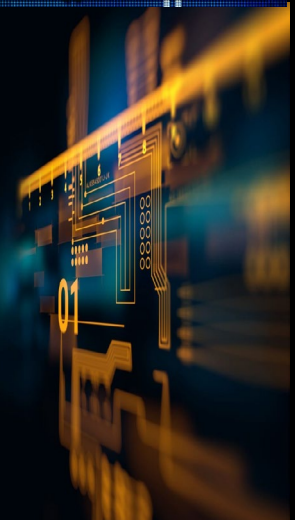

STATE OF NEW MEXICO STATEWIDE CYBERSECURITY PLAN

September 2023

Approved by State of New Mexico Office of Cybersecurity and Statewide Cybersecurity Planning Committee on August 18, 2023
Version 1.0

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from the Cybersecurity Planning Committee **4**
Introduction **5**
Vision and Mission 7
Cybersecurity Program Goals and Objectives 7
Cybersecurity Plan Elements **8**
Manage, Monitor, and Track 9
Monitor, Audit, and Track 10
Enhance Preparedness 11
Assessment and Mitigation 11
Best Practices and Methodologies 12
Safe Online Services 13
Continuity of Operations 14
Workforce 15
Continuity of Communications and Data Networks 15
Protect Critical Infrastructure and Key Resources 16
Cyber Threat Indicator Information Sharing 17
Leverage CISA Services 17
Information Technology and Operational Technology Modernization Review 18
Cybersecurity Risk and Threat Strategies 18
Rural Communities 19
Distribution to Local Governments 19
Funding and Services **19**
Assess Capabilities **20**
Implementation Plan **21**
Organization Roles and Responsibilities 22
Feedback From Local Governments 22
Resource Overview and Timeline Summary 23
Metrics **23**
Appendix A: Cybersecurity Plan Capabilities Assessment **28**
Appendix B: Project Summary Worksheet **32**
Appendix C: Glossary **36**
Appendix D: Acronyms **37**

LIST OF TABLES

Table 1 FY 2022 SLCGP Funding....20
Table 2 Cybersecurity Plan metrics....23
Table 3 NCSR Maturity Levels used to define capability levels....28
Table 4 Initial Cybersecurity Plan Capabilities Assessment....28
Table 5 Project Summary Worksheet....32
Table 6 Glossary....36
Table 7 Acronyms....37

LIST OF FIGURES

Figure 1 Achieving cyber resilience through comprehensive cybersecurity planning....6
Figure 2 Summary of the sixteen required cybersecurity elements....9
Figure 3 Capabilities Assessment process....20
Figure 4 Structure of the NM SLCGP Cybersecurity Planning Committee....21
Figure 5 Collaboration between the NM SLCGP Cybersecurity Planning Committee and Office of Cybersecurity....22
Figure 6 Feedback cycle for the Cybersecurity Plan....22

LETTER FROM THE CYBERSECURITY PLANNING COMMITTEE

Greetings,

The Cybersecurity Planning Committee for the State of New Mexico is pleased to present the 2023 State of New Mexico Cybersecurity Plan. The Cybersecurity Plan represents the State of New Mexico's continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, this update meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the State of New Mexico collaborated with the Cybersecurity Planning Committee to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives to ensure completion. These goals and objectives focus on fostering and increasing collaboration between State and local entities, to mature cybersecurity practices across the State and strengthen our cybersecurity posture using sustainable and scalable solutions. They are designed to support the State of New Mexico in planning for new technologies, navigating the ever-changing cybersecurity landscape, and incorporating the SLCGP required plan elements.

As we continue our efforts, we must remain dedicated to improving our cybersecurity resilience across jurisdictional boundaries. With help from State and local cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for other States.

Sincerely,

Peter Mantos

Cybersecurity Planning Committee Chair

Raja Sambandam

Chief Information Security Officer

New Mexico Office of Cybersecurity

INTRODUCTION

The 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 interoperability over the next one-to-three-years.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within the State of New Mexico along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the State of New Mexico's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The Implementation Plan must include the resources and timeline where practicable.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within the State of New Mexico as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies requirements of the State of New Mexico's cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over the State of New Mexico, local systems, or agencies.
- **How feedback and input from local governments and associations was incorporated:** Describes how inputs from local governments are used to reduce overall cybersecurity risk across the eligible entity. This is especially important to develop a holistic cybersecurity plan.
- **Metrics:** Describes how the State of New Mexico will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

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

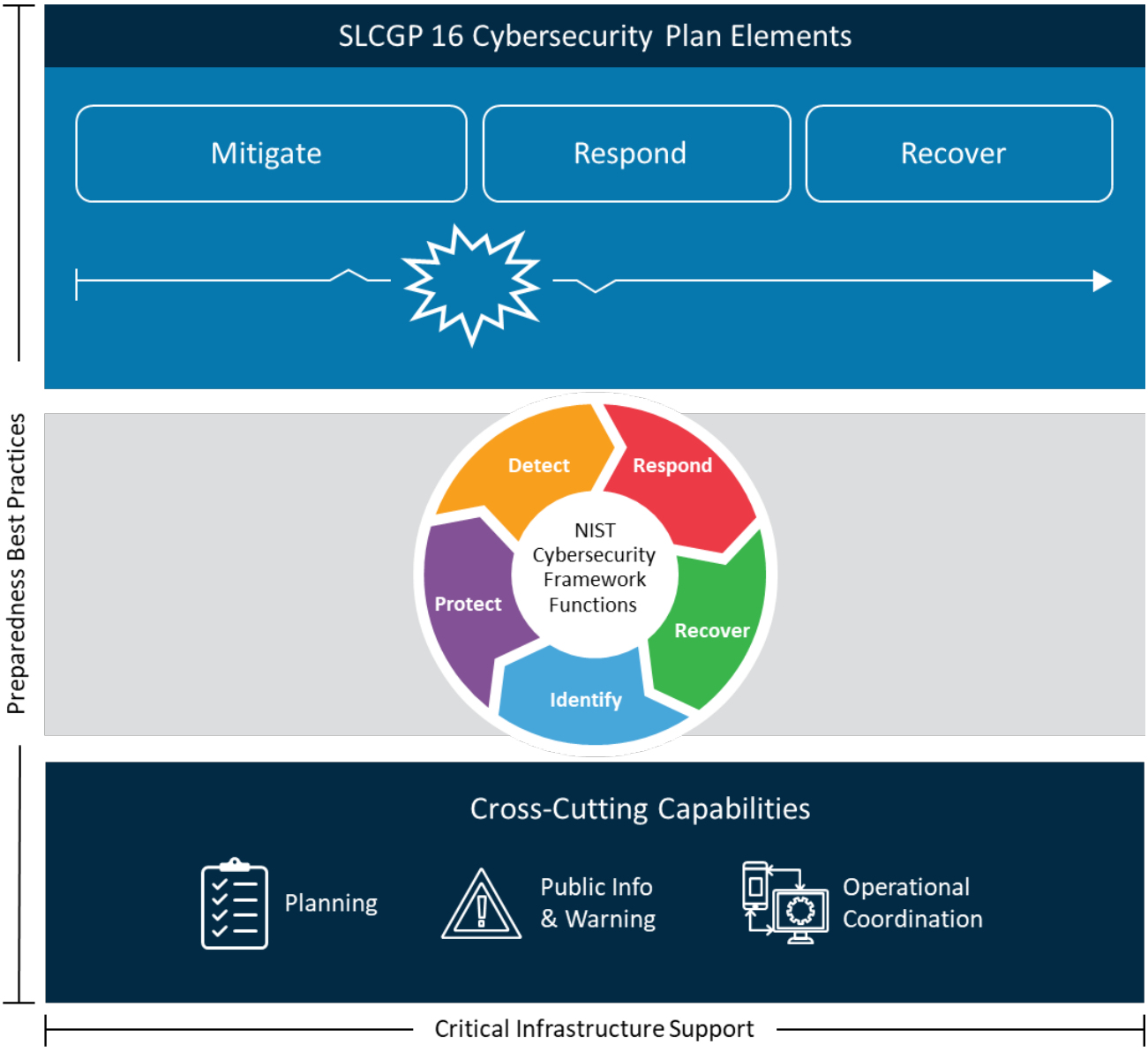

Figure 1 Achieving cyber resilience through comprehensive cybersecurity planning

Vision and Mission

This section describes the State of New Mexico's vision and mission for improving cybersecurity:

Vision:

The State of New Mexico is dedicated to identifying, deterring, and protecting against increasingly sophisticated and malicious cybersecurity threats to protect the health and welfare of the people of this State.

Mission:

Establish cooperation between federal, state, local, and tribal governments, as well as the private sector, to ensure swift, adaptive, and robust action against any current or future cyber threat which may interrupt the delivery of essential services, interfere with functions of government, or threaten protected citizen data.

Cybersecurity Program Goals and Objectives

The Cybersecurity Planning Committee has defined long-term goals to support and implement the Cybersecurity Plan, address identified cybersecurity gaps, and improve the cybersecurity posture across the State of New Mexico. Each of the four (4) goals and objectives described below, aligns to one (1) or more of the required cybersecurity plan elements outlined in the Notice of Funding Opportunity (NOFO) and described in the next section. The Committee utilized a strategic approach, in collaboration with State and Local (e.g., municipality, school district, city, town, township, local public authority, special district, intrastate district, council of governments, county, rural, tribal) entities ('entities'), and considered the results of the Capabilities Assessment to establish the goals and objectives of the Cybersecurity Plan. The following outlines the Cybersecurity Plan's goals and associated objectives intended to guide the selection of cybersecurity investment projects and activities.

Goal 1 – Manage and Monitor Information Systems, Data, and Networks

1.1 Develop and Implement Standards for Asset and Account Management. (SLCGP NOFO Element 1)

1.2 Adopt an Asset Management Platform. (SLCGP NOFO Element 1)

1.3 Identify Leading Monitoring Practices. (SLCGP NOFO Element 2)

1.4 Establish Monitoring Capabilities. (SLCGP NOFO Element 2)

Goal 2 – Enhance Cybersecurity Resilience

2.1 Develop Incident Response Plans. (SLCGP NOFO Element 3)

2.2 Develop Framework and Process to Manage Vulnerabilities. (SLCGP NOFO Element 4)

2.3 Oversee the Adoption of Required Cyber Hygiene Services. (SLCGP NOFO Element 4)

2.4 Establish Vulnerability Management Platform. (SLCGP NOFO Element 4)

2.5 Establish Framework and Process for Continuity of Operations. (SLCGP NOFO Element 7)

2.6 Conduct Response and Recovery Exercises. (SLCGP NOFO Element 7)

2.7 Strategize Resiliency for Communications and Data Networks. (SLCGP NOFO Element 9)

2.8 Identify Critical Infrastructure and Key Resources. (SLCGP NOFO Element 10)

2.9 Protect Critical Infrastructure and Key Resources. (SLCGP NOFO Element 10)

Goal 3 – Develop Statewide Cybersecurity and Risk Management Strategies

3.1 Implement Leading Practices and Methodologies. (SLCGP NOFO Element 5)

3.2 Promote Safe Online Services, including Use of .gov Domain. (SLCGP NOFO Element 6)

3.3 Enable Capabilities to Share Cyber Threat Indicators. (SLCGP NOFO Element 11)

3.4 Adopt and Oversee Implementation of CISA Services. (SLCGP NOFO Element 12)

3.5 Establish IT and OT Modernization Reviews. (SLCGP NOFO Element 13)

3.6 Develop a Statewide Cybersecurity Risk Strategy. (SLCGP NOFO Element 14)

3.7 Coordinate Cybersecurity Planning and Implementation with Entities. (SLCGP NOFO Element 14)

3.8 Provide Services and Programs to Rural Areas. (SLCGP NOFO Element 15)

3.9 Distribute Funds and Services to Local Governments. (SLCGP NOFO Element 16)

Goal 4 – Train and Develop the Cybersecurity Workforce

4.1 Adopt NICE Workforce Framework. (SLCGP NOFO Element 8)

4.2 Conduct Workforce Cybersecurity Training. (SLCGP NOFO Element 8)

4.3 Collaboration with Higher Education. (SLCGP NOFO Element 8)

CYBERSECURITY PLAN ELEMENTS

The following sections describe the Cybersecurity Planning Committee's strategic approach towards implementing the sixteen (16) cybersecurity elements and assisting entities across New Mexico toward maturing their cybersecurity capabilities to protect against cybersecurity risks and threats. The strategic approach for each cybersecurity element was designed to align with leading practices such as NIST CSF and the Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals (CPGs). Each of the required elements also align with one or more associated program objectives. These objectives are intended to guide future cybersecurity investments and projects aimed at helping entities across New Mexico implement the corresponding element. The following graphic summarizes each of the sixteen cybersecurity elements and associated program objectives for achieving intended outcomes.

Figure 2 Summary of the sixteen required cybersecurity elements

Manage, Monitor, and Track

Required Element #1

Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.

The Cybersecurity Planning Committee will coordinate within New Mexico to define and establish standards for entities to manage, monitor, track, and approve assets (applications and systems) and user accounts. In addition, the Committee will seek to invest in solutions or tools that will assist entities with managing assets throughout their lifecycle. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 1.1: Develop and Implement Standards for Asset and Account Management

- Develop standards for maintaining an asset inventory (i.e., hardware, software, devices, licenses) and establish processes to ensure that only approved assets are used by organizational personnel or third parties for business purposes.

- Implement standards for managing and reviewing accounts (e.g., system or user) used to access information systems and networks, incorporating the principle of least privilege and role-based access controls.
- Adopt CISA CPG leading practices for account security:
    - Employ privileged accounts to perform administrative and/or privileged functions and that are separate from ordinary user accounts.
    - Revoke user access credentials (e.g., key cards, user access accounts) whenever an employee depart an organization.

Alignment to Leading Practices:
CPG:
- *1.5 Separating User and Privilege Accounts*
- *1.7 Revoking Credentials for Departing Employees*
- *2.1 Hardware and Software Approval Process*
- *2.3 Asset Inventory*

NIST CSF:
- *ID.AM-1*
- *ID.AM-2*
- *PR.AC-4*

Program Objective 1.2: Adopt an Asset Management Platform

- Identify and invest in asset management solutions or tools to maintain asset inventories and automate capabilities (e.g., detection of new assets, inventory automation and reviews).
    - Verify asset management solutions or tools have a specified degree of control to ensure compliance with established standards for asset and account management.
- Provide guidance and documented procedures on how to manage the asset management platform.

Monitor, Audit, and Track

Required Element #2

Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

Leading practices will be leveraged to enable entities to standardize monitoring capabilities to detect potential cyber threats and events. Network and user monitoring capabilities will be enhanced to allow entities and other relevant stakeholders ('stakeholders') to holistically understand the threat landscape within their networks. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 1.3: Identify Leading Monitoring Practices

- Identify and leverage leading practices (NIST CSF and CISA CPGs) to develop standards for implementing tools to monitor events of interest (i.e., network activity, personnel activity, external service provider activity).
- Assess the threat landscape to identify potential cybersecurity threats to develop monitoring and alert use-cases.

Alignment to Leading Practices:
CPG:
- *8.2 Detecting Relevant Threats and TTPs*

NIST CSF:
- *DE.CM-1*
- *DE.CM-3*
- *DE.CM-6*

Program Objective 1.4: Establish Monitoring Capabilities

- Adopt or enhance cybersecurity monitoring tools to detect and alert on suspicious events and potential threat incidents.
- Integrate threat monitoring capabilities with incident response plans and processes to enable prompt and effective responses to potential threats.

- Partner with higher education and state government entities to establish or extend a statewide or regional Security Operations Center (SOC) and threat intelligence services.

Enhance Preparedness

Required Element #3

Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.

Incident Response Plans will be developed to improve capabilities to detect and contain incidents, minimize the impact of an incident, and reduce the likelihood of future incidents. State, local, and/or tribal entities will coordinate to develop plans and manage incidents. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 2.1: Develop Incident Response Plans

Alignment to Leading Practices:
CPG:
- *6.2 Supply Chain Incident Reporting*
- *7.2 Incident Response (IR) Plans*

NIST CSF:
- *PR.IP-7*
- *PR.IP-9*
- *PR.IP-10*

- Develop procedures and guidelines for internal and external organizations on responding to security incidents which includes instructions on effectively responding to potential threats in a timely manner.
- Collaborate with entities to create a model incident response plan which can be used as a template to create their own customized plans which includes the following:
  - Description of processes to review, update, and test response plans on a specified frequency.
  - Guidance for management to support the implementation of the response plans.
- Define processes for identifying, containing, eradicating, and recovering from security incidents.
- Coordinate Incident Response Plans with Disaster Recovery and Business Continuity Plans to ensure the State can continue to operate in the event of a disruption or disaster.
- Describe processes for coordinating and integrating incident response plans and procedures across entities and stakeholders such as vendors, expert groups, and authorities when incidents occur.
- Report and share cybersecurity incidents with CISA, Multi-State Information Sharing and Analysis Center (MS-ISAC), entities, and stakeholders as part of Cyber Threat Intelligence (CTI) sharing capabilities.

Assessment and Mitigation

Required Element #4

Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

The Cybersecurity Planning Committee will establish a vulnerability management and threat mitigation framework to provide entities and stakeholders with guidelines and leading practices. Additionally, the

Committee will oversee the adoption of required CISA Cyber Hygiene services. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 2.2: Develop Framework and Process to Manage Vulnerabilities

- Develop a standard set of procedures and guidelines for vulnerability management that incorporates leading practices and industry standards, including but not limited to:
  - Mitigating known exploited vulnerabilities within internet-facing systems while prioritizing critical assets; compensating controls (e.g., segmentation, monitoring, etc.) will be applied and recorded where applicable.
  - Performing periodic Vulnerability Assessment and Penetration Testing (VAPT) to maintain an updated list of known, accepted, and mitigated vulnerabilities.
  - Reporting detailed descriptions (e.g., incident type, category, prioritization, etc.) of cyber vulnerabilities and incidents to required stakeholders.
- Extend vulnerability reporting requirements to vendors and other third-party entities to standardize vulnerability reports.
- Engage with entities and stakeholders to provide tailored support and guidance based on their requirements and needs.

Alignment to Leading Practices:
CPG:
- *5.1 Mitigating Known Vulnerabilities*
- *6.3 Supply Chain Vulnerability Disclosure*

NIST CSF:
- *DE.CM-8*
- *ID.RA-1*
- *RS.MI-2*
- *RS.MI-3*
- *RS.CO-2*

Program Objective 2.3: Oversee the Adoption of Required Cyber Hygiene Services

- Monitor and track the adoption of CISA Cyber Hygiene Services by the entities and stakeholders to align with NOFO requirements.

Program Objective 2.4: Establish Vulnerability Management Platform

- Identify and invest in tools and technologies, including automated solutions as appropriate, to help entities enhance their vulnerability scanning, patch management, and configuration management capabilities for more effective and efficient vulnerability identification and cyber risk mitigation.

Best Practices and Methodologies

Required Element #5

Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below. The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:

- *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); and*
- *Migration to the .gov internet domain.*

Leading cybersecurity practices and methodologies, such as those recommended by the NIST CSF and CISA CPGs, will be adopted to standardize cybersecurity capabilities, enhance cybersecurity posture across the State, and manage and protect the IT assets and infrastructure of entities. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.1: Implement leading Practices and Methodologies

- Implement multi-factor authentication (e.g., hardware tokens, authenticator apps, SMS) for remote access and privileged users.
- Enhance logging capabilities to include additional details and store logs within a centralized system to improve the availability of log data.
- Employ strong and agile encryption policies and solutions (e.g., firewalls, VPNs, encryption software) to protect sensitive data while in transit and at rest.
- Perform periodic assessments to identify and retire end of life public facing systems to reduce or mitigate the impact of potential threats and vulnerabilities.
- Establish clear guidelines and standards for credential and password management that include:
    - Changing default manufacturer passwords to prevent unauthorized access.
    - Establishing unique credentials to better manage user access and improve the auditability of user activities.
    - Defining a minimum password strength to protect accounts from brute force attacks.
- Establish system requirements to regularly perform and test backups of data, systems, applications, and other critical and key resources required to restore systems.
- Adopt and implement minimum security standards and policies across entities' IT resources to ensure availability, confidentiality, and integrity of processed, transferred, or stored information.

Alignment to Leading Practices:
CPG:
- *1.2 Changing Default Passwords*
- *1.3 Multi-Factor Authentication (MFA)*
- *1.4 Minimum Password Strength*
- *1.6 Unique Credentials*
- *3.1 Log Collection*
- *3.2 Secure Log Storage*
- *3.3 Strong and Agile Encryption*
- *3.4 Secure Sensitive Data*
- 7.3 System Back Ups

Safe Online Services

Required Element #6

Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.

The Committee will coordinate with entities and nongovernment stakeholders to assess the use and trustworthiness of hosted online services, encourage eligible and appropriate entities to migrate to the .gov domain, and promote safe online services. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.2: Promote Safe Online Services, including Use of .gov Domain

- Assess, support, and promote the transition to the .gov internet domain for State and Local governments eligible to use the domain.
- Develop and maintain a catalog of trusted cybersecurity services for entities across the State.

- Support online services safety improvement for stakeholders that are not eligible for the .gov domain by recommending and assisting them with migrating to other appropriate and more trusted internet domains (e.g., .edu).

Continuity of Operations

Required Element #7

Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

Plans, processes, procedures, and recommended tools and services for enabling continuity of operations will be developed and shared with entities to help reduce the impact and disruption of a cybersecurity incident. Additionally, response and recovery exercises will be conducted to practice responding to a cybersecurity incident, and associated plans, processes, and procedures updated post-exercise. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 2.5: Establish Framework and Process for Continuity of Operations

- Establish a framework to serve as the baseline for continuity of operations planning and exercises based on leading practices during or after an incident.
- Identify recommended Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) for entities to establish the maximum amount and time that critical data can be lost in the event of a disaster or major disruption.
- Provide training and resources to help develop and improve entities' continuity plans, including guidance on best practices and lessons learned from previous exercises.
- Collaborate and coordinate between entities and stakeholders, including by facilitating regular meetings, sharing information and resources, and conducting joint exercises.

Alignment to Leading Practices:
NIST CSF:
- *PR.IP-4*
- *PR.IP-10*
- *ID.SC-5*
- *RS.RP-1*
- *RS.IM-1*
- *RS.IM-2*

Program Objective 2.6: Conduct Response and Recovery Exercises

- Coordinate and facilitate incident response and recovery exercises (e.g., tabletop testing, simulation, fail-over, data backups) with entities, suppliers, third-party providers, and stakeholders to enhance their business continuity preparedness for potentially disruptive incidents.
- Update response strategies after conducting response and recovery exercises to incorporate lessons learned.

Workforce

Required Element #8

Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.

The Cybersecurity Planning Committee will coordinate with entities and stakeholders to adopt the National Initiative for Cybersecurity Education (NICE) framework to identify and mitigate gaps in their cybersecurity workforce and training, establish proper workforce training standards, and collaborate with higher education. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 4.1: Adopt NICE Workforce Framework

- Develop a cybersecurity training plan, guidance, and assessment templates using the NICE Framework to aid entities and stakeholders in assessing their cybersecurity workforce.
- Monitor entities and potential stakeholders' progress towards adopting the NICE Framework and conducting associated cybersecurity workforce assessments.

Alignment to Leading Practices:
CPG:
- *4.3 Basic Cybersecurity Training*
- *4.4 OT Cybersecurity Training*

NIST CSF:
- *PR.AT-1*
- *PR.AT-2*

Program Objective 4.2: Conduct Workforce Cybersecurity Training

- Establish standards requiring cybersecurity training and ensure users, including privileged users, receive role-specific cybersecurity training and are informed of their responsibilities in maintaining cybersecurity measures.
- Provide and facilitate a range of relevant cybersecurity training opportunities (e.g., conferences, role-specific training) to refresh basic security concepts, address identified gaps, and enhance workforce cyber expertise.

Program Objective 4.3: Collaboration with Higher Education

- Partner with higher education institutions to develop and implement education and training opportunities for emerging cybersecurity professionals.

Continuity of Communications and Data Networks

Required Element #9

Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

Communications and data networks will be fortified to help improve communications resiliency and continuity capabilities across entities. Collaboration with entities will help identify weaknesses,

dependencies, and opportunities to mature and protect communications and data networks. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 2.7: Strategize Resiliency for Communications and Data Networks

Alignment to Leading Practices:
NIST CSF:
- *PR.PT-4*
- *PR.PT-5*

- Foster relationships with entities to understand their communications resiliency, weaknesses and pain points, and improvement areas to strengthen continuity capabilities.
- Identify and implement solutions to build resiliency of communications and data networks between entities in normal situations and to minimize the impact of an incident, including:
    - Establishing standard processes for implementing fault tolerance and redundancies.
    - Deploying IDS/IPS solutions for key networks.
    - Defining and periodically reviewing firewall/router requirements and rules.
    - Verifying network and remote access from all wireless devices and client machines.
- Develop statewide plans outlining strategies, requirements, and procedures to enable entities to respond to an event impacting communications and data networks.

Protect Critical Infrastructure and Key Resources

Required Element #10

Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.

Identifying Critical Infrastructure and Key Resources (CIKR) will be an entity-wide approach to assist entities with better understanding their risk landscape and where to enhance their cybersecurity capabilities. This will allow entities to implement measures to identify potential risks and threats, evaluate their impact, and take steps to ensure the availability of CIKR. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 2.8: Identify Critical Infrastructure and Key Resources

Alignment to Leading Practices:
NIST CSF:
- *ID.RA-5*
- *ID.RA-6*
- *ID.AM-5*
- *ID.BE-4*
- *DE.AE-2*
- *DE.AE-4*
- *ID.RM-3*

- Collaborate with entities to identify CIKR necessary for the effective operation of information systems within the jurisdiction of the State.
    - Conduct Business Impact Analysis (BIA) within the entities to assist with the identification process.
    - Record, group, and periodically update key assets based on classification and criticality.
    - Where applicable, coordinate with entities to protect critical infrastructure information (CII) from public disclosure.
- Where appropriate, coordinate with CIKR plan owners to incorporate cybersecurity best practices, cyber threat data, and related assessments into existing plans (e.g., incident response, disaster recovery, business continuity) to protect critical infrastructure and key resources necessary for the effective operation of information systems within the jurisdiction of the State.

- Adopt a standard scoring model and define risk tolerance levels to facilitate creation of risk response plans.
- Leverage threat intelligence data for analysis of detected events against CIKR to better understand attack methods and determine the potential impact of events.

Program Objective 2.9: Protect Critical Infrastructure and Key Resources

- Review cybersecurity risk to CIKR which may impact the effective operation of information systems within the jurisdiction of the State.
- Validate that CIKR owners and operators maintain current cybersecurity response and recovery plans where appropriate.

Cyber Threat Indicator Information Sharing

Required Element #11

Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.

CTI sharing capabilities will be promoted, enabled, and enhanced within the State through engagement and support of entities and stakeholders. Enabling CTI sharing allows the State to identify and share threat intelligence to enhance entities' cybersecurity detection and response capabilities. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.3: Enable Capabilities to Share Cyber Threat Indicators

Alignment to Leading Practices:
CPG:
- *5.2 Vulnerability Disclosure/Reporting*
- *7.1 Incident Reporting*

NIST CSF:
- *ID.RA-2*

- Establish centralized capabilities to share cyber threat intelligence between the Cybersecurity Office and internal organizations, external organizations, and relevant stakeholders throughout the State.
- Foster and lead the adoption of CISA CTI services across entities and stakeholders to mutually share and report cyber threat events.
- Partner with the State's fusion center to conduct cyberthreat information sharing, analysis, and dissemination between state, local, and private organizational levels and the federal level.

Leverage CISA Services

Required Element #12

Leverage cybersecurity services offered by the Department (See NOFO Appendix G for additional information on CISA resources and required services and membership).

The Cybersecurity Planning Committee will guide the adoption of the required CISA services while also encouraging participation in recommended services, memberships, and resources to better understand the cybersecurity posture of entities and stakeholders and assist them in reducing their risk. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.4: Adopt and Oversee Implementation of CISA Services

- Coordinate the annual enrollment of entities and stakeholders in the Nationwide Cybersecurity Review (NCSR) self-assessment program to assess and identify gaps in their cybersecurity program and capabilities.
- Promote and support the adoption of CISA services, including Cyber Hygiene Services, by entities and stakeholders to standardize and reduce duplication of cybersecurity services leveraged across the State.

Information Technology and Operational Technology Modernization Review

Required Element #13

Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

Lead and encourage IT/OT modernization reviews to identify areas where new solutions (e.g., cloud services, upgraded software) can be adopted to improve operations, harden (secure) technologies, reduce costs, and/or proactively phase out legacy and unsupported systems. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.5: Establish IT and OT Modernization Reviews

- Provide guidance to entities for incorporating industry-leading cybersecurity practices in all assessments and implementation projects for modernizing legacy IT and OT systems.

Cybersecurity Risk and Threat Strategies

Required Element #14

Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.

A Cybersecurity Risk Strategy will be developed and coordinated with entities to ensure that both State and local governments uniformly understand and manage risk. The strategy will allow the State and local entities to consistently define how risks, threats, and vulnerabilities should be managed. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.6: Develop a Statewide Cybersecurity Risk Strategy

- Develop a statewide Cybersecurity Risk Strategy based on input from federal, state, and local governments and associations of local governments to help ensure strategic consistency and compatibility across the State.

Alignment to Leading Practices:
NIST CSF:
- *ID.RM-1*

Program Objective 3.7: Coordinate Cybersecurity Planning and Implementation with Entities

- Develop a cybersecurity framework outlining guidelines for managing cybersecurity risks and threats in collaboration with industry experts, government officials, and other stakeholders, and serving as a roadmap for entities in their cybersecurity planning and implementation efforts.
- Establish a centralized function to oversee and coordinate cybersecurity efforts across entities to ensure a consistent approach towards adopting cybersecurity practices and capabilities.
- Establish cybersecurity and data breach notification standards for entities and publish them as guidelines for non-executive agencies and political subdivisions of the State.

Rural Communities

Required Element #15

Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.

An Engagement Subcommittee was established to identify and connect with local government entities and stakeholders (e.g., public education, county, municipal, healthcare) across the State. As part of its outreach efforts, the Engagement Subcommittee provided an initial survey to identify potential participating entities to ensure that rural communities are included in the Cybersecurity Plan development and implementation efforts, including participating in the Capabilities Assessment. The following Cybersecurity program objectives intend to support accomplishments of this SLCGP required element:

Program Objective 3.8: Provide Services and Programs to Rural Areas

- Provide cybersecurity services, products, and programs through investment projects where at least 25% of SLCGP federal funding benefits entities in rural areas of the State.

Distribution to Local Governments

Required Element #16

Distribute funds, items, services, capabilities, or activities to local governments.

The Cybersecurity Planning Committee will engage with local governments and rural areas across the State of New Mexico to establish services, capabilities, and activities that will be accessible to, benefit, and address the cybersecurity needs of those entities in lieu of direct funding.

Program Objective 3.9: Distribute Funds and Services to Local Governments

- Provide cybersecurity services, products, and programs through investment projects where at least 80% of SLCGP federal funding benefits local government entities in the State.

FUNDING AND SERVICES

The State of New Mexico State has been awarded $2,540,403 in federal SLCGP funding and will submit a cost-share waiver for FY 2022 as displayed in the following table:

Table 1 FY 2022 SLCGP Funding

FY 2022 SLCGP Funding			
Anticipated Federal Funding Release	Federal Allocation	New Mexico State Share	Total FY 2022 Award
September 2023	$2,540,403	$282,267 - Submitting cost waiver	$2,822,670

In addition to the funding that will be received as part of the SLCGP, the NM Office of Cybersecurity will also work towards obtaining additional funds sustain cybersecurity initiatives and investments described under this plan.

Additional information on how at least 80% of the federal SLCGP allocation will fund items, services, capabilities, and activities that benefit local governments (including rural areas realizing a benefit of at least 25% of the federal allocation) is included above in the "Rural Communities" and "Distribution to Local Governments" subsections under "Cybersecurity Plan Elements." Projects planned for investment leveraging FY 2022 SLCGP funding are identified, along with a description, cost, status, priority, etc. for each project, in "Appendix B: Project Summary Worksheet."

ASSESS CAPABILITIES

An initial Cybersecurity Capabilities Assessment was conducted with participating entities (e.g., entities and stakeholders) to determine cybersecurity gaps and maturity levels against the sixteen (16) required plan elements and the CISA CPGs. It was conducted through a self-assessment allowing each entity to self-identify its level of maturity using the Multi-State Information Sharing and Analysis Center's (MS-ISAC) NCSR maturity benchmarks, while allowing participants to openly describe cybersecurity risks within their entities. The Capabilities Assessment was formally closed to any additional responses at the end of July 2023 so as to provide an initial baseline of statewide maturity versus the required elements while also enabling identification of initial SLCGP-funded projects for inclusion in the New Mexico Cybersecurity Plan in advance of the plan submission deadline to CISA. The results of the assessment were used to identify, prioritize, and select investment projects to address cybersecurity gaps and needs.

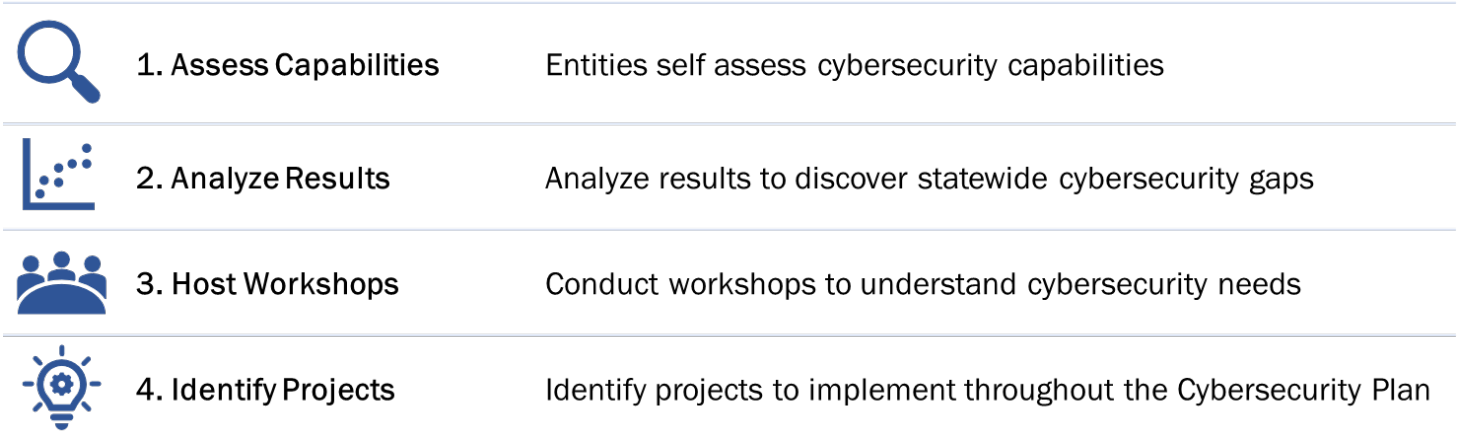

Figure 3 Capabilities Assessment process

IMPLEMENTATION PLAN

Through an Executive Order (EO), the NM SLCGP Cybersecurity Planning Committee has been tasked with the development and maintenance of the SLCGP Cybersecurity Plan to help improve the cybersecurity posture of SLT entities across New Mexico. The Committee has defined roles and responsibilities to implement the Cybersecurity Plan and metrics to measure progress towards implementing the Plan. The graphic below (Figure 5) illustrates the composition of the Committee.

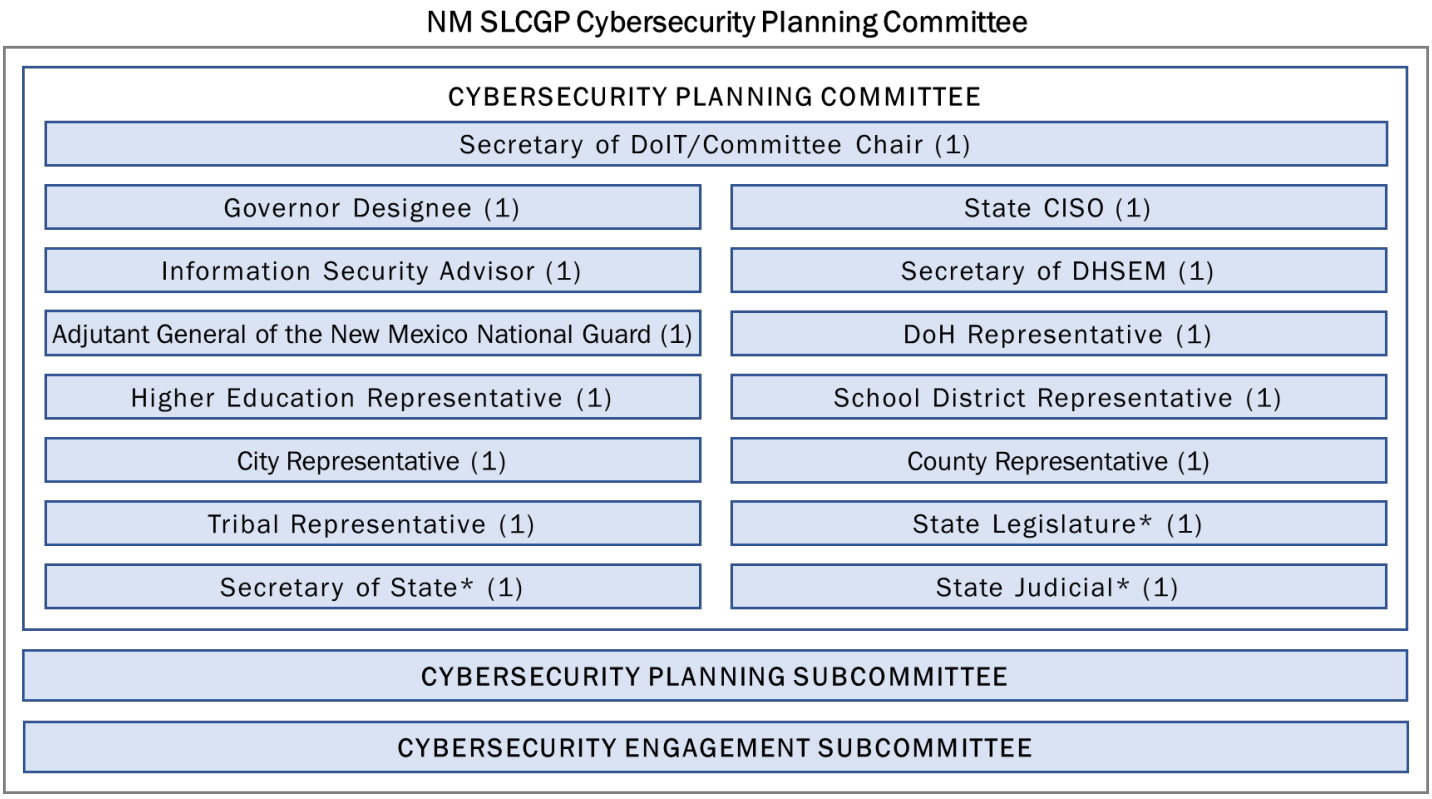

Figure 4 Structure of the NM SLCGP Cybersecurity Planning Committee

Organization Roles and Responsibilities

Strategic initiatives defined in the Cybersecurity Plan will be executed through the State of New Mexico's Office of Cybersecurity and implemented by entities participating in the SLCGP. The Committee developed the Plan and identified cybersecurity services and activities for addressing potential cyber threats. Representatives from local entities assisted the Committee by providing input on the status of their cybersecurity capabilities and key security concerns while participating and voting during Committee activities. Going forward, the Office of Cybersecurity and the NM Cybersecurity Advisory Committee will continue to update the Cybersecurity Plan to ensure that goals, objectives, and investment projects will address cybersecurity risks and the needs of SLT entities going forwards.

The Office of Cybersecurity is responsible for the implementation of the services and activities identified by the Cybersecurity Planning Committee. The Office of Cybersecurity will collaborate with other departments and stakeholders to ensure a comprehensive and coordinated approach to cybersecurity.

The Planning Committee will work with the Office of Cybersecurity and State Administrative Agency (SAA) to deliver investment projects to entities and oversee the implementation of those projects. Local entities within New Mexico will be able to adopt the services or capabilities provided under the cybersecurity grant program.

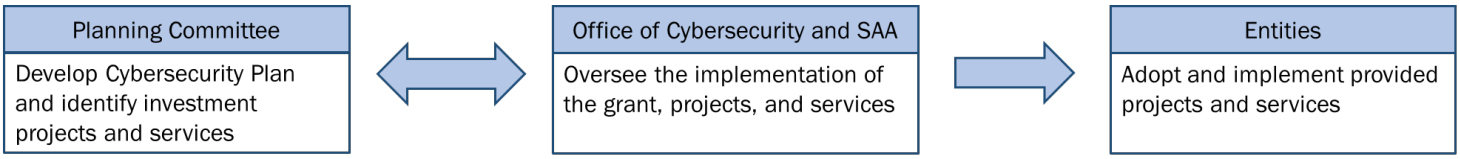

Figure 5 Collaboration between the NM SLCGP Cybersecurity Planning Committee and Office of Cybersecurity

Feedback From Local Governments

The Cybersecurity Planning Committee established an Engagement Subcommittee with the goal of identifying, involving, and soliciting feedback from entities to develop the Cybersecurity Plan and identify investment projects to address cybersecurity risks and threats. Participating entities provided feedback and input through the development of the Cybersecurity Plan and included representation from the following sectors within the State of New Mexico:

- State Government Agency or Department
- Judicial (Courts)
- Justice/Law Enforcement
- Public Education and Charter Schools (K-12)
- Private Education (K-12)
- Higher Education
- County
- Local Municipality (city, town, etc.)
- Tribal Agency
- Healthcare
- Critical Infrastructure

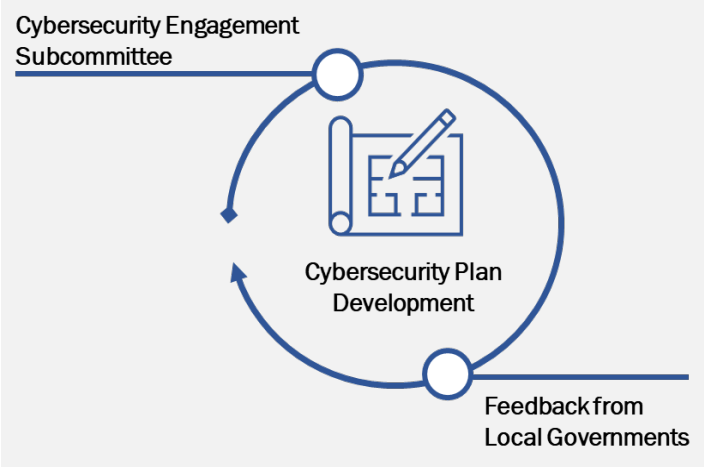

Figure 6 Feedback cycle for the Cybersecurity Plan

Representatives from participating entities will continue to collaborate with the Cybersecurity Planning Committee and New Mexico Office of Cybersecurity to oversee the execution of the Cybersecurity Plan and associated projects.

Resource Overview and Timeline Summary

The Cybersecurity Planning Committee identified necessary resources and a timeline for implementing and achieving the Plan goals and objectives throughout the next two to three years. Within 45 days of FY 2022 SLCGP funding availability for non-Plan development projects, pass-through will be completed in the form of obtaining signed consent agreements from authorized officials of local governments consenting to the receipt of items, services, capabilities, and activities provided by the State on their behalf. A summary of investment projects can be found in "Appendix B: Project Summary Worksheet."

The State of New Mexico Cybersecurity Planning Committee understands that, upon CISA approval, the Cybersecurity Plan is required to be resubmitted for CISA review and approval within two years and then annually thereafter. In between these required, periodic resubmissions to CISA, the Planning Committee will also review the Cybersecurity Plan for any necessary, substantive changes that may be needed and will revise the Plan accordingly. As investment projects are completed, resulting in mitigation of risks, closure of identified capability gaps, and achievement of initially targeted program objectives, new projects will be selected that address additional and potentially new program objectives. Further, as the Cybersecurity Plan is a "living, breathing" strategy for cybersecurity and cyber risk reduction across New Mexico, it is anticipated that project priorities will shift with the changing cybersecurity landscape and as determined by continual cyber risk assessments performed over time (e.g., annual NCSR).

METRICS

The New Mexico Cybersecurity Planning Committee has developed metrics to measure progress towards implementing the Cybersecurity Plan and minimizing cybersecurity threats and risks. These metrics are designed to help stakeholders understand the State's progress towards achieving its Cybersecurity goals and objectives. A baseline level for the associated metrics will be determined before establishing overall metric goals for the rest of the program.

The table below outlines the program goals, objectives, associated metrics, and metric descriptions that the State of New Mexico has established for measuring its progress in implementing its Cybersecurity Plan.

Table 2 Cybersecurity Plan metrics

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
1. Manage and Monitor information Systems, Data, and Networks	1.1 Develop and Implement Standards for Asset and Account Management	▪ Percentage of entities with a documented Asset and Account Management policy or standard	Details: The number of entities that have a documented Asset and Account Management policy or standard in place divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
	1.2 Adopt an Asset Management Platform	▪ Percentage of entities with an IT asset management platform in operation	Details: The number of entities that have an IT asset management platform in operation divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	1.4 Establish Monitoring Capabilities	▪ Percentage of entities that have cyber threat monitoring capabilities in place	Details: The number of entities that have cyber threat monitoring capabilities in place divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
2. Enhance Cybersecurity Resilience	2.1 Develop Incident Response Plans	▪ Percentage of entities that have a documented Incident Response Plan	Details: The number of entities that have a documented Incident Response Plan divided by the total number of each entity type responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.2 Develop Framework and Process to Manage Vulnerabilities	▪ Percentage of entities that have a documented and approved vulnerability management policy or standard	Details: The number of entities that have a documented and approved vulnerability management policy or standard divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.3 Oversee the Adoption of Required Cyber Hygiene Services	▪ Percentage of entities that have implemented multi-factor authentication ▪ Percentage of entities that have implemented enhanced logging ▪ Percentage of entities that have implemented encryption for data at rest and in transit ▪ Percentage of entities that have ended use of unsupported/ end of life software and hardware accessible from the Internet ▪ Percentage of entities that have prohibited use of	Details: The number of entities that have: ▪ Implemented multi-factor authentication; ▪ Implemented enhanced logging; ▪ Implemented encryption for data at rest and in transit; ▪ Ended use of unsupported/end of life software and hardware accessible from the Internet; ▪ Prohibited use of known/ fixed/default passwords and credentials; and ▪ Ensured the ability to reconstitute systems from backups divided by the total number of entities responding to a request for that information

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
		known/ fixed/default passwords and credentials ▪ Percentage of entities that have ensured the ability to reconstitute systems from backups	Source: Cyber risk assessment questionnaire Frequency: Annual
	2.4 Establish Vulnerability Management Platform	▪ Percentage of entities with a vulnerability management platform in operation	Details: The number of entities that have a vulnerability management platform in operation divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.5 Establish Framework and Process for Continuity of Operations	▪ Percentage of entities that have a documented and approved framework and process for Continuity of Operations	Details: The number of entities that have a documented and approved framework and process for Continuity of Operations divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.6 Conduct Response and Recovery Exercises	▪ Percentage of entities that conduct response and recovery exercises (at least annually)	Details: The number of entities that conduct response and recovery exercises (at least annually) divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.7 Strategize Resiliency for Communications and Data Networks	▪ Percentage of entities that develop and execute strategies for enhancing the resilience of communications and data networks	Details: The number of entities that develop and execute strategies for enhancing the resilience of communications and data networks divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	2.8 Identify Critical Infrastructure and Key Resources	▪ Percentage of entities that identify and inventory critical infrastructure and key resources ▪ Percentage of identified non-governmental CIKR owners that identify and inventory critical infrastructure and key resources	Details: The number of entities and non-governmental CIKR owners that identify and inventory critical infrastructure and key resources divided by the total number of each entity type responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
	2.9 Protect Critical Infrastructure and Key Resources	▪ Percentage of entities that analyze and prioritize the protection of critical infrastructure and key resources ▪ Percentage of identified non-governmental CIKR owners that analyze and prioritize the protection of critical infrastructure and key resources	Details: The number of entities and non-governmental CIKR owners that analyze and prioritize the protection of critical infrastructure and key resources divided by the total number of each entity type responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
3. Develop Statewide Cybersecurity and Risk Management Strategies	3.1 Implement Leading Practices and Methodologies	▪ Percentage of entities that are implementing leading cybersecurity practices and methodologies	Details: The number of entities that are implementing leading cybersecurity practices and methodologies divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	3.2 Promote Safe Online Services, including Use of .gov Domain	▪ Percentage of local governments entities that use the .gov domain	Details: The number of local government entities that use the .gov domain divided by the total number of local government entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	3.3 Enable Capabilities to Share Cyber Threat Indicators	▪ Percentage of entities that share cyber threat indicators with the NM Office of Cybersecurity, other entities within the State of New Mexico, and/or CISA ▪ Percentage of identified non-governmental entities that share cyber threat indicators with the NM Office of Cybersecurity, other entities within the State of New Mexico, and/or CISA	Details: The number of entities and identified non-governmental entities that share cyber threat indicators with the NM Office of Cybersecurity, other entities within the State of New Mexico, and/or CISA divided by the total number of each entity type responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	3.4 Adopt and Oversee Implementation of CISA Services	▪ Percentage of entities that participate in CISA's Cyber Hygiene Services (web application and external network vulnerability scanning) ▪ Percentage of entities that complete the Nationwide Cybersecurity Review	Details: The number of entities that: ▪ Participate in CISA's Cyber Hygiene Services (web application and external network vulnerability scanning); and ▪ Complete the Nationwide Cybersecurity Review divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire; CISA for Cyber Hygiene

Cybersecurity Plan Metrics			
Program Goals	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
			Services participation; and/or MS-ISAC for NCSR completion Frequency: Annual
	3.5 Establish IT and OT Modernization Reviews	▪ Percentage of entities that have implemented an IT and OT modernization cybersecurity review process that ensures alignment between IT and OT cybersecurity objectives	Details: The number of entities that have implemented an IT and OT modernization cybersecurity review process that ensures alignment between IT and OT cybersecurity objectives divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	3.6 Develop a Statewide Cybersecurity Risk Strategy	▪ A statewide cybersecurity risk strategy has been developed and approved and is in use and reviewed at least annually.	Details: A statewide cybersecurity risk strategy has been developed and approved and is in use and reviewed at least annually. Source: Policy review Frequency: Annual
	3.8 Provide Services and Programs to Rural Areas	▪ At least 25% of SLCGP-funded cybersecurity items, services, capabilities, or activities benefit rural areas in the State	Details: At least 25% of SLCGP-funded cybersecurity items, services, capabilities, or activities benefit rural areas in the State Source: Pass-through documentation & financial review Frequency: Annual
	3.9 Distribute Funds and Services to Local Governments	▪ At least 80% of SLCGP-funded cybersecurity items, services, capabilities, or activities benefit local governments in the State	Details: At least 80% of SLCGP-funded cybersecurity items, services, capabilities, or activities benefit local governments in the State Source: Pass-through documentation & financial review Frequency: Annual
4. Train and Develop Cybersecurity Workforce	4.1 Adopt NICE Workforce Framework	▪ Percentage of entities that have formally adopted the NICE Framework	Details: The number of entities that have formally adopted the NICE Framework divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual
	4.2 Conduct Workforce Cybersecurity Training	▪ Percentage of entities that conduct workforce cybersecurity training (at least annually)	Details: The number of entities that conduct workforce cybersecurity training (at least annually) divided by the total number of entities responding to a request for that information Source: Cyber risk assessment questionnaire Frequency: Annual

APPENDIX A: CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

After reviewing the Cybersecurity Elements against the results of the Capabilities Assessment, larger entities possess a higher level of cybersecurity maturity than smaller entities. The NCSR Maturity Levels were chosen to determine the "Capability Level" in Table 4. The NCSR utilizes seven (7) defined maturity levels that are depicted in Table 3 below.

Table 3 NCSR Maturity Levels used to define capability levels

NCSR Maturity Levels	
Maturity Level (Capability Level)	**Definition**
1. Not Performed	Activities, processes, and technologies are not in place to achieve the referenced objective.
2. Informally Performed	Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
3. Documented Policy	Your organization has a formal policy in place and some activities related to this area are informally performed.
4. Partially Documented Standards and/or Procedures	Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
5. Risk Formally Accepted	Your organization has chosen not to implement based on a risk assessment.
5. Implementation in Process	Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
6. Tested and Verified	Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
7. Optimized	Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.

Below is an aggregation of the responses across the State and not representative of any individual entity type or individual entity.

Table 4 Initial Cybersecurity Plan Capabilities Assessment

Completed by the State of New Mexico			
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities**	**Capability Level *(See Table 3 for capability level designations)***	**Project # (s)**
1. Manage, monitor, and track information systems, applications, and user accounts	Majority of entities have formal policies but communications issues between management and IT makes following procedures difficult	4. Partially Documented Standards and/or Procedures	TBD
2. Monitor, audit, and track network traffic and activity	Larger entities have a higher capability level than smaller ones but staffing issues across all entities prevents frequent network monitoring	3. Documented Policy	Proposed NM-7 Proposed NM-12
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Larger entities have more mature response plans than smaller ones, but all entities are not testing them as frequently and do not have reporting requirements for third-party vendors	3. Documented Policy	Proposed NM-3
4. Implement a process of continuous cybersecurity risk assessment and	Majority of entities perform vulnerability assessments, but do not have formalized	4. Partially Documented Standards and/or Procedures	Proposed NM-2 Proposed NM-3

Completed by the State of New Mexico			
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities**	**Capability Level *(See Table 3 for capability level designations)***	**Project # (s)**
threat mitigation practices prioritized by degree of risk	criteria to escalate cybersecurity events to enact incident response plans		Proposed NM-4 Proposed NM-10 Proposed NM-11
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	Majority of entities have documented policies in place but lack of cybersecurity staff makes it difficult to follow existing standards and procedures	4. Partially Documented Standards and/or Procedures	Proposed NM-2 Proposed NM-9
a. Implement multi-factor authentication	Larger entities are utilizing MFA at a higher capability level than smaller entities	4. Partially Documented Standards and/or Procedures	Proposed NM-15
b. Implement enhanced logging	Almost all entities have policies to implement enhanced logging, but those entities which do not have policies only informally perform it	4. Partially Documented Standards and/or Procedures	Proposed NM-16
c. Data encryption for data at rest and in transit	All entities have processes to encrypt data in transit at a higher capability level than at rest	4. Partially Documented Standards and/or Procedures	Proposed NM-17
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Almost all entities have policies to remove unsupported components, but those which do not have policies struggle to remove legacy systems from their infrastructure	4. Partially Documented Standards and/or Procedures	Proposed NM-18
e. Prohibit use of known/fixed/default passwords and credentials	Almost all entities have standards and procedures that are in development or have been established to prohibit the use of known/fixed/default passwords and credentials	4. Partially Documented Standards and/or Procedures	Proposed NM-19
f. Ensure the ability to reconstitute systems (backups)	Larger entities have a higher capability to reconstitute systems than smaller ones	5. Implementation in Process	Proposed NM-20
g. Migration to the .gov internet domain	Majority of entities are not eligible and not currently using the .gov domain	N/A	Proposed NM-21
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Entities that are eligible to use the .gov domain are currently using the domain or in the process of migrating over. Those not eligible are mainly entities that are unlikely to change such as educational institutions	N/A	Proposed NM-21
7. Ensure continuity of operations including by conducting exercises	Majority of entities have response and recovery plans in place and that are updated, but they are not tested with third-party vendors	3. Documented Policy	TBD
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and	Majority of entities provide basic training that includes phishing training on a higher frequency than role-based training and do not utilize the NICE Framework for workforce assessments	3. Documented Policy	Proposed NM-5 Proposed NM-6 Proposed NM-13 Proposed NM-14

Completed by the State of New Mexico			
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities**	**Capability Level *(See Table 3 for capability level designations)***	**Project # (s)**
abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)			
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Majority of entities have started developing standards and procedures for resiliency mechanisms but have not implemented the mechanisms	4. Partially Documented Standards and/or Procedures	TBD
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity	Majority of entities utilize risk scores for vulnerabilities, but do not have formal policies to utilize those scores in risk response plans and in analyzing attack targets and methods. Additionally, BIA is only informally used to identify critical infrastructure, functions, and dependencies	3. Documented Policy	Proposed NM-3 Proposed NM-10
11. Enhance capabilities to share cyber threat indicators and related information between the State of New Mexico, local governments within the State, and CISA	Majority of entities have formal policies in place to report incidents in a timely manner, but do not have policies to share or receive information with external organizations such as CISA	3. Documented Policy	Proposed NM-12
12. Leverage cybersecurity services offered by the Department	The number of entities within New Mexico that have completed the NCSR and/or are enrolled in CISA vulnerability and web scanning services is unknown	N/A	Proposed NM-3 Proposed NM-4 Proposed NM-10 Proposed NM-11
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Majority of entities have documented policies, but do not have procedures to replace legacy systems (either IOT or OT) resulting in an overreliance on and difficulty updating legacy systems	3. Documented Policy	TBD
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Most entities have a documented policy for developing strategies to address cybersecurity risks and threats on an individual basis, but they are not coordinated across entities	3. Documented Policy	Proposed NM-2 Proposed NM-9

Completed by the State of New Mexico			
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities**	**Capability Level *(See Table 3 for capability level designations)***	**Project # (s)**
15. Ensure rural communities have adequate access to, and participation in plan activities	Rural communities have minimal access and participation in current activities but have been included in SLCGP planning activities	N/A	TBD
16. Distribute funds, items, services, capabilities, or activities to local governments	For local government entities that consent, items, services, capabilities, and activities will be provided to those local governments in lieu of grant funding distributed to them	N/A	TBD

APPENDIX B: PROJECT SUMMARY WORKSHEET

As depicted in Table 5 below, this Project Summary Worksheet provides a list of cybersecurity projects that the State of New Mexico plans to complete to develop or improve cybersecurity capabilities identified in "Appendix A: Cybersecurity Plan Capabilities Assessment." Previously submitted grant application for FY 2022 only contained amount for Cybersecurity Plan Development. NM-1 through NM-6 represent the planned projects that will be submitted through an amendment for FY 2022. The Cybersecurity Planning Committee expects to submit a cost share waiver for FY 2022 and will be subject to approval, which will in turn impact the total amount available.

Table 5 Project Summary Worksheet

Project Summary Worksheet							
No.	**Project Name**	**Project Description**	**Related Required Element #**	**Cost***	**Status**	**Priority**	**Project Type**
NM-1	Cybersecurity Plan Development	Develop an initial Statewide Cybersecurity Plan to align with State, Local, Cybersecurity Grant Program (SLCGP) requirements.	N/A	$575,000.00	Ongoing	High	Plan
NM-2	Cybersecurity Governance and Planning (Phase 1)	Establish governance structure and channels to coordinate grant activities between the Cybersecurity Planning Committee and eligible grant recipients. This will also include developing guidance (policies and standards) and plan to adopt cyber-hygiene and best practices (e.g., MFA, enhanced logging, migration to .gov, etc.) as required by the grant.	4, 5, 14	$450,000.00	Future (near-term using FY 2022 funding)	High	Plan
NM-3	Cybersecurity Risk Assessments (Phase 1)	Conduct Statewide risk assessments utilizing the NCSR, MS-ISAC Foundational Assessment, etc. to understand entities' cybersecurity posture and identify cybersecurity risks and control gaps. Assessment results will be leveraged to update the Cybersecurity Plan and select future SLCGP investment projects.	4, 10, 12	$500,000.00	Future (near-term using FY 2022 funding)	High	Organize
NM-4	Vulnerability and Attack Surface Management (Phase 1)	Plan the deployment and integration of vulnerability and attack surface management capabilities to assist and support entities with mitigating cybersecurity risks.	4, 12	$488,000.00	Future (near-term using FY 2022 funding)	High	Plan
NM-5	Cybersecurity Training (Phase 1)	Develop and provide basic cybersecurity and phishing awareness training to entities.	8	$250,000.00	Future (near-term using FY 2022 funding)	High	Train
NM-6	Cybersecurity Workforce Development	Develop a plan and strategic roadmap to assist entities with adopting and leveraging the NICE framework to assess their cybersecurity workforce.	8	$150,383.00	Future (near-term using FY 2022 funding)	High	Plan

Project Summary Worksheet							
No.	Project Name	Project Description	Related Required Element #	Cost*	Status	Priority	Project Type
	Planning (Phase 1)						
NM-7	Statewide Security Operations Center (SOC) Planning (Phase 1)	Assess existing cybersecurity monitoring, detection, and response capabilities to develop a roadmap towards implementing a Statewide SOC for New Mexico. This will allow New Mexico to understand existing gaps, requirements, and develop an approach to stand-up a Statewide SOC.	2	TBD	Future	High	Plan
NM-8	Incident Response Planning and Playbook	Develop a model incident response plans and playbook to respond to cyber incidents.	3	TBD	Future	High	Plan
NM-9	Cybersecurity Governance and Planning (Phase 2)	Continue supporting established governance structures to coordinate and plan grant activities between the Cybersecurity Planning Committee and participating entities.	5,14	TBD	Future	Medium	Plan
NM-10	Cybersecurity Risk Assessments (Phase 2)	Perform continuous assessment with participating entities using either NCSR or MS-ISAC Foundational Assessment to identify and prioritize investment projects and serve as a basis to update the Cybersecurity Plan as needed.	4, 10, 12	TBD	Future	Medium	Organize
NM-11	Vulnerability and Attack Surface Management (Phase 2)	Procure and deploy Vulnerability and Attack Surface management tools to participating entities.	4, 12	TBD	Future	Medium	Organize
NM-12	Statewide Security Operations Center (SOC) Implementation	Based on the Statewide SOC Center implementation roadmap, New Mexico will establish and deploy a Statewide SOC to address gaps and mature cybersecurity monitoring and response capabilities.	2, 11	TBD	Future	High	Organize
NM-13	Cybersecurity Training (Phase 2)	Update basic cybersecurity training materials and onboard participating entities to the delivering platform.	8	TBD	Future	Medium	Train
NM-14	Cybersecurity Workforce Development	Assist and coordinate with entities to assess their Cybersecurity Workforce based on the NICE framework.	8	TBD	Future	Medium	Organize

Project Summary Worksheet							
No.	Project Name	Project Description	Related Required Element #	Cost*	Status	Priority	Project Type
	Planning (Phase 2)						
NM-15	Multi-Factor Authentication (Builds on NM-2)	Advise and assist local government and tribal entities implement multi-factor authentication through extending State-contracted MFA service.	5(a)	TBD	Future	High	Organize
NM-16	Enhancing Logging (Builds on NM-2)	Advise and assist local government and tribal entities in implementing enhanced logging.	5(b)	TBD	Future	High	Organize
NM-17	Encrypting data at rest and in transit (Builds on NM-2)	Advise and assist local government and tribal entities encrypt all sensitive data at rest and in transit.	5(c)	TBD	Future	High	Organize
NM-18	Discontinuing use of unsupported /end of life hardware and software (Builds on NM-2)	Advise and assist local government and tribal entities to discontinue the use of unsupported/end of life software and hardware that are accessible from the Internet.	5(d)	TBD	Future	High	Organize
NM-19	Prohibiting use of insecure passwords and credentials (Builds on NM-2)	Advise and assist local government and tribal entities prohibit the use of known/fixed/default passwords and credentials.	5(e)	TBD	Future	High	Organize
NM-20	Ensuring ability to reconstitute systems (Builds on NM-2)	Advise and assist local government and tribal entities ensure the ability to reconstitute systems (backups).	5(f)	TBD	Future	High	Organize

Project Summary Worksheet							
No.	Project Name	Project Description	Related Required Element #	Cost*	Status	Priority	Project Type
NM-21	Migrating to the .gov Internet domain (Builds on NM-2)	Advise and assist appropriate local government and tribal entities with migration to the .gov internet domain.	5(g), 6	TBD	Future	High	Organize

*The cost amounts shown are estimates for each project and sum up to the total federal allocations minus 5% M&A.

APPENDIX C: GLOSSARY

Table 6 Glossary

Term	Description
Agency	Executive cabinet agencies and their administratively attached agencies, offices, boards and commissions
Cybersecurity	Acts, practices or systems that eliminate or reduce the risk of loss of critical assets, loss of sensitive information or reputational harm as a result of a cyber-attack or breach within an organization's network
Entities	State, Local, Tribal entities within the State of New Mexico
Information Security	Acts, practices or systems that eliminate or reduce the risk that legally protected information or information that could be used to facilitate criminal activity is accessed or compromised through physical or electronic means
Information Technology	Computer hardware, storage media, networking equipment, physical devices, infrastructure, processes and code, firmware, software and ancillary products and services, including: 1. Systems design and analysis; 2. Development or modification of hardware or solutions used to create, process, store, secure or exchange electronic data; 3. Information storage and retrieval systems; 4. Voice, radio, video and data communication systems; 5. Network, hosting and cloud-based systems; 6. Simulation and testing; 7. Interactions between a user and an information system; and 8. User and system credentials
Local Entities	Municipality, school district, city, town, township, local public authority, special district, intrastate district, council of governments, county, rural, tribal entities within the State of New Mexico
Security Officer	The State Chief Information Security Officer (CISO)
Stakeholders	Non-SLT entities such as private healthcare agencies, educational institutions, and critical infrastructure owners and operators

APPENDIX D: ACRONYMS

Table 7 Acronyms

Acronym	Definition
BIA	Business Impact Analysis
CIKR	Critical Infrastructure and Key Resources
CISA	Cybersecurity and Infrastructure Security Agency
CPGs	Cybersecurity Performance Goals
CSF	Cybersecurity Framework
CTI	Cyber Threat Intelligence
DHSEM	Department of Homeland Security and Emergency Management
DoH	Department of Health
DoIT	Department of Information Technology
EO	Executive Order
MFA	Multi-Factor Authentication
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCSR	Nationwide Cybersecurity Review
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NOFO	Notice of Funding Opportunity
RPOs	Recovery Point Objectives
RTOs	Recovery Time Objectives
SAA	State Administrative Agency
SLAs	Service Level Agreements
SLCGP	State and Local Cybersecurity Grant Program
SLT	State, Local, Territorial
VAPT	Vulnerability Assessment and Penetration Testing