportunities to potentially help advance a whole-of-state approach to cybersecurity in Kansas. The first is funding from the American Rescue Plan Act (ARPA). Funds from the ARPA are dispersed throughout the state to various local governments and the State. A second source of funding is the Infrastructure Investment and Jobs Act (IIJA) which was recently signed into law by President Biden. The IIJA established the Cybersecurity Grant Program which allocates $1 billion over 4 years to State and Local governments. This program has many similarities to the Homeland Security Grant Program (HSGP). Finally, there is a small percentage of the HSGP dedicated to cybersecurity efforts.

To maximize the Federal funds coming into Kansas over the next several years for cybersecurity, it is recommended to approach the spending of these Federal dollars in a coordinated effort across all levels of government. By coordinating efforts, economies of scale can be obtained by all levels of government by potentially pooling resources. In addition, technical assistance or guidance can be provided to entities to assist them in their efforts. The State can better assist this effort by also focusing efforts on building the master cybersecurity contracts through the State procurement process which is a critical recommendation from the Task Force.

OTHER CYBERSECURITY RELATED EFFORTS

The Task Force heard from numerous stakeholders throughout the effort. Many of the stakeholders identified several existing efforts or areas that need further investigation. However, many of these areas were just outside of the scope of the Task Force, align with other efforts already underway, or could not be fully explored within the time frame of the Task Force. The Task Force recognizes the importance of these efforts and supports further exploration and engagement.

Cybersecurity is continuously becoming more and more important to organizations. The wages paid to cybersecurity professionals are well above average. The demand for cybersecurity professionals presents an opportunity to generate significant economic benefits for Kansas. The Kansas Department of Commerce (KDC) engaged in several efforts to promote the economic development of cybersecurity in Kansas. The Task Force supports the efforts of the Kansas Department of Commerce's Kansas Framework for Growth[8] and executing on recommendations from the report on Establishing the State of Kansas as a Center for Cybersecurity Excellence. In addition, KDC has developed many partnerships with organizations that are furthering the development of information technology and cybersecurity in both the academic area as well as economic development. KDC should be considered a critical partner in building a whole-of-state approach to cybersecurity.

Further efforts to promote computer science and cybersecurity in the K-12 education space are critical. By introducing the concepts to kids early and often, multiple benefits can be achieved. By teaching them to be good cyber citizens helps them safely utilize technology at home, school, and with their online presence. In addition, it prepares them to have a good cybersecurity awareness when they enter the workforce. This benefits themselves and their employers. Efforts should also be made to expose the cybersecurity career field to individuals early on. By exposing youth to the cybersecurity career field early, individuals can begin to see themselves potentially going into that career field and put themselves on a path to enter the profession. The Kansas Department of Education has recently approved the use of computer science courses for graduation credits and continues to develop curriculum for Kansas schools. The Task Force recommends and supports continued efforts to introduce computer science and cybersecurity into the K-12 space.

Finally, cybercrime is rapidly evolving. The perpetrators of cyber-related crimes have changed the way they conduct their activities. In addition, many other criminal activities may be facilitated through the use of technology. While outside the scope and expertise of this Task Force, it is recommended that an effort be made to thoroughly review existing cybercrime laws in Kansas. The laws should be updated to coincide with the activity and the damages that can result from such criminal activity. By updating the laws related to cybercrime, it can better allow our law enforcement organizations to pursue and prosecute this type of activity.

[8] https://www.kansascommerce.gov/kansas-framework-for-growth/

NEXT STEPS

Currently, there is a significant amount of synergy around cybersecurity in Kansas. The recommendations from the Task Force should serve as starting points to advance a whole-of-state approach to cybersecurity in Kansas. The Task Force took care to ensure that recommendations produced are actionable and achievable. A focused effort will need to be made to work on the recommendations by the various stakeholders throughout the state. Resources and funding may be needed to execute certain recommendations. However, there are many recommendations that will only require time and effort. There are many existing structures and resources that can be leveraged to begin or are willing to execute on many of the priority recommendations immediately. Leveraging those existing structures and resources to establish a near-term governance structure can help guide many of the efforts and identify a financial framework that may help fund many of the recommendations.

GLOSSARY OF TERMS

Political Subdivision - Political subdivision is defined "as a reference to a subordinate governmental entity which exists for the purpose of discharging some function of local government within a prescribed territory and which has a governing body possessed of prescribed powers of self-government."

Critical Infrastructure – Refers to the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD-21):

1. Chemical sector
2. Commercial facilities sector
3. Communications sector
4. Critical manufacturing sector
5. Dams sector
6. Defense industrial base sector
7. Emergency services sector
8. Energy sector
9. Financial services sector
10. Food and agriculture sector
11. Government facilities sector
12. Healthcare and public health sector
13. Information technology sector
14. Nuclear reactors, materials, and waste sector
15. Transportation systems sector
16. Water and wastewater systems sector

EXECUTIVE ORDER NO. 21-25

Establishing the Governor's Cybersecurity Task Force

WHEREAS, critical infrastructure, information systems, and networks in Kansas and around the globe face a barrage of increasingly sophisticated cyberattacks perpetrated by foreign and domestic actors;

WHEREAS, protecting Kansas' digital infrastructure is vital to ensuring continued access to critical services provided by both the public and private sectors;

WHEREAS, ransomware attacks in 2019 cost government agencies, academic institutions, and healthcare providers more than $7.5 billion in information loss and operations disruption;

WHEREAS, significant disruptions to economic activity, citizens' privacy, public safety, and the consistent delivery of services have occurred and will continue to occur as a direct result of cyberattacks on critical infrastructure;

WHEREAS, healthcare facilities, water treatment plants, local governments, small businesses, and other entities across Kansas have been the targets of cyberattacks in recent years;

WHEREAS, cyberattacks pose a persistent threat to confidence in public institutions;

WHEREAS, an effective response to escalating and rapidly evolving cybercrime requires a sustained and coordinated partnership between state government, the private sector, local governments, law enforcement agencies, and other entities that embraces a whole-of-state approach to cybersecurity;

WHEREAS, the increasing frequency, severity, and complexity of cyberattacks necessitates enhanced levels of incident management, information sharing, coordination, and emergency response between state government, local government, the private sector, law enforcement agencies, academic institutions, federal agencies, and other entities to best protect Kansans and their digital assets;

WHEREAS, Kansas is well-positioned to benefit from lessons learned by other states that have implemented cybersecurity initiatives and the U.S. Department of Homeland Security; and

WHEREAS, this Administration will do whatever it can to improve Kansas' cybersecurity posture and resilience.

NOW, THEREFORE, pursuant to the authority vested in me as Governor of the State of Kansas, I hereby establish the Governor's Cybersecurity Task Force ("Task Force"):

1. **Membership**. The Governor shall appoint the following to serve as members of the Task Force:
    a. The State Chief Information Technology Officer, or designee (ex officio)
    b. The State Chief Information Security Officer, or designee (ex officio)
    c. The Adjutant General of the Kansas National Guard, or designee (ex officio)
    d. The Attorney General, or designee (ex officio)

e. The Secretary of State, or designee (ex officio)
f. The Director of the Kansas Criminal Justice Information System (ex officio)
g. The Director of the Kansas Intelligence Fusion Center (ex officio)
h. A representative from the Kansas Division of Emergency Management
i. A representative of county governments
j. A representative of municipal governments
k. A representative from a Regents institution
l. Two representatives of critical infrastructure sectors such as energy, healthcare, or transportation
m. Two representatives from the Joint Committee on Information Technology
n. Additional individuals the Governor determines have relevant experience or qualifications; if appropriate, the Governor may determine that any such individual should serve in an advisory, non-voting capacity.

2. **Organization.** The Governor shall select a chair and vice-chair, or co-chairs, from the Task Force's membership, and the Task Force may establish rules for the Task Force's meetings and conduct of business.

3. **Terms.** Members shall serve at the pleasure of the governor.

4. Members shall receive no compensation or reimbursements for expenses and shall serve voluntarily. Officers or employees of state agencies who are appointed to the Task Force as part of their duties shall be authorized to participate on the Task Force and may claim subsistence, allowance, mileage, or associated expenses from their respective agency budgets as permitted by law.

5. The Task Force shall be subject to the Kansas Open Records Act and the KansasOpen Meetings Act.

6. Plans, reports, or recommendations of any nature adopted by the Task Force shall be considered advice to the Governor, and shall not be construed as official policies, positions, or interpretations of laws, rules, or regulations by any department or agency of state government, nor shall any such department or agency be bound in any manner to consider such advice when conducting their advisory and regulatory affairs.

7. The Task Force shall:
    a. Facilitate cross-industry and cross-government collaboration to share best practices and mitigate cybersecurity risks related to critical infrastructure and protected systems;
    b. Identify opportunities to improve the overall cybersecurity posture across all levels of government within Kansas;
    c. Identify partnerships and avenues to maximize and leverage existing cybersecurity resources within the state;
    d. Develop a framework for coordinated information sharing, response, simulation, testing, and mutual assistance between the government and privatesectors;
    e. Develop a coordinated and collaborative State of Kansas Cyber ResponsePlan;
    f. Recommend appropriate and cost-effective safeguards to reduce, eliminate, or recover from identified threats to data;
    g. Recommend resources and possible methods to accomplish the recommendations identified above; and

h. 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 futurework. By December 5, 2021, the Task Force shall submit a comprehensive report and recommendations to the Governor.

8. The Task Force shall meet as determined by the chairs in order to meet the obligations set forth by this order.

9. The Task Force shall be staffed by the Kansas Information Security Office.

10. The Commission shall meet virtually, or in-person as recommended by public health guidance.

This document shall be filed with the Secretary of State as Executive Order No. 21-25. It shall become effective immediately and remain in force until June 30, 2022.

THE GOVERNOR'S OFFICE
July 13, 2021

APPENDIX

APPENDIX A

KANSAS CYBERSECURITY GOVERNANCE STRATEGY

Executive Summary

Cyber threats are an increasingly unpredictable, dangerous, and proliferating hazard to state, local, and tribal governments, as well as private industry and operators of critical infrastructure systems within the State of Kansas. Every day, networks are under attack across the state from a variety of sources, using a variety of methods, all of which are growing in sophistication.

The State of Kansas is developing a plan to address these challenges with a whole-of-state approach. Recognizing the need to provide leadership, share information, and develop resources for a whole-of-state approach to cybersecurity and its impact on the citizens, industry, infrastructure, and government of the State of Kansas, this governance strategy was developed in coordination with the Strategic Vision and Planning Sub-committee recommendations.

Due to the hierarchy of law and the separation of powers, an Executive Order lacks the authority to sustain a change in leadership. Therefore, it is highly recommended that the authority, responsibility, and accountability of this governance body be codified by legislative action into law. Without empowering legislation, the extremely important work of cybersecurity governance will become distracted by changing political winds.

Vision

Develop all of Kansas into a center of excellence regarding cyber education, collaboration, and trust.

Mission

Develop and facilitate a whole-of-state cybersecurity initiative that will raise the security posture of all public and private sector organizations in Kansas, through leadership, information sharing, resource development, education, and incident response preparedness.

Principles of Whole-of-State Cybersecurity Governance

1. **Leadership** – Each respective government and private sector organization has a need for increased cybersecurity awareness and defense. The leadership of this body should seek to promote and communicate best practices in the area of cybersecurity to all levels of state, local, and tribal governments; critical infrastructure owners and operators; and other private sector stakeholders.

2. **Information Sharing and Education** – Information sharing is a principal component of this body's work to improve all stakeholders' ability to manage, mitigate, and respond to the increased risk posed by the cybersecurity threats faced today. This principle further recognizes that information sharing between public and private partners needs to be reciprocal including information about cyber and physical threats and mitigation strategies.

3. **Shared Responsibility** – This body adheres to the belief that all Kansas stakeholders – individuals, private sector organizations, and government agencies have a shared interest with complementary roles and responsibilities in protecting the whole-of-state from malicious cyber activity and managing cyber incidents and their consequences.

4. **Collaborative Command** – Because the large number of public and private cybersecurity stakeholders possess different strengths, weaknesses, authorities, and capabilities that will all need to be brought to bear on any cyber incident; collaboration and coordination will be required to achieve optimal results. Thus, when responding to a cyber-incident in the public or private sector, unity of effort synchronizes the overall state response, which prevents gaps in service and duplicative efforts.

5. **Respecting Privacy** – It is understood that private sector stakeholders hold their privacy and security in high regard and, in some cases, are even forbidden by law to share some information about their environments. Therefore, to the extent permitted under law, this body will respect the privacy, civil liberties, and sensitive information, and generally will defer to the affected entities in notifying other affected private sector entities and the public. In the event of a significant cyber incident where the government interest is served by issuing a public statement concerning an incident, state responders will coordinate their approach with the affected entities to the extent possible.

Governance Structure

Traditionally, cybersecurity governance refers to the governance of cyber risk and cyber threats. The ISO/IEC 27001 standard defines cybersecurity governance as, "The system by which an organization directs and controls security governance, specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks."

Within the confines of a single organization or entity, cybersecurity is considered a technical or operational issue to be handled in the technology space. However, because this body seeks to position itself and its work as a whole-of-state function designed to facilitate information sharing; align planning and preparation; promote education and best practice; and coordinate incident response activities, its work shall be more of an umbrella function guiding and advising the detailed work of other public and private sector organizations.

This governance body is designated to include and support the cybersecurity efforts of all public and private organizations in the state of Kansas and shall include representatives from:

Cybersecurity Executive Group

a. State Chief Information Technology Officer or designee
b. State Chief Information Security Officer or designee
c. The Adjutant General of the Kansas National Guard or designee
d. The Attorney General or designee
e. Secretary of State or designee
f. A representative from the Kansas Division of Emergency Management
g. Director of Kansas Criminal Justice Information System Committee
h. Director of the Kansas Intelligence Fusion Center
i. A representative from a municipal government
j. A representative from the Regents institutions
k. Two representatives from critical infrastructure
l. Representation by members of the Legislature
m. Representative of county governments
n. Judicial CITO
o. Legislative CITO

Cybersecurity Working Group

This group should have the authority to develop, in coordination with the Executive Group, an umbrella function guiding a whole-of-state approach to sharing of information, collaboration, memorandums of understanding, and incident coordination across the state of Kansas with governments, critical infrastructure, businesses, and citizens. Establishing and maintaining these partnerships are essential to the best interest of the State of Kansas to proactively engage them, early and often.

a. Cyber Liaison Officer (Lead)
b. Cyber Liaison Officer (Intelligence)
c. Cyber Liaison Officer (Technical)
d. Cyber Liaison Officer (Government)
e. Cyber Liaison Officer (Business)
f. Cyber Liaison Officer (Critical Infrastructure)
g. Cyber Liaison Officer (Public Information)

Governance Strategies

1. **Risk Identification and Mitigation**
   Cybersecurity risk identification and mitigation involves the use of security policies and processes to reduce the overall risk or impact of a cybersecurity threat.

   This governance body shall use its authority and influence to help all public and private sector organizations in Kansas to identify gaps and needs in existing cybersecurity posture.

2. **Strategy and Planning**

   A cybersecurity plan is an organization's guide to follow and improve its overall risk management and defenses against the ongoing threat of cybercrime.

   This governance body shall use its authority and influence to help all public and private sector organizations in Kansas to identify and inventory their cybersecurity capabilities and resources and identify partnership opportunities.

3. **Information Sharing**

   Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. By exchanging cyber threat information within Kansas, public and private sector organizations can leverage the collective knowledge, experience, and capabilities of the whole-of-state to gain a more complete understanding of the threats the organizations may face.
   This governance body shall use its authority and influence to help all public and private sector organizations in Kansas to identify key communication and collaboration paths for cybersecurity issues; identify who owns the communication/collaboration process; and identify collaboration and communication opportunities (State cyber conference, cyber workshops, interacting with other IT groups).

4. **Incident Response**

   Incident response (IR) refers to the plan for responding to a cybersecurity incident to quickly contain, minimize, and avoid damage. But not every cybersecurity event in Kansas will be serious enough to warrant activation of a whole-of-state incident response plan. The incident response plan will have to identify when an IR should be initiated at the state level because initiating an IR every time a false positive or unsuccessful attack occurs can be costly, not to mention desensitizing to the rest of your organization.

   This governance body shall use its authority and influence to develop a whole-of-state incident response plan and protocols designed to identify how the state should respond to public and private sector organization incidents and establish the responsibilities of various agencies and organizations during significant incidents.

5. **Budget and Resources**

   How much does Kansas need to invest in terms of money, person-hours, and other resources to promote, provide and facilitate adequate cybersecurity to all public and private sector organizations in Kansas? Budgeting for cybersecurity is a challenging process, in part because developing and implementing security measures is not a one-time task. It is an ongoing series of interrelated agile processes designed to both proactively and reactively address cyber threats and risks. Developing appropriate cybersecurity resources should be a priority.

   This governance body shall use its authority and influence to help all public and private sector organizations in Kansas to identify what the state can do to help with the high cost of cybersecurity (Open contracts, grants, personnel, services) and identify funding needs and opportunities to meet those needs (Grants, budgets, chargeback).

6. **Workforce Development and Education**
   Demand for cybersecurity and information security resources has been growing for decades. It is imperative to the success of any cybersecurity program to have a strong workforce of qualified and prepared cybersecurity specialists and a pipeline of future cybersecurity resources to populate the labor pool.

   This governance body shall use its authority and influence to evaluate opportunities to apply or further research to establish a Cyber Center of Excellence; identify partnership opportunities with local universities; identify training needs to enhance workforce; identify a staff training pipeline; and identify other state efforts to introduce computer science/cyber into grade school curriculum.

Sub-committee's recommendation on missions, goals, and priority strategies.

Sub-Committee Strategic Vision and Planning

Mission: Develop and facilitate a whole-of-state cybersecurity initiative that will raise the security posture of all public and private sector organizations in Kansas, through leadership, information sharing, resource development, education, and incident response preparedness.

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

Priority Strategies:

1) Continue the Task Force giving time for the whole-of-state formal cybersecurity governance to be developed for Kansas and ratified by the Legislature in statute. This Task Force is critical to continue driving, coordinating, and organizing a whole-of-state approach.
2) Identify funding
3) Identify a dedicated group to carry out the mission, goals, and strategies of the governor.

Sub-Committee Statewide Coordination and Collaboration

Mission: Establish public/public and public/private mutual threat and mitigation information sharing and community collaboration with a proactive program of assessments, guidance, and MOUs

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

Priority Strategies:

1) Create a cybersecurity position(s) to focus on communicating, coordinating, and collaborating with public and private cybersecurity partners.
2) Begin building and establishing formal relationships with local governments, K-12, Regents institutions, critical infrastructure, and other partners.
3) Conduct an annual conference with public and private partners

4) Conduct a state assessment of current cybersecurity capabilities across the state.

Sub-Committee Cyber Disruption and Incident Response

Mission: Provide incident response preparedness and assistance with a developed combination of a mutual aid structure of public and private partners and subject matter experts.

Goal: To build and extend a culture of awareness and preparedness throughout the state of Kansas and to develop a mechanism for information and resource sharing; knowledge transfer, and skills development in both preparations for, response to, and recovery from cybersecurity incidents.

Priority Strategies:

1) Establishment of a set of standards that is available to all public and private sector participants and provide access to the information and other best practice material to aid public and private sector organizations in preparation and planning for cybersecurity incident response. The information will need to be continuously maintained and refreshed so the content remains relevant and applicable.
2) Development and implementation of a cybersecurity incident response partner program. This partner program provides access to pre-negotiated contract vehicles for hardware, software, and services; funding support for cybersecurity initiatives; and cybersecurity mutual aid or retainer agreements.

Sub-Committee Workforce Development and Education

Mission: To develop partnerships with commerce, academia, and K–12 schools throughout Kansas to create a highly skilled and educated workforce and public. To develop information technology career paths to enhance opportunities throughout the state to attract technology companies and career opportunities to Kansas.

Goal #1: Utilize all available resources to provide education on cybersecurity to all entities within the State of Kansas. Extend these resources to all interested parties within the state.

Priority Strategies:

1) Find opportunities to make cybersecurity resources available through collaborating and sharing across the state and across entities
2) Define what resources need to be included
3) Create an inventory of all interested parties
4) Identify a dedicated group to carry out these strategies

Goal #2: Develop, coordinate, or inform the workforce to provide opportunities to learn, engage and practice cybersecurity for entities within the state of Kansas. Make this training available starting in K-12 and extending through adult learning.

Priority Strategies:

1) Create common learning opportunities across all sectors
2) Identify successful implementations, coordinate and replicate
3) Identify a dedicated group to carry out these strategies

APPENDIX B

THANK YOU

We would be remiss if we did not give a proper thank you to all the organizations and individuals who took their time meeting with the Task Force and subcommittees to share their experiences and expertise. Your insights provided us with valuable information that guided us in the development of these recommendations.

From law enforcement and business associations to K-12 and higher education, these are just a few of the types of entities that joined us as thought partners to provide information on what's working in their organizations and what the Task Force should consider. A special thank you to the following individuals and organizations who joined our meetings to talk with Task Force members:

John Guerriero, NGA
Meredith Ward and Doug Robinson, NASCIO
Tony Weingartner and Ryan Boyer, KBI
Dr. Eugene Vasserman, Kansas State University Center for Information and Systems Assurance
Mike Mayta, City of Wichita
Jonathan York, KDEM
Col. David Hewlett, Kansas National Guard
Joe Jabara and Ken Harmon, Wichita State University
Bill Glynn, KIFC
Trent Armbrust, Department of Commerce
Cort Buffington, KanREN
Bruce Chladny, KAC
Erik Sartorius, LKM
Leo Haynos, KCC
April Boyd-Noronha, University of Saint Mary
Sharmelle Winsett, KC Scholars
Steven Funk, Kansas Board of Regents
Dr. Stephen King and Meg Richard, Kansas Department of Education
Geoff Jenista, DHS Region 7 Cybersecurity Navigator
Matt Singleton, State of Oklahoma
Cameron Gray, City of Tulsa
Kylie Dickneite and Angela Robinson, State of Missouri
Alisha King, Brig. Gen. Gent Welsh, and Zack Hudgins, Washington State
Cinnamon Albin, State of Oregon

APPENDIX C

Bi-Weekly Task Force Meetings

The full Task Force held eight (8) bi-weekly meetings. Meetings were hosted on a virtual platform and open to the public through a live stream on YouTube. Meetings included presentations from relevant Kansas stakeholders and outside experts. Meetings also provided opportunities for task force members to discuss stakeholder feedback and information gathered during learning sessions.

Task Force Meetings: Focus of Discussion	Date
Opening Remarks from Governor Kelly and Task Force Member Introductions. Presentation from NGA on "National Landscape of Cyber Governance and Strategies"	8/10/2021
Organizational Cybersecurity Capabilities Presentations from, The KBI, Kansas State University Center for Information and Systems Assurance, City of Wichita, KDEM, and the Kansas National Guard	9/1/2021
Organizational Cybersecurity Capabilities Presentations from Wichita State University, Kansas Intelligence Fusion Center	9/15/2021
Discussion of and Approval of Recommendations for the Initial Report.	9/29/2021
Presentation of the Kansas Framework for Growth and National Security Crossroads, Incident Response and Best Practices from the City of Tulsa	10/13/2021
Guidance on Final Report, Report Outs of New Ideas from Subcommittees	10/27/2021
Update on Infrastructure Investment and Jobs Act, Review of Public Feedback and Recommendations	11/10/2021
Discussion of and Approval of Recommendations for Final Report.	12/1/2021

Subcommittee Meetings

In addition to the full Task Force meetings, the various subcommittees met regularly to hear from various stakeholders and partners and to begin identifying specific recommendations. Each subcommittee then reported out the to the full Task Force on their discussions and recommendations.

Task Force Subcommittee Meetings	Date
Strategic Vision and Planning	
Introduction to the subcommittee and its goal. State of Kansas Chief Information Security Officer "State Cybersecurity Governance and Strategies"	8/25/2021
Presentation from NGA "NGA Policy Academy to Advance Whole-of-State Cybersecurity"	9/8/2021
Recommendation Discussion	9/22/2021
Discussion on Interim Report	10/20/2021
Presentations from the State of Missouri and State of Oklahoma	11/3/2021
Prioritization and Fine Tuning of Recommendations	11/17/2021
Statewide Coordination and Collaboration	
Introduction to the subcommittee and its goal. Presentation from NASCIO "Statewide Cybersecurity Coordination and Collaboration "	8/27/2021
Presentations from KanREN, Kansas Board of Regents, and Wichita State University	9/10/2021
Presentations from the KCC and LKM	9/24/2021
Presentations from the State of Oregon and State of Washington	10/22/2021
Presentation from the KCC	11/5/2021
Prioritization and Fine Tuning of Recommendations	11/19/2021
Cyber Incident and Disruption Response	
Introduction to the subcommittee and its goal. Presentation from National Association of State Chief Information Officers "Cyber Incident & Disruption Response "	8/27/2021
Recommendations Discussion	9/10/2021
Presentation from Department of Homeland Security Region 7 Cybersecurity Coordinator	9/24/2021
Presentations from the State of Oregon and State of Washington	10/22/2021
Recommendations Discussion	11/5/2021
Prioritization and Fine Tuning of Recommendations	11/19/2021
Workforce Development and Education	
Introduction to the subcommittee and its goal. Presentation from National Association of State Chief Information Officers "Cybersecurity Workforce Overview "	8/25/2021
Presentation from NGA "Workforce Development"	9/8/2021

Recommendation Deep Dive	9/22/2021
Organizational Cybersecurity Capabilities Presentation from University of Saint Mary, Organization Presentations from KC Scholars and Kansas Department of Education	10/20/2021
Discussion of Recommendations, Visiting Other Subcommittees	11/3/2021
Prioritization and Fine Tuning of Recommendations	11/17/2021

TASK FORCE MEETING AGENDAS

CYBERSECURITY TASK FORCE

Tuesday, August 10
9:00-11:30 am
Recorded Meeting

Agenda

9:00 am	**Opening Remarks (Jeff Maxon and Mike Mayta)**
	Welcome Remarks – Governor Laura Kelly
	Members and Introductions
	Task Force Overview
	National Governors Association (NGA) Overview – John Guerriero
	State of Kansas – What's happening in Kansas related to Cybersecurity
	Subcommittee Overview
	Closing Remarks
11:30 am	**Conclude**

CYBERSECURITY TASK FORCE

Wednesday, September 1
10:00-12:00 pm
Recorded Meeting

10:00 am	**Opening Remarks (Jeff Maxon and Mike Mayta)**
10:05 am	**Capabilities Briefings** **Tony Weingartner, KBI**
10:20 am	**Dr. Eugene Vasserman, Director, KSU Center for Information and Systems Assurance**
10:35 am	**Mike Mayta, City of Wichita**
10:50 am	**Jonathan York, KDEM**
11:05 am	**Col. David Hewlett, National Guard**
11:20 am	**Subcommittee Updates** **5 min review from chairs of what each subcommittees discussed**
11:40 am	**Open discussion**
12:00 pm	**Conclude**

CYBERSECURITY TASK FORCE

Wednesday, September 15
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Introduction of Accenture (Jeff Maxon)**

10:05 am **Joe Jabara, Director, HUB for Cybersecurity Education and Awareness, Wichita State University**

10:35 am **Bill Glynn, Director, Kansas Intelligence Fusion Center**

10:55 am **Open Discussion on Subcommittee Activities (Jeff)**

- Overlapping themes, recommendations

11:45 am **Next Steps (Jeff Maxon)**

12:00 pm **Conclude**

CYBERSECURITY TASK FORCE

Wednesday, September 29
10:00-12:00 pm
Recorded Meeting

9:00 am **Opening Remarks and Framing (Jeff Maxon and Mike Mayta)**

9:15 am **Recommendations Discussion**
- Strategic Visioning and Planning – Overview from Subcommittee
- Go line-by-line

10:00 am **Break**

10:10 am **Recommendations Discussion**
- Workforce Development and Education – Overview from Subcommittee
- Go line-by-line

10:55 am **Break**

11:05 am **Recommendations Discussion**
- Cyber Incident and Disruption Response – Overview from Subcommittee
- Go line-by-line

11:50 am **Break**

12:00 pm **Recommendations Discussion**
- Statewide Coordination and Collaboration – Overview from Subcommittee
- Go line-by-line

12:45 pm **Final Comments, Next Steps (Jeff Maxon and Mike Mayta)**

1:00 pm **Conclude**

CYBERSECURITY TASK FORCE

Wednesday, October 13
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks (Jeff Maxon and Mike Mayta)**

10:10 am **Interim Report Discussion**

10:30 am **Kansas Framework for Growth and National Security Crossroads (Trent Armbrust, Department of Commerce)**

11:00 am **Report 2**

- New Recommendations
- Deeper dive into broader recommendations
- K-12 – LPA report on their cybersecurity – what do districts have

11:30 am **Incident and Response Best Practices with the City of Tulsa (Cameron Gray, IT Operations IT Security and Special Operations Manager)**

12:00 pm **Conclude**

CYBERSECURITY TASK FORCE

Wednesday, October 27
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening and Welcome (Jeff Maxon and Mike Mayta)**

Subcommittee Report Outs

- Overview of subcommittee meetings from the week of October 18
- New ideas, takeaways from the subcommittee meetings

Schedule

- Canceling meeting on Wednesday, November 24
- Scheduling an extended meeting week of November 29 to prepare recommendations for final report

12:00 pm **Conclude**

CYBERSECURITY TASK FORCE

Wednesday, November 10
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening and Welcome (Jeff Maxon and Mike Mayta)**

Infrastructure Investment and Jobs Act (Secretary Burns-Wallace)

Public Feedback (Jeff Maxon and Mike Mayta)

Recommendations

- Review what we determined needed significant work during the review of the interim report

12:00 pm **Conclude**

CYBERSECURITY TASK FORCE

Wednesday, December 1
9:00-1:00 pm
Recorded Meeting

9:00 am	**Opening Remarks and Framing (Jeff Maxon and Mike Mayta)**
9:15 am	**Overall Report Discussion**
10:20 am	**Break**
10:30 am	**Recommendations Discussion**
11:45 am	**Break** • Grab Lunch
12:00 pm	**Recommendation Discussion**
12:45 pm	**Final Comments, Next Steps (Jeff Maxon and Mike Mayta)**
1:00 pm	**Conclude**

STRATEGIC VISION AND PLANNING SUBCOMMITTEE MEETING AGENDAS

STRATEGIC VISIONING AND PLANNING SUBCOMMITTEE

Wednesday, August 25
3:00-5:00 pm
Recorded Meeting

3:00 pm	**Opening Remarks and Introductions (John Berghuis)**
3:10 pm	**Speaker (Jeff Maxon)**
3:30 pm	**Open Discussion (Subcommittee Members)**
4:30 pm	**Additional Resources (John Berghuis)**
5:00 pm	**Adjourn**

STRATEGIC VISIONING AND PLANNING SUBCOMMITTEE

Wednesday, September 8
3:00-5:00 pm
Recorded Meeting

3:00 pm **Opening Remarks and Recap of Previous Meeting (John Berghuis)**

3:10 pm **Speaker (John Guerriero, NGA)**

3:35 pm **Recommendations Discussion (Subcommittee Members)**

- Review of strategy statements, goals, and objectives
- Draft recommendations

5:00 pm **Adjourn**

STRATEGIC VISIONING AND PLANNING SUBCOMMITTEE

Wednesday, September 22
3:00-5:00 pm
Recorded Meeting

3:00 pm **Recommendations Discussion**

5:00 pm **Adjourn**

STRATEGIC VISIONING AND PLANNING SUBCOMMITTEE

Wednesday, October 20
3:00-5:00 pm
Recorded Meeting

3:00 pm **Welcome and Introduction (John Berghuis)**

Open Discussion on Interim Report

- Looking at the recommendations from the other subcommittees, think about how to pull those together into an overall strategy

5:00 pm **Adjourn**

STRATEGIC VISIONING AND PLANNING SUBCOMMITTEE

Wednesday, November 3
3:00-5:00 pm
Recorded Meeting

3:00 pm **Welcome and Introductions (John Berghuis)**

Speaker (Matt Singleton, State of Oklahoma)

- Q&A to Follow

Speakers (Kylie Dickneite and Angie Robinson, Missouri Department of Public Safety)

- Q&A to Follow

Open Discussion on Recommendations

- Notes from other meetings
- Recommendations based on what was heard today and the last few meetings
- Recommendations from interim report we should consider adding context to or refining
- Prioritization of recommendations

5:00 pm **Adjourn**

STRATEGIC VISIONING AND PLANNING SUBCOMMITTEE

Wednesday, November 17
3:00-5:00 pm
Recorded Meeting

3:00 pm **Welcome (John Berghuis)**

Review of Subcommittees Recommendation on Missions, Goals, and Priority Strategies

5:00 pm **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE MEETING AGENDAS

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE

Friday, August 27
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Introductions (John Godfrey)**

10:10 am **Speaker (Doug Robinson, NASCIO)**
- Overview and Q&A

10:40 am **Open Discussion (John Godfrey)**

11:40 am **Resources (John Godfrey)**

12:00 pm **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE

Friday, September 10
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Recap of Previous Meeting (John Godfrey)**

10:05 am **Presenter (Cort Buffington, Executive Director, KanREN)**
- Q&A to follow

10:30 am **Recommendations Discussion**

11:00 am **Presenters (Steve Funk, Director of IT, Kansas Board of Regents and Ken Harmon, CIO, WSU)**
- Q&A to follow

11:30 am **Recommendations Discussion Continued**

12:00 pm **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE

Friday, September 24
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening and Introductions**

10:10 am **Speaker (Erik Sartorius, League of Kansas Municipalities)**
- Overview and Q&A

10:30 am **Speaker (Bruce Chladny, Kansas Association of Counties)**
- Overview and Q&A

10:50 am **Recommendations Discussion**

12:00 pm **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE

Friday, October 22
10:00-12:00 pm
Recorded Meeting

10:30 am **Speakers (Alisha King, Brig. Gen. Gent Welsh, Zach Hudgins, State of Washington)**

11:00 am **Recommendations Discussion**

- Where do we go from here?
- What needs to be refined?
- What are new recommendations to consider?

12:00 pm **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE

Friday, November 5
10:00-12:00 pm
Recorded Meeting

10:00 am **Welcome (John Godfrey)**

Speaker (Leo Haynos, Kansas Corporation Commission)

- Q&A to Follow

Recommendations Discussion

- Review any public feedback
- Discussion of ideas from other meeting notes or other ideas we have from our own notes
- Recommendations from the interim report that need more context or refinement
- Prioritization, if any, of the recommendations – low hanging fruit that can be quickly accomplished, recommendations that need to happen first before others can be tackled

12:00 pm **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMMITTEE

Friday, November 19
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks (John Godfrey)**

Recommendations Discussion

- Clarify and Refine Interim Report Recommendations
- New Recommendations
- Themes of Recommendations
- Priority of Recommendations

12:00 pm **Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE MEETING AGENDAS

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE

Friday, August 27
9:00-11:00 am
Recorded Meeting

9:00 am **Opening Remarks and Introductions (Charles King)**

9:10 am **Speaker (Doug Robinson, NASCIO)**
- Overview and Q&A

9:40 am **Open Discussion (Charles King)**

10:40 am **Resources (Charles King)**

11:00 am **Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE

Friday, September 10
9:00-11:00 am
Recorded Meeting

9:00 am	**Opening Remarks and Introductions (Charles King)**
9:10 am	**Overview of Draft Response and Model, Recommendations Discussion**
11:00 am	**Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE

Friday, September 24
9:00-11:00 am
Recorded Meeting

9:00 am **Introduction (Charles King)**

9:05 am **Speaker (Geoff Jenista, Cybersecurity and Infrastructure Security Agency)**
- Overview and Q&A

9:30 am **Opening Discussion on Draft Proposal and Recommendations**

11:00 am **Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE

Friday, October 22
9:00-11:00 am
Recorded Meeting

9:00 am **Welcome (Charles King)**

Speaker (Cinnamon Albin, State of Oregon)

- Q&A to Follow

Speakers (Alisha King, Brig. Gen. Gent Welsh, Zach Hudgins, State of Washington)

11:00 am **Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE

Friday, November 5
9:00-11:00 am
Recorded Meeting

9:00 am	**Welcome (Charles King)**
	Open Discussion on Recommendations
11:00 am	**Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMMITTEE

Friday, November 19
9:00-11:00 am
Recorded Meeting

9:00 am **Opening Remarks (Charles King)**

Recommendations Discussion

- Clarify and Refine Interim Report Recommendations
- New Recommendations
- Themes of Recommendations
- Priority of Recommendations

11:00 am **Adjourn**

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE MEETING AGENDAS

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE

Wednesday, August 25
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Subcommittee Goal (Secretary DeAngela Burns-Wallace)**
- Introduction of Meredith Ward, NASCIO

10:10 am **Workforce Development Overview (Meredith Ward, NASCIO)**
- Q&A throughout and to follow

10:30 am **Open Discussion (Secretary DeAngela Burns-Wallace)**

11:30 am **Resources (Secretary DeAngela Burns-Wallace)**

12:00 pm **Adjourn**

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE

Wednesday, September 8
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Brief Recap of Previous Meeting (Secretary DeAngela Burns-Wallace)**

10:15 am **Workforce Development (John Guerriero, NGA)**

- Q&A to Follow

10:35 am **Recommendations Discussion (Secretary DeAngela Burns-Wallace)**

12:00 pm **Adjourn**

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE

Wednesday, September 22
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Framing (Secretary DeAngela Burns-Wallace)**

10:10 am **Recommendations Deep Dive (Secretary DeAngela Burns-Wallace)**

12:00 pm **Adjourn**

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE

Wednesday, October 20
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Introduction of Speaker (Secretary DeAngela Burns-Wallace)**

10:05 am **Speaker (April Boyd-Noronha, University of Saint Mary)**

- Q&A to Follow

10:45 am **Introduction of Next Speaker (Secretary DeAngela Burns-Wallace)**

Speaker (Sharmelle Winsett, KC Scholars)

- Q&A to Follow

11:20 am **Introduction of Next Speakers (Secretary DeAngela Burns-Wallace)**

Speakers (Meg Richard and Stephen King, Kansas Department of Education)

- Q&A to Follow

12:00 pm **Adjourn**

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE

Wednesday, November 3
10:00-12:00 pm
Recorded Meeting

10:00 am **Opening Remarks and Framing (Secretary DeAngela Burns-Wallace)**

10:10 am **Recommendations Deep Dive (Secretary DeAngela Burns-Wallace)**

12:00 pm **Adjourn**

WORKFORCE DEVELOPMENT AND EDUCATION SUBCOMMITTEE

Wednesday, November 17
10:00-12:00 pm
Recorded Meeting

10:30 am **Opening Remarks and Framing (Secretary DeAngela Burns-Wallace)**

- Introduction of guest and thought partner – Trent Armbrust, Department of Commerce

Prioritization of Recommendations

New Recommendations

12:00 pm **Adjourn**