Kansas Cybersecurity Task Force

OCTOBER 2021

Kansas Cybersecurity Task Force Interim Report

Report to

Governor Laura Kelly

[THIS PAGE WAS INTENTIONALLY LEFT BLANK]

FROM THE CO-CHAIRS

First, we would like to thank Governor Laura Kelly for launching the Kansas Cybersecurity Task Force. Cyberattacks are a growing threat to all organizations and individuals within Kansas. Cyberattacks could create significant disruption for government entities, critical infrastructure, and private organizations. By working together on cybersecurity with a "Whole-of-State" approach we can provide efficient and effective direction, coordination, response, and education for all Kansans.

We want to thank the Task Force members for their time and ideas. We recognize that participation in this Task Force was not a light ask and it required a significant amount of time and effort. We realize that their time is valuable and their commitment to this effort is appreciated. The members' thought leadership is a critical component to the success of this effort.

Further, we would want to thank all individuals and organizations who contributed their time and expertise in presenting to the Task Force and subcommittees. The information and ideas shared with the members helped frame the cybersecurity landscape within Kansas. We were impressed by the sheer number of interested parties wanting to share with the Task Force.

We want to extend a special thank you to John Guerriero from the National Governors Association (NGA). NGA's Policy Academy to Advance the Whole-of-State Cybersecurity has been an incredible partnership that has allowed the Task Force to understand the national landscape and what other states have successfully accomplished. We would not have been able to gather that information within our timelines.

Lastly, we would especially like to thank the individuals that assisted the Task Force. There was a great deal of planning, coordinating, and organizing of the work for the Task Force. Thank you to Allie Denning and Samir Arif from the Department of Administration Public Affairs Office for the work they did to support the Task Force. Without their efforts, the Task Force would not be able to successfully function.

This initial report provides recommendations on addressing the cybersecurity challenges with a "Whole-of-State" approach. There is still much room for continued collaboration and growth. We are encouraged by the discussion and participation that has already occurred. Kansas has a significant amount of cybersecurity capabilities within the state. There is significant momentum, and we want to continue to press forward. We look forward to the additional recommendations that the Task Force develops and the future opportunities to ensure that the State of Kansas is a safe place for all digital engagements across all sectors.

Mike Mayta
Co-Chair

Jeff Maxon
Co-Chair

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 to 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 consists of subject matter experts from various stakeholder organizations. Members represent multiple viewpoints consisting of state government, local government, academia, private sector, and critical infrastructure. The Task Force is 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 are 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 have met on a biweekly basis since August of 2021. The Task Force will produce an initial report due October 5, 2021, and a final report that is due on December 5, 2021.

Stakeholders and subject matter experts from Kansas and across the nation have 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.

Subcommittees

Strategic Vision and Planning

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

Statewide Coordination and Collaboration

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

Cyber Incident and Disruption Response

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

Workforce Development and Education

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

Bi-Weekly Task Force Meetings

The full Task Force held four (4) 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 National Governors Association on "National Landscape of Cyber Governance and Strategies"	8/10/2021
Organizational Cybersecurity Capabilities Presentations from, The Kansas Bureau of Investigation, KSU Center for Information and Systems Assurance, City of Wichita, Kansas Division of Emergency Management, 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 initial report.	9/29/2021

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 national Governors Association "NGA Policy Academy to Advance Whole-of-State Cybersecurity"	9/8/2021
Recommendation Discussion	9/22/2021
Statewide Coordination and Collaboration	
Introduction to the subcommittee and its goal. Presentation from National Association of State Chief Information Officers "Statewide Cybersecurity Coordination and Collaboration "	8/27/2021
Presentations from KANREN, Kansas Board of Regents, and Wichita State University	9/10/2021
Presentations from Kansas Association of Counties and League of Kansas Municipalities	9/24/2021
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
Recommendation Discussion	9/10/2021
Presentation from DHS Region 7 Cybersecurity Coordinator	9/24/2021
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 National Governors Association "Workforce Development"	9/8/2021
Recommendation Deep Dive	9/22/2021

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, to providing citizen services, and everything in-between. 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 cyber criminals and nation states. Cybersecurity has become a major business risk to organizations and Kansas citizens.

In recent years, we have seen cyberattacks devastate organizations worldwide. In 2017, we saw the destructive NotPetya cyberattack cause an estimated $10 Billion in damages[1]. We have seen 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, we have seen numerous data breaches that have led to the theft of hundreds of millions of records of personally identifiable information. There have 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 (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[2]. While this represents significant positive progress to close the gap, a major gap still remains. Public sector organizations have trouble competing with the private sector for these valuable and scarce resources.

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.

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

RECOMMENDATIONS

The cybersecurity landscape is very dynamic, and the Governor is seeking actionable recommendations to approach cybersecurity in Kansas with a "whole of state" approach. The Task Force approached this by breaking recommendations into categories based on time to implement. Recommendations will be categorized as either near term recommendations (within six (6) months) or long-term recommendations (longer than six (6) months) for implementation. The Task Force also attempted to identify the resources needed to implement recommendations.

The recommendations outlined below are the Task Force's initial recommendations for the interim report. Many of these recommendations may be further developed and refined by the Task Force and subcommittees for the final report. The final report is due to the Governor on December 5, 2021. Efforts will be made to identify potential resources and potential funding mechanisms to help with implementation. In addition, there is still much to learn from various stakeholders as well as other areas to investigate for recommendations to advance whole-of-state of cybersecurity within Kansas.

NEAR-TERM

Common Recommendations

The following are common near-term recommendations that came out of multiple subcommittees:

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

CR. N1 | STATE/AGENCY

Having a multi-vendor master cybersecurity contract that covers cybersecurity services and cybersecurity solutions and tools has multiple benefits. By consolidating these into a master contract, it allows organizations to quickly and easily locate needed cybersecurity services and solutions, it reduces the RFP effort by only needing to release one RFP and allows for a resource that can be readily compiled and shared to organizations. In addition, the State of Kansas is able to 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 are open to political subdivisions.

CR. N2 | STATE/AGENCY

Opening all state cybersecurity contracts 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 subdivision, 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. Provide awareness and a list of vendors to private industry partners.

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

CR. N3 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFRASTRUCTURE

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.

Begin building and establishing formal relationships with local governments, K-12, regent's institutions, critical infrastructure and other partners.

CR. N4 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFRASTRUCTURE

Building and establishing formal relationships and networking avenues with various stakeholders is imperative for success of a whole-of-state approach. Relationships allow for open communication and flow of information.

Strategic Vision and Planning

The following are near-term recommendations related to Strategic Vision and Planning:

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

SVP. N1 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFRASTRUCTURE

There are many services and tools that all organizations could leverage to enhance their cybersecurity posture such as security and vulnerability assessments. Organizations could procure these individually at a higher rate or procure multiple assessments 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.

Identify a short-term cybersecurity governance model to continue the work of this taskforce

SVP. N2 | STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE, EDUCATION

Continue the Task Force for 1-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. (see appendix A)

Statewide Coordination and Collaboration

The following are near-term recommendations related to Statewide Coordination and Collaboration:

Explore the use of grant funding to 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.

SCC. N1 | 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. A long-term solution to funding this role will need to be identified.

Hold an annual cybersecurity conference for public and private partners.

SCC. N2 | STATE/AGENCY

By holding an annual cybersecurity conference, stakeholders are given a platform to network, share experiences, learn best practices and build relationships with other stakeholders and peers.

Develop model cybersecurity and information security contract language that can be modified as needed and is incorporated in information technology contracts or contracts that involve organizational data.

SCC. N3 | STATE/AGENCY

Many organizations are heavily reliant on vendors and contractors to help manage or deliver IT services and solutions. Many organizations would benefit from having customer centric contract language that ensures data and IT services meet a certain level of cybersecurity requirements and ensures due care and due diligence by those vendors and contractors.

Create a catalogue of state contracts and services that can be shared with political subdivisions and ensure that it is readily available and communicated.

SCC. N4 | STATE/AGENCY

Developing a catalogue of state contracts and services that are available to political subdivisions can provide easy reference to available cybersecurity services. This can save those political subdivisions valuable time in trying to locate cybersecurity contracts and services.

Identify an individual or group to specifically address cybersecurity grants.

SCC. N5 | STATE/AGENCY

An individual needs to be hired or appointed to specifically address cybersecurity grants. An individual focused on helping organizations identify and apply for cybersecurity grant opportunities such as the Homeland Security Grant Program. This position can also properly vet applications to ensure they meet the cybersecurity requirements of various grants. This position would also be responsible for communicating out the cybersecurity grant opportunities to various stakeholders.

Cyber Incident and Disruption Response

Based on this information, the following are near-term recommendations related to Cyber Incident and Disruption Response and can be thought of as the who, how and where:

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

CIDR. N1 | STATE/AGENCY, LOCAL

Cyber incidents require specialized skillsets for effective response. Additional stakeholders that have not traditionally been involved in emergency management and response will need to be identified and included.

Identify and assign the appropriate roles and associated responsibilities to be filled by stakeholders in a cyber incident and disruption response plan.

CIDR. N2 | STATE/AGENCY

Identifying and assigning the appropriate roles and responsibilities of stakeholders during a cyber incident ensures a strategic communication and chain-of-command response is followed to minimize confusion and overlap of efforts.

A cyber incident and disruption response plan should exist and be maintained as part of an annex in the current State of Kansas response plan.

CIDR. N3 | STATE/AGENCY

The Kansas emergency management and response framework has multiple avenues where they can place a statewide cyber incident and disruption response plan, with the recommendation being that it be developed as part of an annex to the response plan. Inserting the plan as an annex into existing framework and structures to ensure that it is properly maintained, exercised, and communicated is critical to its success. The incident and disruption response plan takes effect when an incident reaches the level that requires a declaration of emergency by the Governor, or an incident is beyond the capacity of the impacted entity to handle.

Workforce Development and Education

The following are near-term recommendations related to Workforce Development and Education:

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

WDE. N1 | STATE/AGENCY, LOCAL, EDUCATION, PUBLIC AND 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, educational resources and programs offered, 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.

Establish partnerships with regent's institutions to begin developing a talent pipeline through work-based learning opportunities.

WDE. N2 | STATE/AGENCY, LOCAL, EDUCATION

Many of the regent's institutions in Kansas have both computer science programs or 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 prior to entering the workforce.

Explore remote work options to attract new talent to job openings.

WDE. N3 | STATE/AGENCY, LOCAL, EDUCATION

By allowing remote and telework positions for cybersecurity jobs, a larger talent pool can be leveraged. In addition, this would allow for these high paying jobs to potentially be located in more rural areas spurring additional economic impact in those communities. This work could require a culture shift to support and promote remote work as well as a review of job descriptions and requirements at the state and local level to identify what roles can function remotely.

Utilize the Learning Management System to train staff on the most current IT and cybersecurity practices.

WDE. N4 | STATE/AGENCY

Set up customized IT training tracks for current staff using the Learning Management System that will be rolled out across all Executive Branch agencies in the near future. IT training tracks will be customized based on roles and responsibilities of employees. For example, executive level employees would receive different training than individuals who are end users.

LONG-TERM

Common Recommendations

The following are common recommendations that came out of multiple subcommittees:

Establish a process to continuously assess the landscape of the State to determine the needs of the various organizations through gaps or risk assessments and identify solutions or ways to address those needs and gaps through collaboration.

CR. L1 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFASTRUCTURE

The cybersecurity landscape is constantly changing and evolving. Long term efforts need to be made to continuously assess the changing landscape for risks and gaps. By identifying the risks and gaps, steps can be taken to close or remediate those gaps. In addition, this action will also allow for identifying needed resources and capabilities.

Strategic Vision and Planning

The following are long-term recommendations related to Strategic Vision and Planning:

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

SVP. L1 | STATE/AGENCY, LEGISLATIVE, LOCAL, EDUCATION, CRITICAL INFASTRUCTURE

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 CITO/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. *(See appendix A, In coordination with SVP. L2, L3)*

Strategy and Governance must establish ownership, accountability, and funding for each strategy and goal.

SVP. L2 | STATE/AGENCY, LEGISLATIVE, LOCAL, EDUCATION, CRITICAL INFASTRUCTURE

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. *(In coordination with SVP. L1)*

Develop outreach effort to work with critical infrastructure and localities that consists of standard and consistent communication.

SVP. L3 | STATE/AGENCY, LOCALITIES, CRITICAL INFRASTRUCTURE, EDUCATION, PRIVATE SECTOR

Critical infrastructure organizations and localities provide critical services to citizens and the State of Kansas. It is in the best interest of the State of Kansas to proactively engage them, early and often, when it involves cybersecurity matters. Many partners from multiple sectors can bring valuable cybersecurity expertise to the conversation and continuing partnership. Establishing and maintaining these

partnerships are essential to sharing of cybersecurity education and information. To develop a successful outreach effort, may require additional staff with the funding to support it. *(In coordination with SVP. L1)*

Statewide Coordination and Collaboration

The following are long-term recommendations related to Statewide Coordination and Collaboration:

Partner alongside organizations like League of Municipalities, Association of Counties, KanREN, and others to utilize their communication networks to reach broader audiences to raise cybersecurity awareness, raise awareness of the cybersecurity resources and services the State has to provide, and build rapport and increase trust with cities and counties. A more extensive list of potential partner organizations will continue to be built upon and included in a future annex.

SCC. L1 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFASTRUCTURE

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.

Build a continuous education campaign to raise awareness that cybersecurity is a business risk to the continuity of government.

SCC. L2 | STATE/AGENCY

Cybersecurity issues affect more than just information technology. Cybersecurity attacks disrupt daily business operations which in turn impacts citizens. Continuing to raise the awareness on the impacts of cyberattacks can prioritize cybersecurity efforts.

Build a continuous education campaign to share and promote best practices that come out from the federal government such as leveraging .gov domains.

SCC. L3 | STATE/AGENCY, LOCAL

The federal government regularly publishes recommendations to assist all levels of government. Efforts should be taken to ensure further dissemination and awareness of those recommendations to the various partners throughout the state.

Explore ways to encourage local government employees to take cybersecurity awareness training and make the training resources available to the education and private sectors.

SCC. L4 | STATE/AGENCY, LEGISLATIVE, LOCAL

Disruptive cyberattacks have impacted all levels of government. 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. Provide education to the private sector on available resources to assist with training their employees.

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.

SCC. L5 | 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 engineer. This could also include cybersecurity awareness training being recognized as a continuing education credit.

Cyber Incident and Disruption Response

The following are long-term recommendations related to Cyber incident and Disruption Response:

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

CIDR. L1 | 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 are mechanisms for annually testing and exercising any cyber incident and disruption response plan with partners throughout the state.

CIDR. L2 | 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. Cybersecurity and Infrastructure Security Agency (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 all cyber incident reporting to the State has protection mechanisms to maintain confidentiality and not hinder response.

CIDR. L3 | STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE, LEGISLATIVE

To encourage reporting 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 if they feel they may be made public. This may require a review of current policies around information sharing.

Create and message a cyber triage intake process or central notification system for communication of cyber incidents.

CIDR. L4 | STATE/AGENCY, LOCAL, CRITICAL INFRASTRUCTURE

In the event of an incident, cities, counties, 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.

Ensure that there is a continuous education component around the cyber incident and disruption response plan.

CIDR. L5 | STATE/AGENCY, LOCAL, 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. 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.

Establish a framework such as Memorandums of Understanding (MOU) and Statement of Work (SOW) templates in advance to remove initial barriers and reduce risk to the Governor in directing state resources such as the National Guard, Emergency Management or others cybersecurity resources to an incident.

CIDR. L6 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFRASTRUCTURE

By establishing agreements between organizations ahead of time, this allows organizations to respond quicker to cybersecurity incidents and not have to wait for agreements to be drafted from scratch. It also allows the participating organizations to clearly understand roles and responsibilities in supporting those incidents.

Create a communication model (entities to contact when an incident occurs) or predefined role-based incident response plans based on the potential scope, roles, and responsibilities in those plans.

CIDR. L7 | STATE/AGENCY, LOCAL, EDUCATION, CRITICAL INFRASTRUCTURE

To encourage reporting and communication, a communication model should be developed that identifies who an entity can contact for assistance during a cybersecurity incident. The model can also include details on other partners to contact depending on the type of incident. Based on the interconnectivity between public entities, the importance of reporting incidents to the state should be heavily communicated.

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 other public entities, critical infrastructure and education as needed.

CIDR. L8 | 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 network. By creating language to protect them from liability, organizations will be able to provide additional support more openly to other entities.

Workforce Development and Education

The following are long-term recommendations related to Workforce Development and Education:

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

WDE. L1 | STATE/AGENCY, LOCAL, EDUCATION

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.

Identify state and regional opportunities where the State can create engagements and find alignment around cybersecurity.

WDE. L2 | LOCAL, STATE/AGENCY, EDUCATION

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.

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

WDE. L3 | STATE/AGENCY, LOCAL, EDUCATION

The scholarship for service program pays for an individual's degree while requiring them to complete government service once they graduate for a certain number of years. A whole-of-state specific approach that requires individuals to work for state, county, or city government could help fill some of the existing staffing shortages especially in rural and underserved areas

Establish public to private pathways with salaries where it makes sense.

WDE. L4 | STATE/AGENCY, LOCAL, EDUCATION

In many cases, the private sector can out pay the public sector for cybersecurity resources. Developing a public to private partnership where private industry shares qualified entry level employees with public sector organizations at the State, county, and city level gives the employee experience for several years. The private industry partners will then be able to bring the seasoned employee over to the private sector after a couple of years in the public sector. This model allows the public sector to leverage additional human capital that it may not normally have access to.

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

WDE. L5 | STATE/AGENCY, LOCAL, 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.

Using the National Institute Standards and Technology NICE framework (cybersecurity workforce framework), work with the private sector to compartmentalize work with right job titles and descriptions.

WDE. L6 | STATE/AGENCY, LOCAL, 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 cybersecurity position roles and descriptions to the NICE framework enhances hiring and recruiting, developing career progression paths for employees, and developing education and certification paths. Reclassify and align current job responsibilities and align from a salary standpoint where able.

Develop work-based learning opportunities through public and private partners for continued learning and training of staff.

WDE. L7 | STATE/AGENCY, LOCAL, EDUCATION, PRIVATE

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 for employees to continue their learning and development.

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

WDE. L8 | STATE/AGENCY, LOCAL, 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.

Develop and support efforts to incorporate and boost teacher training and retention efforts for K-12 teachers who are teaching computer science or cybersecurity concepts.

WDE. L9 | STATE/AGENCY, LOCAL, 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.

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

WDE. L10 | LOCAL, STATE/AGENCY, 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.

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 cyber-attacks 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 cyber-attacks on critical infrastructure;

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

WHEREAS, cyber-attacks 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 cyber-attacks 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 cyber security 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.

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 on-going 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.

TASK FORCE MEETING AGENDAS

CYBERSECURITY TASK FORCE

Tuesday, August 10
9:00-11:30 a.m.
Recorded Meeting

Agenda

9:00 a.m.	Opening Remarks
	Welcome Remarks – Governor Laura Kelly
	Members and Introductions
	Task Force Overview
	National Governor's Association (NGA) Overview – John Guerriero
	State of Kansas – What's happening in Kansas related to Cybersecurity
	Subcommittee Overview
	Closing Remarks
11:30 a.m.	Conclude

Wednesday, September 1
10:00-12:00 p.m.
Recorded Meeting

Agenda

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

Wednesday, September 15
10:00-12:00 p.m.
Meeting Recorded

Agenda

10:00 am	Opening Remarks and Introduction of Accenture (Jeff)
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	Subcommittee Activities and Interim Report Structure (Jeff)
11:45 am	Next Steps (Jeff)
12:00 pm	Conclude

CYBERSECURITY TASK FORCE

Wednesday, September 29
9:00 a.m. – 1:00 p.m.
Meeting Recorded

Agenda

9:00 a.m.	**Opening Remarks and Framing**
9:15 a.m.	**Recommendations Discussion**
10:00 a.m.	**Break**
10:10 a.m.	**Recommendations Discussion**
10:55 a.m.	**Break**
11:05 a.m.	**Recommendations Discussion**
11:50 a.m.	**Break**
12:00 p.m.	**Recommendations Discussion**
12:45 p.m.	**Final Comments, Next Steps (Jeff and Mike)**
1:00 p.m.	**Conclude**

STRATEGIC VISION AND PLANNING SUBCOMITTE MEETING AGENDAS

STRATEGIC VISION AND PLANNING SUBCOMMITTEE

Wednesday, August 25
3:00 p.m.-5:00 p.m.
Recorded Meeting

Agenda

3:00 p.m. **Opening Remarks & Introductions *(John Berghuis)***

3:10 p.m.: **Speaker Jeff Maxon**

3:30 p.m.: **Open Discussion *(Subcommittee Members)***

4:30 p.m. **Additional Resources *(John Berghuis)***

5:00 p.m. **Adjourn**

Kansas Cybersecurity Task Force

STRATEGIC VISION & PLANNING SUBCOMMITTEE

Wednesday, September 8
3:00 p.m.-5:00 p.m.
Recorded Meeting

Agenda

3:00 p.m. **Opening Remarks & Recap of Previous Meeting *(John Berghuis)***

3:10 p.m.: **Speaker *(John Guerriero, National Governors Association)***

3:35 p.m.: **Recommendations Discussion *(Subcommittee Members)***

- Review of Strategy Statements, Goals, and Objectives
- Draft recommendations

5:00 p.m. **Adjourn**

Kansas Cybersecurity Task Force

STRATEGIC VISION & PLANNING SUBCOMMITTEE

Wednesday, September 22
3:00 p.m.-5:00 p.m.
Recorded Meeting

Agenda

3:00 p.m. **Recommendations Discussion**

5:00 p.m. **Adjourn**

STATEWIDE COORDINATION AND COLLABORATION SUBCOMITTE MEETING AGENDAS

Kansas Cybersecurity Task Force

STATEWIDE COORDINATION & COLLABORATION SUBCOMMITTEE

Friday, August 27
10:00 a.m.-12:00 p.m.
Recorded Meeting

Agenda

10:00 a.m. **Opening Remarks & Introductions *(John Godfrey)***

10:10 a.m.: **Speaker *(Doug Robinson, NASCIO)***

- Overview and Q&A

10:40 a.m.: **Open Discussion *(John Godfrey)***

11:40 a.m. **Resources *(John Godfrey)***

12:00 p.m. **Adjourn**

STATEWIDE COORDINATION & COLLABORATION SUBCOMMITTEE

Friday, September 10
10:00 a.m.-12:00 p.m.
Recorded Meeting

Agenda

10:00 a.m. **Opening Remarks & Recap of Previous Meeting *(John Godfrey)***

10:05 a.m. **Presenter *(Cort Buffington, Executive Director, KANREN)***
- Q&A to follow

10:30 a.m. **Recommendations Discussion**

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

11:25 a.m. **Recommendations Discussion Cont.**

12:00 p.m. **Adjourn**

Kansas Cybersecurity Task Force

STATEWIDE COORDINATION & COLLABORATION SUBCOMMITTEE

Friday, September 24
10:00 a.m.-12:00 p.m.
Virtual Meeting Recorded

Agenda

10:00 a.m. **Opening & Introductions**

- We have two speakers joining us today
  - Erik Sartorius, Executive Director, The League of Kansas Municipalities
  - Bruce Chladny, Executive Director, Kansas Association of Counties

10:10 a.m. **Speaker *(Erik Sartorius, LKM)***

- Overview and Q&A

10:30 a.m. **Speaker *(Bruce Chladny, KAC)***

- Overview and Q&A

10:50 a.m. **Recommendations Discussion**

12:00 p.m. **Adjourn**

CYBER INCIDENT AND DISRUPTION RESPONSE SUBCOMITTE MEETING AGENDAS

Kansas Cybersecurity Task Force

CYBER INCIDENT & DISRUPTION RESPONSE SUBCOMMITTEE

Friday, August 27
9:00 a.m.-11:00 a.m.
Meeting Recorded

Agenda

9:00 a.m. **Opening Remarks & Introductions *(Charles King)***

9:10 a.m.: **Speaker *(Doug Robinson, NASCIO)***

- Overview and Q&A

9:40 a.m.: **Open Discussion *(Charles King)***

10:40 a.m. **Resources *(Charles King)***

11:00 a.m. **Adjourn**

Kansas Cybersecurity Task Force

CYBER INCIDENT & DISRUPTION RESPONSE SUBCOMMITTEE

Friday, September 10
9:00 a.m.-11:00 a.m.
Meeting Recorded

Agenda

9:00 a.m. **Opening Remarks & Introductions *(Charles King)***

9:10 a.m.: **Overview of Draft Response and Model, Recommendations Discussion**

11:00 a.m. **Adjourn**

Kansas Cybersecurity Task Force

CYBER INCIDENT & DISRUPTION RESPONSE SUBCOMMITTEE

Friday, September 24
9:00 a.m.-11:00 a.m.
Meeting Recorded

Agenda

9:00 am	**Introduction (Charles King)**
9:05 am	**Guest Speaker (Geoff Jenista, Cybersecurity and Infrastructure Security Agency)**
9:30 a.m.	**Open Discussion on Draft Proposal and Recommendations**
11:00 a.m.	**Adjourn**

WORK FORCE DEVELOPMENT AND EDUCATION SUBCOMITTEE MEETING AGENDAS

Kansas Cybersecurity Task Force

WORKFORCE DEVELOPMENT & EDUCATION SUBCOMMITTEE

Wednesday, August 25
10:00 a.m.-12:00 p.m.
Recorded Meeting

Agenda

10:00 a.m. **Opening Remarks & Subcommittee Goal *(Secretary DeAngela Burns-Wallace)***

- Introduction of Meredith Ward, NASCIO

10:10 a.m.: **Workforce Development Overview *(Meredith Ward)***

- Q&A throughout and to follow the presentation

10:30 a.m.: **Open Discussion *(Secretary DeAngela Burns-Wallace)***

11:30 a.m. **Resources *(Secretary DeAngela Burns-Wallace)***

12:00 p.m. **Adjourn**

WORKFORCE DEVELOPMENT & EDUCATION SUBCOMMITTEE

Wednesday, September 8
10:00 a.m.-12:00 p.m.
Recorded Meeting

Agenda

10:00 a.m. **Opening Remarks & Brief Recap of Previous Meeting *(Secretary Burns-Wallace)***

10:15 a.m.: **Workforce Development *(John Guerriero, NGA)***

- Q&A to follow

10:35 a.m.: **Recommendations Discussion *(Secretary DeAngela Burns-Wallace)***

12:00 p.m. **Adjourn**

WORKFORCE DEVELOPMENT & EDUCATION SUBCOMMITTEE

Wednesday, September 22
10:00 a.m.-12:00 p.m.
Recorded Meeting

Agenda

10:00 a.m. **Opening Remarks & Framing *(Secretary Burns-Wallace)***

10:10 a.m.: **Recommendations Deep Dive *(Secretary Burns-Wallace)***

12:00 p.m. **Adjourn**