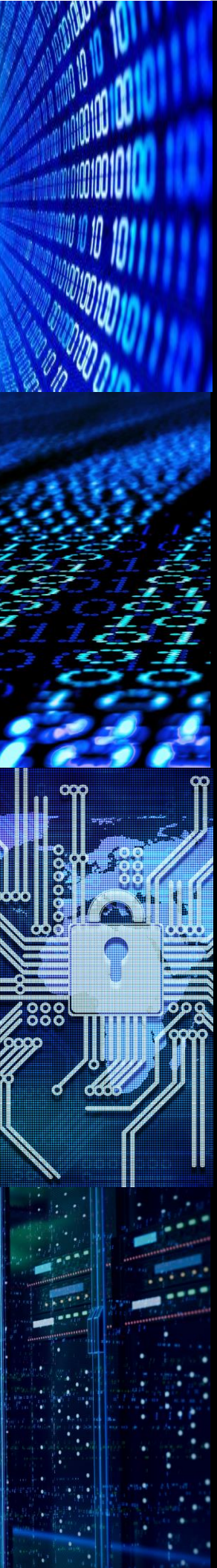

NEBRASKA STATEWIDE CYBERSECURITY PLAN

February 2023

Approved by Nebraska SLCG Cybersecurity Planning Committee on February 9th, 2023.
Approved by the State Chief Information Officer on February 10th, 2023
Version 1.0

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from Cybersecurity Planning Committee **2**
Introduction **2**
Vision and Mission 6
Cybersecurity Program Goals and Objectives 6
Cybersecurity Plan Elements **8**
Manage, Monitor, and Track 9
Monitor, Audit, and Track 9
Enhance Preparedness 9
Assessment and Mitigation 9
Best Practices and Methodologies 10
Safe Online Services 11
Continuity of Operations 11
Workforce 12
Continuity of Communications and Data Networks 12
Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources 12
Cyber Threat Indicator Information Sharing 12
Leverage CISA Services 13
Information Technology and Operational Technology Modernization Review 13
Cybersecurity Risk and Threat Strategies 13
Rural Communities 13
Funding & Services **13**
Distribution to Local Governments 14
Assess Capabilities **15**
Implementation Plan **15**
Organization, Roles and Responsibilities 15
Resource Overview and Timeline Summary 15
Metrics **16**
Appendix A: Project Summary Worksheet **21**
Appendix B: Acronyms **22**

NEBRASKA
Good Life. Great Vision.

OFFICE OF THE CIO

February 10th, 2023

IIJA Cybersecurity Planning Committee
501 S. 13th St.
Lincoln, NE 68508

RE: Letter Approving the Statewide Cybersecurity Plan

Dear IIJA Cybersecurity Planning Committee:

Thank you for participating in the Infrastructure Investment and Jobs Act (IIJA) Cybersecurity Planning Committee. I appreciate your thoughtful input and your continuing commitment to providing cybersecurity guidance that works to improve the public sector technology infrastructure for every Nebraskan through the IIJA grant process. The purpose of this memo is to document my approval of the Nebraska Statewide Cybersecurity Plan as drafted and prepared by the committee.

This plan proposes a building strategy that emphasizes fundamental cybersecurity principles. The plan adheres to established frameworks to make progress, year after year, toward promoting security best practices and reducing cyber risks to networks, systems, and data throughout Nebraska's State, Local, and Tribal governments, as well as public political subdivisions and critical infrastructure.

Sincerely,

Ed Toner
Chief Information Officer

Office of the Chief Information Officer
501 S. 14th Street, P.O. Box 95045
Lincoln, Nebraska 68509

cio.nebraska.gov

Ed Toner, Chief Information Officer
OFFICE 402-471-3560 FAX 402-471-4864
SERVICE DESK 800-982-2468

LETTER FROM CYBERSECURITY PLANNING COMMITTEE

Greetings,

The Cybersecurity Planning Committee for the State of Nebraska (Committee) is pleased to present the 2023 Nebraska Statewide Cybersecurity Plan. The Statewide Cybersecurity Plan represents Nebraska's continuing commitment to improving cybersecurity at the State, County, and Local levels. In addition, this update meets the requirement of current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the Nebraska Association of County Officials, The League of Municipalities, Nebraska Public Power District, Educational Service Unit Coordinating Council, University of Nebraska, Representation from Public Health Organizations, Nebraska Emergency Management and Emergency Management Departments from across the state of Nebraska, as well as the Nebraska National Guard and Office of the CIO have all collaborated to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have dedicated champions identified to ensure successful completion. These goals and objectives focus on the assessment of cybersecurity throughout the State, the identification of gaps in security, establishment of key governance topics, promotion of cybersecurity best practices, and exercise of the plan and capabilities. They are designed to support Nebraska in planning for new technologies and navigating the ever-changing cybersecurity landscape, while incorporating the SLCGP required plan elements.

As Nebraska continues to enhance its cybersecurity capabilities, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Sincerely,

Patrick Wright
State Information Security Officer
State of Nebraska
Cybersecurity Planning Committee Chairperson

INTRODUCTION

The proliferation of information and operational technologies throughout all facets of life, commerce, and government is expected to continue unabated for the foreseeable future. Advances in areas such as elastic cloud computing, artificial intelligence, big data, and network speeds have enabled government organizations to realize new and improved capabilities and provide services to the public that were inconceivable just a few years ago. The State of Nebraska is home to approximately 1,500 state and local government organizations, including counties, municipalities, K-12 schools, institutions of higher education and public health, three branches of state government, along with an array of political subdivisions. Each of these organizations is in some way connected to the others, as well as a broader global network of networks. This interconnectedness results in an interdependence where every entity is vulnerable to the actions or inactions of others.

Individuals, businesses, and governments that employ information and operational technologies are exposed to an increasingly dangerous threat landscape that provides opportunities for threat actors to maliciously target cyber infrastructure and information for foreign policy/national interests, or financial gain, to foment chaos and anarchy, to sow social division, and for other hostile motivations. Malicious acts conducted in support of such motivations may ultimately lead to the loss of mission-critical information and information systems, thereby threatening public safety, undermining public confidence, negatively affecting the economy, and diminishing the security posture of the State of Nebraska and, more broadly, the United States.

In the context of widespread deployment of increasingly complex and networked digital systems, growing cyber threats are outpacing societies' ability to effectively prevent and manage them. It is unrealistic to expect any one state or local government organization to have the resources and capabilities to unilaterally defend against nation-state actors, criminal syndicates, terrorist groups, hacktivists, and others who can launch cyberattacks from anywhere in the world at any time. A more effective approach from both a cost and resiliency perspective are to adopt a collective defense model in which organizations collaborate to detect, share intelligence about, and respond to threats together in real time. This Nebraska Statewide Cybersecurity Strategic Plan (the "Plan") focuses on improving the cybersecurity capabilities and reducing risk in state and local governments and presents Nebraska with opportunities to adopt a collective defense model. While this Plan focuses on reducing cyber risk in Nebraska's public-sector organizations, fully adopting a collective defense model requires robust collaboration with Federal, State, and Local government, private sector, and other applicable stakeholders.

Cyber incidents have no geographic boundaries; incidents impacting Nebraska public-sector organizations may have cascading effects across the State, the region, the nation, and the world. Conversely, cyber incidents initially impacting geographies outside Nebraska may have cascading effects that threaten or impact the State. Expanding and strengthening State and Local government partnerships with a broad array of key cybersecurity stakeholders ensures critical information is shared broadly and resources are coordinated across applicable sectors. The Federal government and private industry, in particular information technology and service providers that provide the backbone for communications networks, equipment, software, and information systems, play vital

roles in the success of Nebraska’s cybersecurity efforts. As such, the concept of a collective defense is central to Nebraska's cybersecurity resilience efforts and is referred to throughout this Plan. Incorporating a collective defense model into this Plan represents both a holistic and practical approach to reducing risk within and across Nebraska's State and Local government organizations.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, is based on existing standards, guidelines, and best practices for organizations to better manage and reduce cybersecurity risks across various levels of an organization from senior executives to the business and process level, as well as implementation and operations.

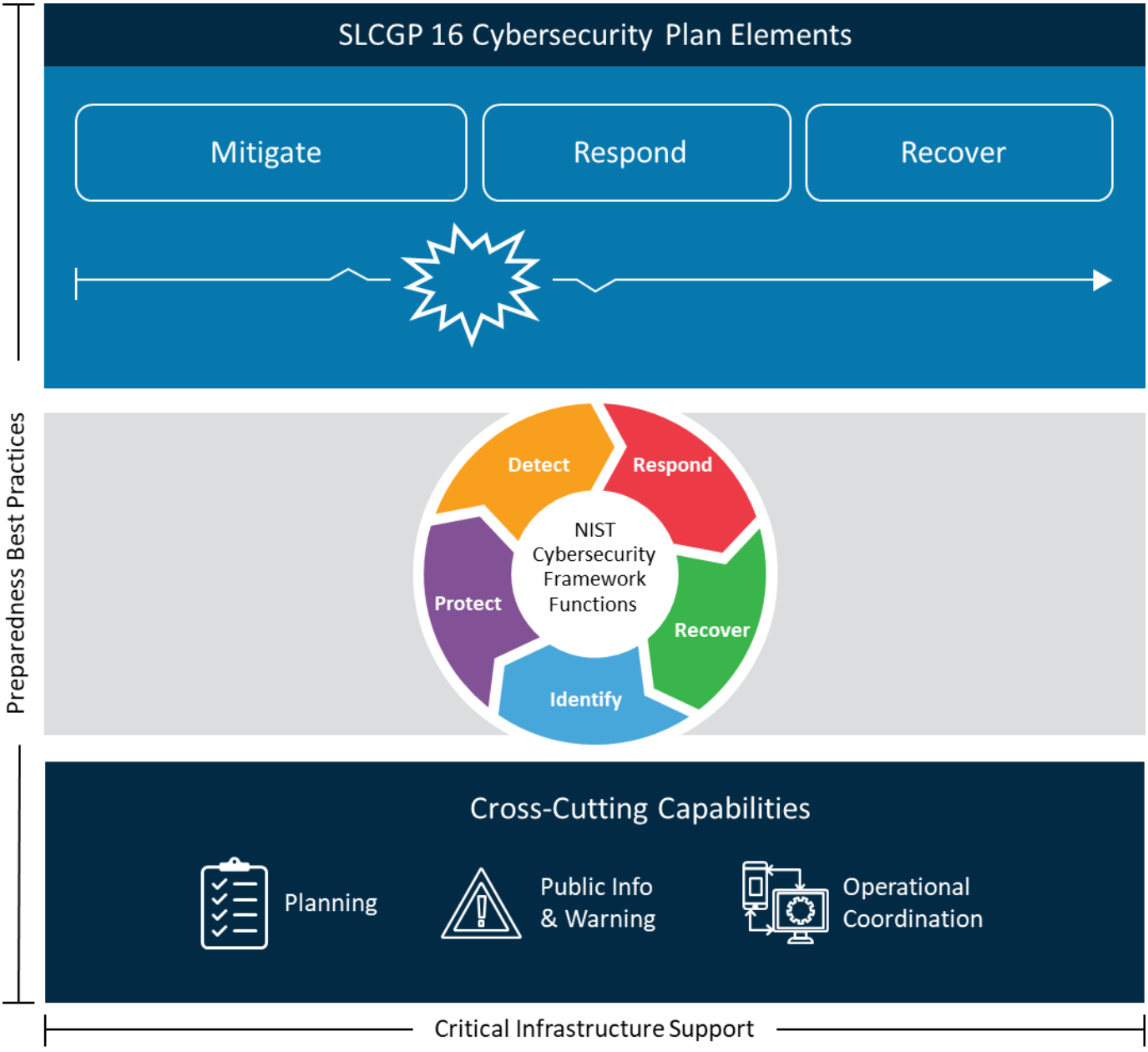

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

[1] https://www.nist.gov/cyberframework/getting-started

Vision and Mission

Vision:

To have an ongoing and mature cybersecurity program that continually reduces cyber risk exposure of entities throughout Nebraska.

Mission:

The mission of the Nebraska Cybersecurity Program is to promote security best practices, reduce cyber risks to networks, systems and data across Nebraska and to educate and protect organizations of the State.

Cybersecurity Program Goals and Objectives

The plan's overall objective is to reduce cyber risk while enhancing Nebraska's State and Local government cyber resilience. It is understood that different organizations may be at various levels of cybersecurity maturity. As a result of this, it is imperative to establish a baseline assessment of cyber capabilities throughout the State of Nebraska. With that goal in mind, each year will build on the previous by focusing on different aspects of the NIST Cybersecurity Framework to create a comprehensive implementation across the State of Nebraska.

Throughout the period of performance for the SLCGP, the following goals and objectives will be pursued, and their supporting action items will be performed to execute the plan fully. The goals, objectives, and action items are interrelated, such that performing the action items will allow the realization of their supported objectives, and achieving the objectives will allow for the realization of meeting the strategic goals and, ultimately, the plan's principal goal. Six principle goals are integrated within and across these objectives and action items, along with the 16 key elements set out in the SLCGP NOFO.

On an annual basis, the Committee will review and, if necessary, revise the plan to measure progress and ensure its goals, objectives, and action items effectively reduce risk in the face of an increasingly complex and hyperconnected threat landscape. Over the next three years, objectives include the following:

FY22 Identify and Protect (NIST SP 800-59, NIST SP 1800-5, NIST SP 800-55, NIST SP 800-53)

Cybersecurity Program		
Program Goal	**Program Objectives**	**Action Items**
1. Assessment of Cybersecurity Capabilities	1.1 Develop and conduct assessments to identify critical enterprise processes and assets, document information flows, identify and document hardware and software inventories.	Projects to discover assets on the network, either through automated or manual means, establish software and hardware inventories and record information data flows are projects and tasks.
	1.2 Review or establish policies for cybersecurity that include roles and responsibilities	1. Establish cybersecurity organizational policies, cyber incident response and disaster recovery plans within organizations. 2. Create templates for organizations to follow that currently have the expertise to follow the requirements of the created documentation.
	1.3 Identify threats, vulnerabilities, and risks to assets identified during assessments	Focus on individual organizational projects to conduct risk assessments, vulnerability scans, and penetration tests to identify vulnerabilities, threats and risks to the organizations.
2. Assessment of Protection Capabilities	2.1 Assess and manage access control measures to assets and information	Assessment of access controls to information and the implementation of least privilege.
	2.2 Assessment of measures to protect sensitive data	Projects to implement taxonomy of data and identify, improve, enhance measures to protect sensitive data.
	2.3 Assessment of device configuration, security controls, and vulnerabilities.	Individual organizational projects to test configuration of devices, security controls and vulnerabilities within organizational assets.
	2.4 End user training to determine cyber awareness capabilities	Implementation of programs to provide security awareness training to end users.

FY23 Detect and Respond Phase (NIST SP 800-137, NIST SP 800-34, NIST SP 800-30)

Cybersecurity Program		
Program Goal	**Program Objectives**	**Action Items**
1. Identify the occurrence of cybersecurity events	1.1 Development and assessment of detection methods, processes, and procedures	Individual projects that focus on identification and detection capabilities. (i.e. deployment of EDR solution)
	1.2 Development and assessment of logging practices and enhancement of logging	Individual projects that focus on procuring SIEM tools or enhancing logging capabilities.
	1.3 Map networks and data flows	Organizations should map their networks and data flows
	1.4 Cyber Risk Assessments	Utilizing information from the assessments, conduct risk and cyber risk assessments.
2. Increase Response Activities	2.1 Develop and test cyber incident response plans	Organizations should conduct tabletop exercises to test plans
	2.2 Stakeholder coordination	As part of development of an incident response plan or tabletop exercise, organizations should coordinate interaction with both internal and external stakeholders
	2.3 Best Practice Implementation	Individual organizational projects that focus on the implementation of best practices.

FY24 Recovery Phase NIST SP 800-184

Cybersecurity Program		
Program Goal	**Program Objectives**	**Action Items**
1. Recover Systems	1.1 Ensure the ability to reconstitute systems in the event of a cyber incident	Individual organizational projects that focus on increased backup and restoration capabilities.
	1.2 Development and assessment of logging practices and enhancement of logging	Individual projects that focus on procuring SIEM tools or enhancing logging capabilities.
	1.3 Map networks and data flows	Organizations should map their networks and data flows
2. Increase Response Activities	2.1 Develop and test cyber incident response plans	Organizations should conduct tabletop exercises to test plans
	2.2 Stakeholder coordination	As part of development of an incident response plan or tabletop exercise organizations should coordinate interaction with both internal and external stakeholders

Program Goal	Program Objectives	Action Items
	2.3 Establish Enterprise Resiliency	Establishment of Out of band communications, communication plan, off-site storage, infrastructure, hardware, and software recovery plans, proactive cybersecurity activities, and not reactionary.

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track Systems, Applications, Users

In order to establish better monitoring of systems, entities throughout Nebraska should consider the implementation of monitoring solutions. These can be paid-for solutions or by leveraging offerings from CISA or organizations such as the MS-ISAC.

Monitor, Audit, and Track network traffic, activities to and from systems, applications, and users

Currently, the State of Nebraska has communications and data network connectivity to every county within the State of Nebraska managed by the Office of the CIO (OCIO). The OCIO also partners with the University of Nebraska under the Network Nebraska Consortium to provide data network services to all K-12 school districts in the State, community colleges, and public and private higher education institutions. Similarly local municipalities and libraries have the option to join Network Nebraska and to leverage this infrastructure. Redundancy is purposefully designed into these network backbones to ensure the continuity of the **data** networks. The goal of this plan is to continue to support the communication between State and Local government, as well as educational institutions. DDoS protection was recently increased for these networks, along with planned future security enhancements. These networks are monitored 24/7 by operations centers servicing both education and local governments.

Enhance Preparedness

Preparedness maturity will vary among organizations. However, more than having an incident response, disaster recovery, or continuity of operations plan alone is required; those plans must also be tested. One of the goals of this plan is to provide template documentation to organizations that currently do not have any cyber incident response plan. A goal is also to support and promote opportunities that provide personnel with hands-on cybersecurity and incident handling training through tabletop exercises, incident response training exercises, et al.

Assessment and Mitigation

While different organizations may have varying strategies for assessment and mitigation, this is no doubt a vital component of the cyber risk reduction strategy. Cyber Risk Assessment and Mitigation (CRAM) are essential steps for validating current controls and mitigations, but they also aid in discovering new risks and vulnerabilities. Organizations should engage in projects that offer assessments of security controls through penetration testing and risk assessment.

Entities at every level are encouraged to have a CRAM program that includes third-party and supply-chain risk management. In order to lead the way, the State of Nebraska will be formulating policies and procedures to foster this development.

Best Practices and Methodologies

Organizations throughout the State of Nebraska are encouraged to implement best practices. The committee's goal is to provide thought leadership and champion the adoption of cybersecurity best practices and initiatives across Nebraska in the face of new and emerging cybersecurity risks and threats. The committee works with industry-specific groups and stakeholders to promote the adoption of these best practices. However, different organizations are at different maturity levels and must establish a baseline to determine which next steps will be needed for their organization.

All eligible entities in the State should strive to apply the following cybersecurity best practices within their organization during the grant performance period:

- 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 default passwords and credentials.
- Ensure the ability to reconstitute systems (backups).
- Migration to the .gov top level domain or approved industry domain (i.e. .edu,).

A baseline is applied to all State-owned, leased, licensed, or managed information systems, system components, and system services and is derived from the controls defined by NIST Special Publication 800-171 R2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

NIST Principles

The Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST) is a collective of standards and guidelines to provide direction and guidance for organizations to reduce and better manage cyber risks at every level of the organization. Eligible entities are encouraged to adopt and follow the NIST CSF framework within their organization. By following a standardized framework, organizations can better determine where investment needs to occur to protect the organization and ensure service delivery.

Supply Chain Risk Management

It is also important for organizations to understand their supply chains and the risk that it potentially poses to their organization. Organizations should develop a cyber supply chain risk management (C-SCRM) program that addresses best practices identified by NIST 800-171. This involves identifying, prioritizing, and assessing information technology suppliers, vendors, and service providers to understand the related and cascading risks to the organizational supply chain.

Tools and Tactics

Engaging the MS-ISAC, CISA, puts an organization in a great position to understand tactics, techniques, and procedures of Advanced Persistent Threat Groups and Nation-state Actors, as well as gaining access to partner organizations and systems to gain access to knowledge bases of adversary tools and tactics to improve your cybersecurity efforts.

Safe Online Services

Eligible entities must utilize top-level domains (TLD) to deliver safe, recognizable, and trustworthy online services. While utilizing a TLD is a critical first step, those domains also need to incorporate secure communications, such as HTTPS, TLS, and certificates, for all State and Local government websites. Along with trusted TLDs and secure communications, secure authentication mechanisms for State and Local government email systems, including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting, and Conformance (DMARC) should be included.

Leveraging a known domain such as .gov or .edu promotes trust to site visitors and aids in combating mis, dis, and mal information. Leveraging secure communications and secure authentication mechanisms reduce fraud from spoofing and phishing. The goal is to promote and support the use of TLD and proper security in association with those domains and the promotion of legitimate email services and security associated with email services. The committee will engage with stakeholders within their specific sector and promote the implementation of safe, recognizable, and trustworthy online services.

Continuity of Operations

Continuity of operations is the first priority when it comes to State and Local government. Ensuring that residents of Nebraska are able to receive the necessary services that they rely on is critical. The plan encourages entities to conduct regular cybersecurity training exercises to test and improve the ability of personnel to recognize and respond to cybersecurity threats.

Workforce

In general, there is a delta of 3.4 million in the cybersecurity workforce and available positions worldwide. The pace in which technology advances and the evolving threat landscape makes the need for cybersecurity essential, but the workforce isn't keeping pace. To address deficit in Nebraska, the goal is to:

Support and promote cybersecurity training and education initiatives for professional development and re-skilling current workers.

1. Continue to support and promote opportunities that provide hands-on cybersecurity and incident handling training to cybersecurity personnel, including continued support for programs such as Cyber Tatanka, GridEx, etc
2. Continue to support and promote organizations conducting regular cybersecurity training exercises to test and improve the ability of personnel to recognize and respond to cybersecurity threats
3. Continue to partner with K-12 and higher education institutions to develop cybersecurity education and training programs to develop a capable cyber workforce of the future
4. Develop and distribute relevant security awareness materials, alerts, and advisories, and provide notifications to key State and Local government stakeholders
5. Continued support of continuing education

Continuity of Communications and Data Networks

Currently the State of Nebraska has communications and data network connectivity to every county within the State of Nebraska managed by the Office of the CIO (OCIO). The OCIO also partners with the University of Nebraska under Network Nebraska to provide data network services to all of the K-12 school districts in the State, and both public and private higher education institutions. Redundancy is purposefully designed into these network backbones to ensure continuity of the networks. The goal of this plan is to continue to support the communication between State and Local government, as well as educational institutions. The level of DDoS protection was recently increased for these networks, along with future planned security enhancements.

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

The goal is to continually assess state and local government networks, systems, and applications to identify vulnerabilities, misconfigurations, gaps in cyber defenses, and emerging threats and prioritize remediation efforts and resources based on risk. This will be accomplished through active scanning done within the State and Local government entities, as well as elements of critical infrastructure within Nebraska. This is accomplished through establishing projects to enhance these activities, and well as increasing relationships with Federal partners and industry organizations.

Cyber Threat Indicator Information Sharing

Currently, the State of Nebraska has the capabilities to source and receive actionable cyber threat intelligence to include indicators of compromise (IOC). At this time, any threat intelligence received or discovered regarding specific entities within the state is required to be passed along to the organization. General IOCs and general threat intelligence are not currently shared outside the State.

As part of a comprehensive cybersecurity program organizations are encouraged to be receiving IoCs and threat intelligence from various sources such as the FBI, CISA, MS-ISAC, or other services. Ensuring that actionable threat intelligence is received and acted upon should be a priority for any eligible entity under the SLCGP.

Leverage CISA Services

As is required by the State and Local Cybersecurity Grant Program any entity that receives funds from the grant is required to enroll in CISA services. However, it is highly encouraged that all eligible entities engage in the free services offered by partner organizations such as CISA, MS-ISAC, FBI, and other industry specific entities.

Information Technology and Operational Technology Modernization Review

The State of Nebraska's strategic approach to ensure alignment between information technology and operational technology cybersecurity objectives is that although much of the funding comes from different sources to protect the totality of these systems, a distinction is not made between controls applied to information technology and operational technology as the convergence of the (formerly) two technologies is almost complete. SLCGP participants may also replace end of life/outdated equipment found at this convergence, e.g., Windows XP and/or Windows 7 Machines if equipment purchases are approved by the SLCGP Planning Committee at some point in the future.

Cybersecurity Risk and Threat Strategies

The Committee should use this plan and operate under their approved charter to develop and coordinate strategies and projects to address cybersecurity risks and threats with other organizations, including consultation with local governments and associations of local governments. Specifically, the Committee includes representatives from the League of Nebraska Municipalities and the Nebraska Association of County Officials, along with the Nebraska Office of the CIO, to continuously solicit and receive input and feedback from their respective members.

Rural Communities

Based on 49 USC § 5302(17) the definition for rural area is any "an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce". Most of the State of Nebraska falls into this category, having only four geographic areas that exceed this limit or have been designated by urbanized areas.

Funding & Services

First year funds will focus on projects that emphasize assessment of cyber capabilities and establishing baselines for future improvements. Establishing a baseline ensures the ability to measure year over year improvement throughout the performance period of the grant. Without baseline data, it's difficult to estimate any changes or to demonstrate progress. Baseline assessment projects will need to focus on current risk and vulnerability through vulnerability scans, penetration tests and risk assessments. Acceptable assessments could also include a focus on governance and the establishment of policies, procedures, and plans, such incident response or disaster recovery plans. For organizations in essence starting from square one, assessments may also include asset discovery, software, hardware inventory and documenting information and data flows. These elements are foundational to information security, in that you can't secure what you don't know you have.

For more mature organizations assessments may include not only penetration tests, vulnerability scans, and governance projects, but also assessment of access controls to information and the implementation of least privilege and assessments of protections of sensitive data types. Assessments may also include audits of device configuration, security controls, and vulnerabilities. However, focus for project scoring and decisions will take into account an organizations cybersecurity maturity, and the goal to increase capabilities across the state. Organizations that are more mature in their cybersecurity capabilities, may not be looked at as favorably when it comes to project proposals. The goal is to get those entities that struggle up to the same bar as the more mature organizations to increase capabilities for the entire State, and not just a select few.

Regardless of an organization's maturity level, an objective would be for eligible entities to implement or enhance current opportunities to provide cybersecurity awareness training to staff and users. Raising awareness is a critical first step in getting the baseline increased.

For subsequent years funding new project proposals will be accepted that focus emphasis on achieving that year's goals, objectives, and action items.

Distribution to Local Governments

The committee has opted to distribute funds through a project-based approach, where project proposals will be scored and ranked. As part of the project proposal and scoring criteria, a projects alignment with this plan and NOFO requirements is taken into consideration, including the distribution to local government and rural areas. One of the scoring criteria is for local and rural stakeholders and impact. Within the scoring criteria for individual project proposals there is a multijurisdictional element to award additional points to support multijurisdictional projects, where impact and effectiveness of funding dollars can be maximized.

At this time, it is not anticipated that the state level will be providing any additional services or capabilities to the local governments beyond what is already provided. The organizational structure in its current form doesn't support the ability to provide additional security capabilities to local government entities. Funds will be leveraged to enhance local government capabilities. This is the reason for the emphasis on multijurisdictional projects. The majority of funds within the SLCGP will be to provide sub-grants or direct pass through of funds as part of this program in order to fund projects that aligned with this plan and the NOFO.

ASSESS CAPABILITIES

The first year of projects and initiatives and elements of year-two are to focus on the assessment of capabilities throughout the State of Nebraska. This focus on State and Local government is to establish a baseline of capabilities throughout Nebraska, ensuring that there is an initial baseline to work from, and to build upon. Because organizations will be at different levels of cybersecurity maturity, establishment of a baseline is imperative to the success of the program.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require support and cooperation from numerous individuals, groups, or agencies, and may be added as formal agenda items for review during regular governance body meetings.

Within the State of Nebraska Executive Branch, the State Information Security Officer (SISO) is responsible for information and data security, with the State Chief Information Officer (CIO) ultimately being accountable for data security. Organizations will have their own staff responsible for data security when it comes to projects regarding data security and those operations may vary based on organization and structure.

A**ppendix A: Project Summary Worksheet** provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

Resources will be allocated as necessary based on organizational projects. This will be part of the organizations project proposal to estimate the necessary resources to complete the project on time and on budget. Funds will be awarded based on project estimates and additional funds for delays and budgetary overruns will not be authorized because of the limited amount of grant funds available.

METRICS

Below are the metrics defined for year FY22 – FY24 Projects based on goals and objectives

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1. Assessment of Cybersecurity Capabilities	1.1 Develop and conduct assessments to identify critical enterprise processes and assets, document information flows, identify and document hardware and software inventories.	Assessment status update and final reports. Did the project stay on budget?	For projects that receive funds, a quarterly status update will need to be provided to the SAA and Committee, a project report after the project identifies that all the project's elements have been completed and implemented, and copies of the deliverables.
	1.2 Review or establish policies for cybersecurity that include roles and responsibilities	Assessment status and final reports. Did the project stay on budget? Was the project complete and objective of delivery of a comprehensive cybersecurity policy accomplished yes or no?	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed, as well as deliverables. (e.g. if you had a project to create a cybersecurity policy, the committee wants to see the policy.)
	1.3 Identify threats, vulnerabilities, and risk to assets identified during assessments	Assessment status to include percentage completion and final reports.	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed, as well as deliverables (e.g. reports from assessments).

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
2. Assessment of Protection Capabilities	2.1Assess and manage access control measures to assets and information	Assessment status update and final reports. Did the project stay on budget? What changes were implemented based on assessment findings	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed, as well as outcomes and changes that have been made to control measures.
	2.2 Assessment of measures to protect sensitive data	Assessment status update and final reports. Did the project stay on budget? What changes were implemented based on assessment findings	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed, as well as outcomes and changes that have been made to protect sensitive data.
	2.3 Assessment of device configuration, security controls, and vulnerabilities.	Assessment status update and final reports. Did the project stay on budget? What changes were implemented based on assessment findings	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed, as well as outcomes and changes that have been made to harden system configurations and or replace legacy systems and applications

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	2.4 End user training to determine cyber awareness capabilities	Has the organization implemented end user cyber awareness assessments and training as part of it policy and operations?	It is strongly encouraged that organizations implement assessments and training for cybersecurity awareness. Entities will either do this or they won't. Some currently have.

Below are the metrics for FY23 Projects

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1. Identify the occurrence of cybersecurity events	1.1 Conduct an assessment of detection methods, processes, and procedures	Assessment status update and final reports. Did the project stay on budget? What changes were implemented based on assessment findings.	Final report will allow for the determination of an organizations detection capabilities and were changes made in order to enhance detection capabilities?
	1.2 Development and assessment of logging practices and enhancement of logging	Current Logging status, project status reports and final reports. Did the project stay on budget? What organizational technology changes were made to develop or enhance logging practices?	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed, as well as deliverables.
	1.3 Cyber Risk Assessments, Identification of organizational risk tolerance.	Assessment status to include percentage completion and final reports. Did the project stay on budget? What changes are being made based on risk assessment.	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed.

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
2. Increase Response Activities	2.1 Develop and test cyber incident response plans through exercises.	At a minimum the organization needs to complete a tabletop exercise in order to test developed plans?	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed.
	2.2 Stakeholder coordination	Has the organization engaged with stakeholders to discuss cybersecurity, incident response, and involved them in a tabletop exercise?	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed. Provide documentation of the tabletop exercise.
	2.3 Best Practice Implementation	Has the organization implemented a best practice they previously hadn't employed? What is the organizations doing to implement best practices established in this plan? Report to the committee which best practices they are implementing and risk reduction impact it has on the organization.	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed. Provide documentation of how the organization is implementing best practices.

FY24 Recovery Phase NIST SP 800-184

Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1. Recover Systems	1.1 Ensure the ability to reconstitute systems in the event of a cyber incident	Assessment status update and final reports. What changes were implemented based on assessment findings. Did the project stay on budget?	Final report will allow for the determination of an organizations detection capabilities and changes were made in order to enhance recovery capabilities?
	1.2 Establish or enhance a backup program for critical data and systems.	Has the organization developed or enhanced capabilities to back up and reconstitute critical systems and data?	For projects that receive funds a quarterly status update will need to be provided to the SAA and Committee, as well as a project report at the conclusion of the project identifying that all the elements of the project have been completed and confirming the ability to reconstitute critical systems and data.
2 Increase Response Activities	2.1 Communicate with internal and external stakeholders	Has the organization conducted a tabletop exercise and engaged with internal and external stakeholders?	Documentation needs to be reported to the committee as validation of internal and external stakeholder engagement.
	2.2 Ensure recovery plans are updated	Does the organization have policies and procedures in place to review plans at specified intervals?	For instance, a policy that states all plans will be reviewed and updated annually. Plans should be provided to committee.
	2.3 Manage public relations and company reputation	Is public relations and reputation management defined as part of the incident response plan to include designating who is responsible?	Provide a copy of the strategic communications policy and procedures to the committee.

APPENDIX A: PROJECT SUMMARY WORKSHEET

This will be completed after project scoring and decisions are made by the committee.

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve capabilities and meet the elements of the NOFO.

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type

APPENDIX B: ACRONYMS

Acronym	Definition
NOFO	Notification of Opportunity for Funding
SLCGP	State and Local Cybersecurity Grant Program
OCIO	Nebraska Office of the Chief Information Officer
SISO	State Information Security Officer
CIO	Chief Information Officer
NIST	The National Institute of Standards and Technology
CSF	The NIST Cybersecurity Framework
IOC	Indicators of Compromise
CISA	Cybersecurity and Infrastructure Security Agency
FBI	Federal Bureau of Investigation
MS-ISAC	Multi-State Information Sharing & Analysis Center
CRAM	Cyber Risk Assessment and Mitigation
TLS	Transport Layer Security
HTTPS	Hypertext Transfer Protocol Secure
DKIM	DomainKeys Identified Mail
DMARC	Domain-Based Message Authentication, Reporting, and Conformance
TLD	Top Level Domain