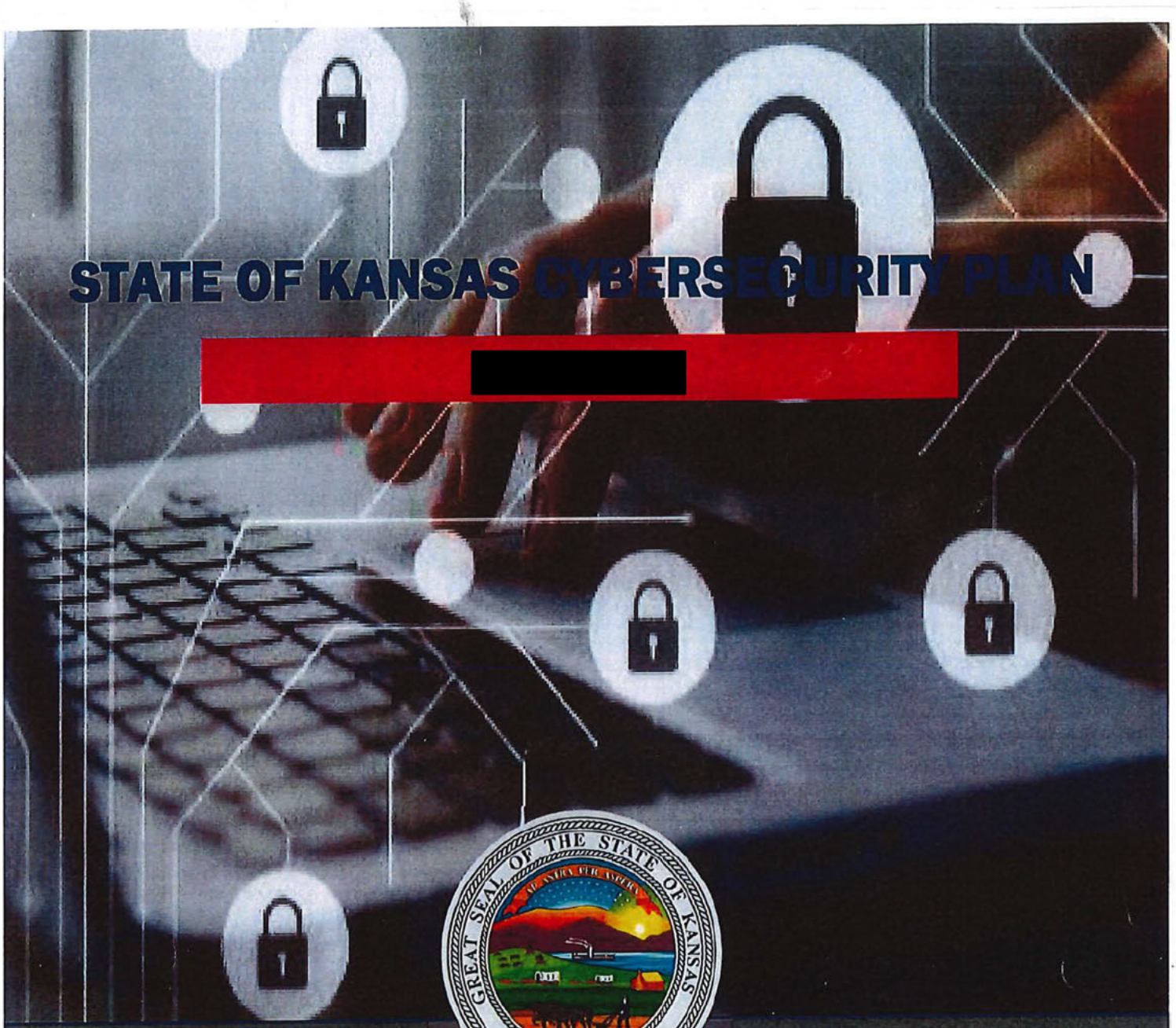


STATE OF KANSAS CYBERSECURITY PLAN

[redacted]

SEPTEMBER 2023

Approved by Kansas Cybersecurity Planning Committee,

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM KANSAS CYBERSECURITY PLANNING COMMITTEE

Greetings,

The Cybersecurity Planning Committee for the State of Kansas is pleased to present to you the 2023 Kansas Cybersecurity Plan. The Cybersecurity Plan represents the deep and continued commitment of the State of Kansas to improving cybersecurity and support our whole-of-state approach to cybersecurity with the cities, counties, public schools, public hospitals, and public utilities.

Representatives from Kansas' state, cities, counties, schools, health care and public utilities collaborated on this effort. Together, we developed, reviewed, and approved the Cybersecurity Plan with actionable and measurable goals and objectives.

With the understanding that we in Kansas are only as strong as our weakest link, these goals and objectives are primarily focused on our small and rural communities that are the most vulnerable sector of the state's cybersecurity environment and are vital partners in the protection of Kansas resources and infrastructure. Our goals and objectives incorporate the State and Local Cybersecurity Grant Program's (SLCGP) required plan elements.

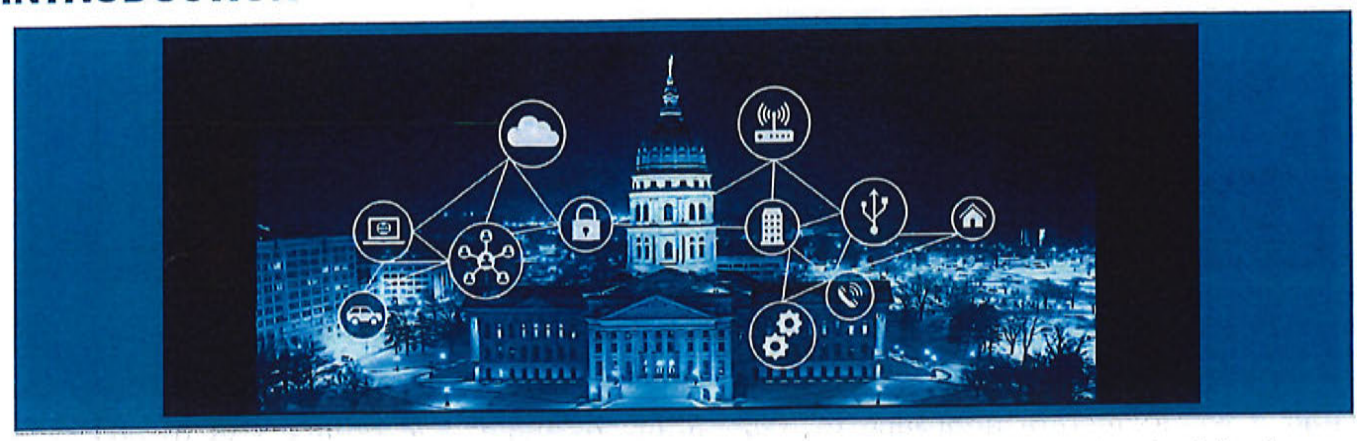
As part of our continuous journey towards enhanced IT and cybersecurity capabilities across the State of Kansas, we will remain dedicated to information sharing and collaboration with all stakeholders as we build a more resilient and protected cyber community to serve the citizens of the State of Kansas. Kansas will work to achieve the goals set forth in the Cybersecurity Plan to become a model for cyber resilience.

Sincerely,

Jeff Maxon
State of Kansas CISO
Office of Information Technology Services

Brenda Ternes
IT Director, City of Newton, KS
President Elect GMIS

INTRODUCTION



The Kansas Cybersecurity Plan is a three-year strategic planning document that contains the following components:

- **Vision and Mission:** Articulates the vision and mission for improving cybersecurity resilience and interoperability across the State of Kansas over the next three years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within the State of Kansas as well as successes, challenges, and priorities for improvement. The plan also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program will be supported. In addition, this section includes our governance approach that identifies authorities for, and requirements of, the State of Kansas cybersecurity program. This Cybersecurity Plan is a guiding document and does not create any authority or direction over any of the state or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** Describes how we engaged and received input from local governments about their current cybersecurity posture, gaps, with best cyber practices, and most pressing needs to reduce overall cybersecurity risk across Kansas. This is especially important in order for us to develop a holistic cybersecurity plan that meets the needs of our most vulnerable stakeholder entities.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across Kansas' cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within the State of Kansas along with methods and strategies for sustaining and further enhancing funding to meet our State's long-term cybersecurity goals.
- **Implementation Plan:** Describes the State of Kansas' plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward our identified goals. The implementation plan includes the resources and timeline where practicable.
- **Metrics:** Describes how the state will measure the outputs and outcomes of the program across the entities.

Vision and Mission

Vision:

A secure and resilient cybersecurity and information technology infrastructure for the Citizens of the State of Kansas.

Mission:

Lead a whole-of-state approach to understand, manage, and reduce risk to all public cybersecurity and information technology infrastructures, where all public entities are capable of identifying, detecting, protecting, mitigating, responding to, and recovering from, cybersecurity and technology threats and attacks.

Cybersecurity Program Goals and Objectives

The State of Kansas Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. Cyber Defense: Create and maintain a whole-of-state effort to ensure defense and resiliency of cybersecurity/technology at all levels of public entities.	1.1 Assist public entities with education and support on transitioning to a .gov environment. 1.2 Assist public entities with implementing proper cyber hygiene. 1.3 Assisting public entities with protecting operational technology.
2. Risk reduction and resilience: Reduce risk to and strengthen the resilience of Kansas public sector IT/cybersecurity infrastructure.	2.1 Increase Cybersecurity awareness for all public entities. 2.2 Educate public entity leadership on risk reduction and resiliency. 2.3 Assist public entities with education and implementation of Technology/Cyber Resiliency Planning.
3. Operational Collaboration: Strengthen a whole-of-state operational/technical collaboration and information sharing.	3.1 Provide for information sharing amongst all public entities. 3.2 Promote awareness of available resources.
4. Governance: Encouraging all leadership to actively support, foster, and manage an environment of cybersecurity awareness, engagement, and compliance.	4.1 Educate public entity leadership on proper Cybersecurity/IT Governance. 4.2 Assist public entities leadership with creation and implementation of Cybersecurity Governance.

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track

All public entities should be utilizing best practices as defined by the state and federal guidelines for cybersecurity. Each entity should be setting through policy and procedure, the mandates to utilize proper backups, proper cyber hygiene, conduct security trainings, and have the tools necessary for monitoring systems health and intrusion detection.

Monitor, Audit, and Track

All public entities should:

- utilize or deploy means to monitor and audit the systems for malicious intrusions.
- utilize free or discounted service to assist in the auditing, tracking, and monitoring of traffic within their systems.
- continue to collaborate with CISA, MS-ISAC, and Kansas Information Security Office (KISO).

The state aims to lift the current capability level in this area from Foundational to Functional over the ensuing three years.

Enhance Preparedness

All public entities should:

- communicate and coordinate with local emergency management.
- actively participate in the Local Emergency Planning Commissions.
- provide personnel into the Local Emergency Operations Center as an emergency support function.
- provide a cyber annex to the existing Local Emergency Operations Plan.
- participate in exercises and trainings with local entities as appropriate.

Assessment and Mitigation

All major systems, applications, and general support systems operated by or on behalf of public entities should undergo security assessments to ensure adequate security and privacy controls. Assessments shall be performed utilizing risk management processes based on best practices as identified by state and federal guidelines and standards, as applicable.

Best Practices and Methodologies

The state will continue to drive whole-of-state adoption of industry best practices and methodologies to enhance cybersecurity across all public entities regarding information security policies, standards, and procedures. Applicable security controls tailored to Kansas' current cyber maturity and as defined by NIST Special Publication (SP) 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, CISA Cybersecurity Performance Goals (CPG), and the newly updated NIST Cybersecurity Framework (CSF) 2.0 are being made available as a resource.

The Kansas Information Security Office continues to increase awareness of resources and promote adoption of best practices and methodologies by all public entities.

The following best practices should be considered for adoption:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit.

- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Prohibit use of known/fixed/default passwords and credentials.
- Ensure the ability to reconstitute systems (backups).
- Migration to the .gov internet domain.

NIST Principles

The State of Kansas will continue to promote awareness and adoption of NIST principles and practices across all public entities.

Supply Chain Risk Management

All public entities shall participate in proper procurement practices as outlined in 2 CFR. All public entities should vet all vendors/contractors ensuring that proper service level agreement language is included in the contracts. Kansas participates in the State Risk and Authorization Management Program (StateRAMP). StateRAMP provides shared vendor vetting and approval processes for public entities. Additionally, the State of Kansas is opening IT/Cybersecurity contracts to all political sub-divisions.

Tools and Tactics

The State of Kanas promotes engaging the MS-ISAC, CISA, and other partners and systems to gain access to knowledge bases of adversary tools and tactics to improve cybersecurity efforts.

Safe Online Services

The State of Kansas will promote the delivery of safe, recognizable, and trustworthy online services (including using the .gov internet domain), through continued outreach, education, and training.

Continuity of Operations (COOP)

Public entities are encouraged to participate in Continuity of Operations Planning with Local Emergency Managers to understand the business priorities of the public sector organizations they support. Public entities should utilize the business priorities set out in the COOP, to assist in the prioritization for restoration of systems included in their Technology/Cyber Resiliency Plan.

Workforce

KISO promotes and provides educational and training resources to existing state employees and public personnel. The training programs adhere to the NICE Framework and can be conducted in-person or virtually. Additionally, there are certification bootcamps available for IT personnel of the public entities to enhance their skills.

The state is encouraging the recruitment of retired information technology/cybersecurity employees who previously worked in the government, military/National Guard, or private sectors, into a public service. The state also encourages the use of interns by building relationships with tech/trade schools, colleges, high schools, and community colleges.

Continuity of Communications and Data Networks

The state provides training on the DHS GETS/WPS (Government Emergency Telecommunication Service/Wireless Priority Service) program. Additionally, the State of Kansas has a Statewide Interoperable Coordinator who has resources available to all public entities upon request through the Local Emergency Manager. The state also maintains contracts with cellular providers for emergency support for phone and data during disaster situations.

The State Interoperability Advisory Committee (SIAC) advises on the development and deployment of a centralized, interoperable-communications plan.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

The state will continue to partner with CISA Region 7 to create risk assessments based on national best practices to identify and mitigate, threats, hazards, and risks, relating to critical infrastructure.

Cyber Threat Indicator Information Sharing

The state encourages utilization of MS-ISAC, CISA, KBI, and the State Fusion Center for threat intelligence. The state also strongly encourages participation in other organizations that focus on sharing local risk and threat intelligence.

Department Agreements

The state will share threat intelligence in accordance with local and federal laws and regulations, and Kansas State Law "HB 2019."

Leverage CISA Services

The State of Kansas will continue to support, promote, and utilize CISA's cybersecurity risk and vulnerability services, especially the no cost MS-ISAC services such as Malicious Domain Blocking and Reporting (MDBR), Cyber Threat Intelligence (CTI), Real-Time Indicator Feeds, Malicious Code Analysis Platform (MCAP), water and wastewater treatment assessment, and the CIS SecureSuite membership for Access Control policies/procedures and Anti-Phishing training program support. All recipients and sub-recipients will be required to sign up for CISA's Cyber Hygiene Services and complete the MS-ISAC NCSR.

Due to the heavy demand and long wait list for these no cost services by CISA and MS-ISAC, the state will continue to provide vendor contracts open to any political sub-division for augmenting these services.

Kansas will continue to leverage its relationship with CISA Region 7 Liaison for cybersecurity-related activities, seminars, and outreach programs that will benefit public entities on a regular basis.

Information Technology and Operational Technology Modernization Review

As the whole-of-state plan is currently at a foundational level the current priority is standardization and implementation of best practices. The whole-of-state plan will utilize a "crawl, walk, run" approach and modernization will be addressed in future plans.

Cybersecurity Risk and Threat Strategies

The Kansas Information Security Office will continue to promote a whole-of-state approach to cybersecurity through outreach, education, coordination, and collaboration. These efforts involve all public entities, state agencies, and federal partners.

Rural Communities

Ninety-five (95) of Kansas' 105 counties are classified as rural – having a population of under 50,000. The Kansas Information Security Office (KISO) collaborates with the Kansas League of Municipalities (KLM), the Kansas Association of Counties (KAC), the Kansas Board of County Commissioners Association (KBCCA), and the Kansas GMIS (Government Management of Information Science). Additionally, the KISO has started a repository of all IT contacts for public entities, ensuring they receive notifications and invitations to participate in all events tied to the SLCGP.

FUNDING & SERVICES

The State of Kansas will absorb the required grant match responsibility to alleviate hardship and ensure all public entities across Kansas have an equal opportunity to actively participate in this grant program.

All threats, gaps, hazards, and needs identified in this plan will be addressed through projects approved by the Cybersecurity Planning Committee, CISA and FEMA. The approved projects must be sustainable and benefit the greatest number of public entities possible. The State strongly encourages all public entities to actively participate in low and no-cost programs available through CISA, FEMA, MS-ISAC, and DHS.

Distribution to Local Governments

The State of Kansas intends to use the SLCGP to fund projects and services in accordance with the published grant guidance of 80% benefiting local public entities.

ASSESS CAPABILITIES

In developing the cybersecurity plan elements, the state conducted outreach programs to our local jurisdictions over a three-week period by inviting representatives of cities, counties, schools, public hospitals, and public utilities to attend regional workshops. The capability assessment also included online surveys and virtual webinars to ensure input from the widest representation of all public entities. Constructive feedback and ideas were provided by stakeholders. Input received from our stakeholders formed the basis for our strategic decision to essentially allocate the entirety of our near term SLCGP funds toward providing critical security and basic IT services to our small and rural communities across the state.

During the course of the program, this plan will be revised and updated as necessary, including using input from our stakeholders.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

The State of Kansas, being a home rule state, has no central entity with overarching responsibilities over all local jurisdictions.

The State Cybersecurity Planning Committee was created by legislative authority through the Information Technology Executive Council (ITEC). It is chartered to be the State of Kansas, cybersecurity planning committee and cybersecurity governance body for the SLCGP. Membership is made up of the following committee members:

Cybersecurity Planning Committee	
Jeff Maxon	CISO/ Interim CITO, State of Kansas
Jonathan York	Response & Recovery Bureau Director, Kansas Division of Emergency Management, State of Kansas
Brenda Ternes	Director of IT, City of Newton, Kansas (VP GMIS International)
Rod Dickson	CIO, Kansas USD 259
Michael Leiker	Director of IT, Ellis County, Kansas (President GMIS International)
Alan Weis	CITO, Kansas Legislative Branch, State of Kansas
Kelly O'Brien	CITO, Kansas Judicial Branch, State of Kansas
Kevin Comstock	Director of IT, Secretary of States Office, State of Kansas
Lt. Col. Janet Dial	J6 CIO, Kansas Adjutant General's Office, State of Kansas
Jay Emler	CISO, Kansas Attorney General's Office, State of Kansas (former)
Jake Coffman	CISO, for University of Kansas
David Marshall	Director, Kansas Criminal Justice Information Systems Committee
Joe Mandala	CIO, Kansas Bureau of Investigation, State of Kansas
David Young	Deputy Homeland Security Advisor for Kansas and Directory for the Kansas Intelligence Fusion Center
Glen Yancy	Kansas Department of Health and Environment (*since retired*)

Coordination of cybersecurity activities across the state is being undertaken by the KISO. The initial approach has been focused on gaining the trust of these entities, especially the small and rural communities, through outreach programs.

Anticipated timeline for SLCGP Grant

Activity	Date
Submission of SLCGP Cybersecurity Plan	September 30, 2023
Plan Application Evaluation	October 2023
Anticipated CISA/FEMA approval of State of Kansas Cybersecurity Plan	November 2023
Provide project application guidance to all qualified entities	December 2023
Application acceptance period for FY 2022 SLCGP	January 2024-March 2024
Kansas FY 2022 Cybersecurity Projects internally formalized, submitted to Cybersecurity Planning Committee for approval.	April 2024
Selected approved plans presented to CISA/FEMA for approval and funding.	May 2024

METRICS

State of Kansas - Cybersecurity Plan Metrics			
Program Goals	Program Objectives	Associated Metrics	Metric Description (Details, source, frequency)
1. Cyber Defense	Assist public entities with education and support on transitioning to a .gov environment	Number of entities who have transitioned to use of the .gov environment.	• Source to be determined as part of supporting projects. • To be assessed not less than every year.
2. Cyber Defense	Assist public entities with implementing proper cyber hygiene.	Assessments, audits, scans, incidents, policies, and procedures.	• Source to be determined as part of supporting projects. • To be assessed not less than every year.
3. Cyber Defense	Assisting public entities with identifying, detecting, and protecting operational technology.	Assessments, audits, scans, policies, and procedures.	• Source to be determined as part of supporting projects. • To be assessed not less than every other year.
4. Risk and Resilience.	Increase Cybersecurity awareness for all public entities.	Number of delivered presentations, workshops, seminars, drills, tabletops, and trainings.	• Assessed quarterly.
5. Risk and Resilience	Educate public entity leadership on risk reduction and resiliency.	Number of delivered presentations, workshops, seminars, drills, tabletops, and trainings.	• Assessed quarterly
6. Risk and Resilience	Assist public entities with education and implementation of Technology/Cyber Resiliency Planning	Number of plans started, in process, updated or tested.	• Source to be determined as part of supporting projects. • To be assessed not less than every year.
7. Operational Collaboration	Provide for information sharing amongst all public entities.	Including but not restricted to: Number of groups, number of meeting attendees, website statistics, number of consultations.	• Source to be determined as part of supporting projects. • To be assessed not less than every year.
8. Operational Collaboration	Promote awareness of available resources.	Including but not restricted to: Number of presentations, workshops, seminars, webinars, website	• Source to be determined as part of supporting projects. • To be assessed not less than every year.

State of Kansas - Cybersecurity Plan Metrics			
Program Goals	Program Objectives	Associated Metrics	Metric Description (Details, source, frequency)
		statistics, and consultations.	
9. Governance	Educate public entity leadership on proper Cybersecurity/IT Governance.	Number of delivered presentations, workshops, seminars, drills, tabletops, and trainings.	• Source to be determined as part of supporting projects. • To be assessed not less than every year.
10. Governance	Assist public entities leadership with creation and implementation of Cybersecurity Governance.	Completed, started, or in process, policies and procedures; assessments, audits, and scans.	• Source to be determined as part of supporting projects. • To be assessed not less than every year.

APPENDIX C: ENTITY METRICS

The below table reflects the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (Details, source, frequency)**
1. The state of Kansas has an approved Cybersecurity Plan that meets the SLCGP requirements as defined in the NOFO.	1.1 Kansas Cybersecurity Planning Committee approves Cybersecurity Plan.	Cybersecurity Plan signed by CITO/CISO and local delegate.	Committee meeting minutes
	1.2 Submit Cybersecurity Plan to CISA/FEMA	Confirmation of receipt	Email from CISA/FEMA
	1.3 CISA/FEMA approves Cybersecurity Plan	Statement of Approval	Email from CISA/FEMA
2. Submit approved projects to CISA/FEMA for approval and funding.	2.1 Funding received to execute approved projects	Receipt of funds	Acceptance of funds
3. Execute life cycle process by SAA for each approved project	3.1 Execute approved projects	Projects are invoiced and paid	Financial reporting
	3.2 Closeout approved projects	Projects are terminated or renewed	Financial reporting
4. Process services to local entities	4.1 Enroll local entities in services	Number of entities enrolled for each approved project	Financial reporting
5. Review, revise, and update plan as necessary.	5.1 Reference above Program Goal 1	Reference above Program Goal 1	Reference above Program Goal 1

APPENDIX D: ACRONYMS

Acronym	Definition
BCDR	Business Continuity and Disaster Recovery
BIA	Business Impact Analysis
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CITO	Chief Information Technology Officer
COOP	Continuity of Operation Plan
CSF	Cybersecurity Framework
DHS	US Department of Homeland Security
DR	Disaster Recovery
EDR	Endpoint Detection and Response
FEMA	Federal Emergency Management Agency
FY	Fiscal Year
GETS/WPS	Government Emergency Telephone System/Wireless Priority Service
GMIS	Government Management Information Sciences
IT	Information Technology
ITEC	Information Technology Executive Council
KBI	Kansas Bureau of Investigation
KDEM	Kansas Department of Emergency Management
KISO	Kansas Information Security Office
KS-GMIS	Kansas Chapter of Government Management Information Science
LEOP	Local Emergency Operation Plan
MCAP	Malicious Code Analysis Platform
MDBR	Malicious Domain Blocking and Reporting
MOU	Memoranda of Understanding

Acronym	Definition
MS-ISAC	Multi-State Information Sharing and Analysis Center
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OT	Operational Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
SIAC	State Interoperability Advisory Committee
SIEM	Security Information and Event Management
SLCGP	State and Local Cybersecurity Grant Program
SOC	Security Operation Center
SP	Special Publication
StateRAMP	State Risk and Authorization Management Program
SWIC	State Interoperability Advisory Committee
TCRP	Technology and Cyber Resilience Planning
TTX	Tabletop Exercise