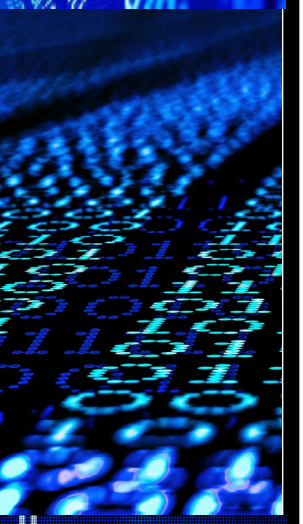

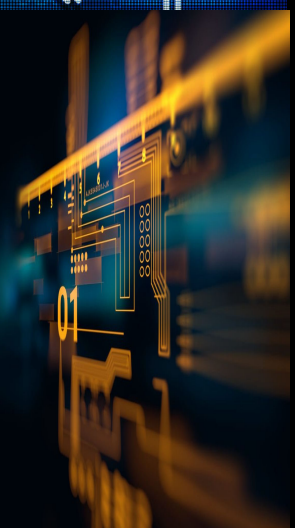

STATE OF MONTANA
CYBERSECURITY PLAN
2022-2024

Approved by the State of Montana

Cybersecurity Planning Committee

on September 25 , 2023

Version 1.3

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM THE CYBERSECURITY PLANNING COMMITTEE

Greetings,

The State of Montana Cybersecurity Planning Committee (the Committee) is pleased to present to you the State of Montana Cybersecurity Plan (the Plan). The Plan represents the State of Montana'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 state, county, municipal, public health, and education sectors within Montana formed the Committee to develop and update the Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus leveraging economies of scale to maximize funds to implement risk-based programs that directly benefit the entities represented on the Committee. This document is structured to meet the required plan elements defined in the Notice of Funding Opportunity.

As we continue to enhance the State of Montana's cybersecurity posture, we are committed to improving our resilience across disciplines and jurisdictions. With help from FEMA, CISA, other federal partners, and cybersecurity practitioners throughout the State of Montana, we will work to achieve the goals set forth in The Plan and become a model for cyber resilience.

Sincerely,

Kevin Gilbertson
Chief Information Officer and
Chair of the Montana Cybersecurity Planning Committee
State of Montana
Department of Administration

INTRODUCTION

Montana faces unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on networked technologies for the day-to-day operation of critical infrastructure. Cyber risk management is further complicated by the ability of malicious actors to operate remotely, linkages between cyber and physical systems, and the difficulty of reducing vulnerabilities.

Considering the risk and potential consequences of cyber incidents, strengthening the cybersecurity practices and resilience of state, local governments is an important homeland security mission and the primary focus of State Local Cyber Grant Program (SLCGP). Through funding from the Infrastructure Investment and Jobs Act, the SLCGP enables Montana to make targeted cybersecurity investments in government agencies, thus improving the security of critical infrastructure and improving the resilience of the services Montana's governments provide their communities.

The Statewide Cybersecurity Strategic Plan is to guide aspects of Montana's critical infrastructure sectors and create a unity of effort. The approach focuses on how we will collectively reduce risk and build resilience to cyber threats to the state's cybersecurity posture of all participants.

The Plan is a two-year strategic planning document for SLCGP years 2022-2024 that contains the following components:

- Vision and Mission: Articulates the vision and mission for improving cybersecurity resilience interoperability over the next two years.
- Organization, and Roles and Responsibilities: Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within the State of Montana 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 authorities and requirements of the State of Montana cybersecurity program. The Plan is a guiding document and does not create any authority or direction over any of the State of Montana's or local systems or agencies.
- How feedback and input from local governments and associations was incorporated. Describes how inputs from local governments was used to reduce overall cybersecurity risk across the eligible entity. This is especially important in order to develop a holistic cybersecurity plan.
- 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 Montana along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- Implementation Plan: Describes the State of Montana's plan to implement, maintain, and update the Plan to enable continued evolution of and progress toward the identified goals. The implementation plan must include the resources and timeline where practicable.
- Metrics: Describes how the State of Montana will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, and the CIS Security Controls[2], included in Figure 2, 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. CIS controls map to the NIST CSF and are often used to help guide discussion with locals as they are more easily digested and have implementation groups to guide maturity efforts.

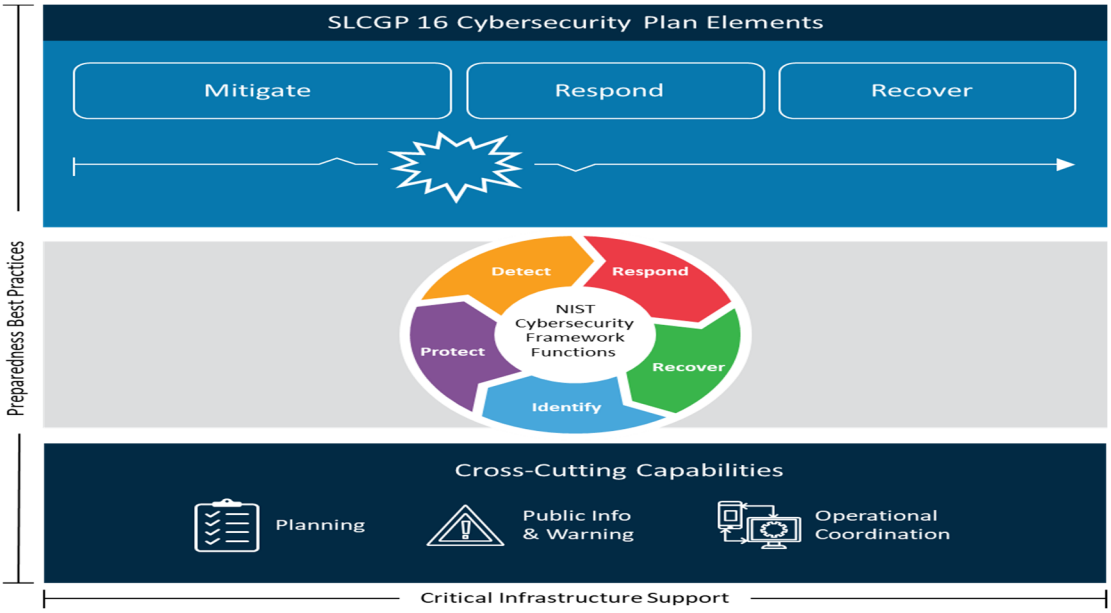

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

Figure 2: The Critical Security Controls are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks.

[1] https://www.nist.gov/cyberframework/getting-started
[2] https://www.cisecurity.org/controls

Vision and Mission

This section describes State of Montana's vision and mission for improving cybersecurity:

Vision:

To enhance the cybersecurity posture and increase the resilience of Montana governments by unifying state and local experience and expertise.

Mission:

To unify State and Local resources to create a safer digital landscape for Montana.

Cybersecurity Program Goals and Objectives

State of Montana Cybersecurity goals and objectives that align with NIST Cyber Security Framework include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. Identify	**Asset Management** **1.1** Leverage the Montana Information Security Advisory Council (MT-ISAC) to create a workgroup focused on increased cybersecurity apprenticeships and internships opportunities in Montana (CSF ID.AM-6) **Governance** **1.2** Leverage MT-ISAC monthly sharing of cyber threat information and industry best practices to all Montana's: Governments, Critical Infrastructure, and Small Businesses. Use MT-ISAC to also promote Council approved groups and associations (Cyber406, CyberMontana, MT National Guard, other ISACs, DHS, etc.) that are promoting situational awareness (CSF ID.GV-4) **Risk Management Strategy** **1.3** Leverage MT-ISAC and industry best practices to support and standardize on NCSR as annual risk assessment. Provide additional guidance for use of other Council NIST based (CISA CPGs & CRE & CRR, & EDM, CIS Critical Controls) approved assessments. (CSF ID.RM-1) **1.4** Deliver support for State and Local governments to move to .GOV for email and websites. Explore options for K-12. (CSF ID.RM-1)

Program Goal	Program Objectives
	1.5 Leverage MT-ISAC and industry best practices to create a standard naming convention for government entities moving to .GOV(CSF ID.RM-1)
2. Protect	**Identity Management, Authentication and Access Control** **2.1** Leverage MT-ISAC to create a guideline or reference an established industry best practice on Multifactor Authentication with options to use current state services and contracts (CSF PR.AC-7, CIS Control 6.3, 6.4, 6.5) **2.2** Deliver solutions to Local Governments and K-12 to help protect network integrity with proper network segmentation (CSF PR.AC-5, CIS Control 12.2) **2.3** Leverage MT-ISAC to create a guideline or reference an established industry best practice on prohibiting use of known/fixed/ default passwords and credentials with options to use current state services and contracts (CSF PR.AC-1, CIS Control 4.7) **Awareness and Training** **2.4** Deliver basic end user security awareness training for Montana State & Local governments and K-12 (CSF PR-AT-1, CIS Control 14) **2.5** Deliver cyber education to privileged users and cyber professionals within Montana State & Local governments and K-12 (CSF PR-AT-2, CIS Control 14.9) **2.6** Deliver access for Montana State & Local governments and K-12 privileged users and cyber professionals to cyber ranges (CSF PR-AT-2, CIS Control 14.9) **Data Security** **2.7** Leverage MT-ISAC to create a guideline or reference an established industry best practice on encryption for data at rest and in transit with options to use current state services and contracts (CSF PR.DS-1 & 2, CIS Control 3.6 & 3.9 & 3.10 & 3.11) **Information Protection Processes and Procedures** **2.8** Leverage MT-ISAC to create a guideline or reference an established industry best practice on limiting use of unsupported/end of life (EOL) software and hardware and ending the use of EOL on systems that are accessible from the internet with options to use current state services and contracts (CSF PR-IP-2, CIS Control 12.1 & 13.5 & 16.5) **2.9** Leverage MT-ISAC to create a guideline or reference an established industry best practice on backup and recovery with options to use current state services and contracts (CSF PR-IP-4, CIS Control 11) **Protective Technology**

Program Goal	Program Objectives
	2.10 Leverage MT-ISAC to create a guideline or reference an established industry best practice on audit/log records with options to use current state services and contracts (CSF PR.PT-1, CIS Control 8)
3. Detect	**Anomalies and Events** **3.1** Deliver Network Monitoring and Management Intrusion Detection Systems (IDS) solutions for County Governments for better protection for Election Offices, Emergency Services, and Public Water System Municipalities. (CSF DE.CM-1, CIS Control 13.3) **3.2** Deliver support for State & Local governments and K-12 to utilize MS-ISAC's no cost Malicious Domain Blocking and Reporting (MDBR) or like service (CSF DE.CM-1 & PR.AC-5, CIS Control 9.2) **Security Continuous Monitoring** **3.3** Deliver Endpoint Detection and Response solution for Montana Local Governments and K-12 (CSF DE.CM-4, CIS Control 10) **3.4** Deliver support for all State and Local government public facing IPs to have external vulnerability scanning with weekly report to entity (CSF DE.CM-8, CIS Control 7.6)
4. Respond	**Response Planning** **4.1** Leverage MT-ISAC and industry best practices to create a statewide incident response reporting process (CSF RS.RP-1 & PR.IP-9, CIS Control 17)
5. Recover	**Recovery Planning** **5.1** Leverage MT-ISAC and industry best practices by delivering training, workshops, exercises on incident response and recovery planning (CSF RC.RP-1 & PR.IP-10, CIS Control 17)

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track information systems and user accounts

Entities should establish procedures that effectively control and restrict access to information assets to authorized users based on defined business and legal requirements. Mechanisms will be implemented that provide for the control, administration, and tracking of access to, and the use of, information assets, as well as the protection of such assets from unauthorized or unapproved activity and/or destruction.

The Cybersecurity Framework and CIS Security Controls both start with knowing what you have in both hardware and software. This includes physical and virtual, on premises and off. It is hard to secure what you do not know. Once you know what you have then the security frameworks turn to who has access to those assets. This is addressed with Access Management. Poor practices in these areas lead to compromised systems and data breaches. In today's everchanging world of technology best practice is to use security orchestration, automation and response technologies.

The State of Montana manages, monitors, and tracks information systems, applications, and user accounts that are used to conduct state business. A combination of asset inventory tools with both active and passive discovery are used to inventory and identify assets and users connected to the state's networks. A Governance, Risk and Compliance (GRC) tool is used to inventory state systems and for tracking risk and compliance against state policy.

Montana has a Network Security Operations Center (NSOC) and a Cyber team that ingests alerts and responds to risks identified by these solutions.

The strategic approach for improvement is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist and identify the right tools that can be leveraged to benefit State, Local and K-12. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

Monitor, Audit, and Track network traffic and activity

Entity asset owners, asset custodians, and information security and privacy officers should:

- Ensure the information assets under their purview are assessed for security and privacy risks and configured such that event logging is enabled to ensure an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems are identified and managed; and
- Review and retain event logs in compliance with all applicable Local, State and Federal laws, regulations, executive orders, circulars, directives, internal agency and state information security policies, and contractual requirements.

Montana's methodology to monitor, audit, and track network activity includes Albert Sensors that are placed strategically throughout our network. Defense in depth is used for our firewalls and edge devices. All user traffic will cross a next generation firewall performing packet inspection for IDS/IPS, virus, URL and DNS monitoring. A SIEM and monitoring agents are used to feed data into our security operations center. The centralized log management approach is used for actionable data and long-term storage of logs so that all statutory requirements are met.

State of Montana is using a standardized XDR solution to better protect, detect, audit, and track network traffic and activity. This solution and its deployment allow for complex auditing and monitoring of attacks and allows for quicker reaction and detection.

The strategic approach for improvement is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist and identify the right tools that can be leveraged to benefit State, Local and K-12. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

Enhance Preparedness

Entities should implement continuous risk management processes that account for the identification, assessment, treatment, and monitoring of risks that can adversely impact their operations, information systems, and information. These processes will inform the exercise and execution of Incident Response Plans, Continuity of Operations Plans and the State Emergency Operation Plan. Lessons Learned from these exercises will be incorporated into future planning, inform organizational decisions, and demonstrate additional equipment and training needs.

Montana is embracing preparedness in the following ways:

- Planning – Montana has worked with state agencies and others to develop Business Continuity (BC) plans and has semi-annual Disaster Recovery (DR) tests.
- Organization – Montana takes a whole of government approach to protect the state and prepare for disasters before they occur.
- Equipment – Montana is working on redundant systems and services to protect the state and its citizens.
- Training – Montana is working with other entities in the state and expanding its testing of disaster recovery and incident response.
- Exercise – Montana has held joint tabletop exercises with a variety of public and private partners to better enhance our response capability. We work closely with the National Guard.

The solutions above are primarily from the perspective of Montana state government and do not necessarily provide coverage for Montana local governments and K-12.

The strategic approach for improvement is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist and identify the right tools that can be leveraged to benefit State, Local and K-12. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

Assessment and Mitigation

All information systems and applications should undergo security assessments to ensure adequate security and privacy controls are implemented and risks are managed to acceptable levels throughout their lifecycles. Risk management processes including identifying, assessing, and addressing security and privacy risks at the inception of the project to build a system until the decommissioning of a system. These actions enable State and Local Government entities to maintain security and privacy of a system throughout its lifecycle. To aid in satisfying the ongoing assessment requirements, assessment results from the following sources can be used: continuous monitoring, audits and authorizations, and other system development life cycle activities.

Montana has an Information Security Policy and Standards that define the processes and procedures the State of Montana uses to identify, prioritize, and escalate for remediation, vulnerabilities in the State's IT infrastructure. The plan outlines the various vulnerability identification processes that feed into the program.

Montana currently participates in the CISA Cyber Hygiene services including vulnerability scanning of our external facing network assets.

Montana uses a combination of both agent and non-agent-based, credentialed, and non-credentialed, internal and external, vulnerability scans. Critical, high, and exploitable vulnerabilities for state agencies are imported into ESM for tracking and remediation.

Critical applications are reviewed on a yearly basis or as changes are made. The Incident Response & Technical Security team along with the Policy and Risk Management team tracks any issues and works with the responsible parties to work toward remediation.

The solutions above are primarily from the perspective of Montana state government and do not necessarily provide coverage for Montana local governments.

As a condition of receiving SLCGP funding, the grant recipients will sign up for and maintain CISA's no cost Vulnerability Scanning(CyHy) and Web Application Scanning services as well as complete annually the no cost Nationwide Cybersecurity Review (NCSR) assessment administered by MS-ISAC. The NCSR is open to complete in October through late February, check with MS-ISAC on availably.

The strategic approach for improvement is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist and identify the right tools that can be leveraged to benefit State, Local and K-12. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

Best Practices and Methodologies

All State and Local governments should adopt and incorporate best practices and methodologies to enhance cybersecurity. The following cybersecurity best practices must be included:

These are not required to be implemented immediately, but all cybersecurity plans must clearly articulate efforts to implement these best practices across the eligible entity within a reasonable timeline. Individual projects that assist SLTT entities adopt these best practices should also be prioritized.

Montana is adopting the following cybersecurity best practices:

- Implement multi-factor authentication (MFA) – While used for state agencies, this is not fully implemented for Local Governments or K-12 school districts.
- Implement enhanced logging – Montana captures various log sources such as authentication logs, device logs, network logs and firewall logs. Enhanced logging is enabled through our XDR solution.
- Data encryption for data at rest and in transit – This is a state standard for encryption for agencies and a potential opportunity for Local Governments or K-12 school districts.
- End use of unsupported/end of life software and hardware that are accessible from the Internet – This is an area of needed improvement, and we would like to use future funds from IIJA to address this issue.
- Prohibit use of known/fixed/default passwords and credentials – State agencies have adopted this best practice, but Local Governments or K-12 school districts have much work in this area to achieve compliance.

- Ensure the ability to reconstitute systems (backups) – This is another area that we would like to use future years IIJA funds to improve our Local Governments or K-12 school districts.
- Migration to the .gov internet domain – While this process is ongoing there is more work to be done here for the Local Governments or K-12 school districts.

The strategic approach for improving this element is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

NIST Principles

Montana has adopted a cybersecurity framework that was developed from the NIST cybersecurity framework (CSF). The Montana cybersecurity framework specifically applies to Montana State Information Technology Services Division (SITSD) and the information assets under its control.

Supply Chain Risk Management

Montana Information Technology's Governance, Risk, and Compliance team uses the risk management framework and is investigating using StateRamp to help address supply chain risk.

Tools and Tactics

The State of Montana's SITSD cyber team actively engages the Montana Analysis and Technical Information Center (MATIC), MS-ISAC, CISA, FBI and other government and industry partners to share knowledge of adversary tools and tactics.

The strategic approach for improvement is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist and identify the right tools that can be leveraged to benefit State, Local and K-12. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

Safe Online Services

For Organizations eligible to receive funds under the SLCGP who have not previously migrated to the .gov domain, one of the projects under consideration is a managed service to assist with this migration.

Montana is promoting the .gov domains to all our city, county, school and other partners. We believe there are many benefits and are encouraging this move in the following ways:

- State of Montana's Chief Information Security Officer (CISO) promotion of .gov domain and benefits at numerous conferences and presentations each year
- Cannot be spoofed
- Available at no cost
- Helps the public quickly identify Local Governments as a trusted government website
- Signed up multiple entities for this migration
- Assisted several counties through CISA to get moved to .gov domain

Continuity of Operations

State and Local Government entities should develop, implement, test, and maintain contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical functions. Contingency planning is an important aspect of risk management. Ensuring availability for critical and essential systems and components allows agencies to meet its mandates that are dictated by statute, executive order, policy, or contract, and to ensure delivery of vital government services.

The State of Montana reviews the Continuity of Operations Plan (COOP) at least annually to align with shifting industry trends, such as remote workforce and updated technologies. Communication is a cornerstone of any continuity of operation plan. We believe that plans are of little value if not tested. The State of Montana COOP includes the following:

1. Mission essential functions and business essential functions,
2. Alternate site determination to permit the storage and retrieval of information system backup information, along with establishing alternate telecommunications services to permit the resumption of essential missions and business functions within a defined period when primary telecommunications capabilities are unavailable.
3. Disaster recovery tests are conducted semi-annually
4. Tabletop exercises are conducted throughout the year with key State and non-State stakeholders through public-private partnerships. Lessons learned are documented and may require updates to the plan. Incident response plans and procedures are also validated during these exercises to ensure core security incident response team, responsibilities, incident reporting, escalation matrix, and notification procedures are current.

Cloud-hosted solutions undergo a third-party risk assessment, which includes a thorough review of vendor service level agreements (SLAs), disaster recovery tests, and business continuity plans. Availability is agreed upon in contractual language. Vendor incidents impacting availability of systems is formally tracked to ensure agreed-upon SLAs are met.

The strategic approach for improvement is to assess the capabilities of this element across the whole of Montana government and identify where gaps exist and identify the right tools that can be leveraged to benefit State, Local and K-12. Through collaboration with the members of the Committee, projects will be proposed to help address those gaps.

Workforce

State and Local Government Entities should develop cybersecurity workforce retention and recruiting policies to compete in a high demand / low supply cybersecurity workforce job market. A skilled and diverse cybersecurity workforce is key to protecting Montana businesses and citizens from global threats.

Montana has modified its job requests to better match skills. Employees have a training program that has both technical and non-technical training.

Montana also works to take a whole of state training plan working through a phishing and cyber awareness training and testing to assist in sending training to state entities and Local Governments or K-12 school districts to promote knowledge of all employees to be cyber smart and have the knowledge and information to understand how and what they should do when reacting to an event.

Montana also works through cybersecurity.mt.gov, Cyber406.org, CyberMontana.org websites to share trainings, security information, and other information to state citizens and employees alike. Every year the

website is updated to have links and information for National Cyber Security Awareness Month to highlight that year's key action steps and insights.

Continuity of Communications and Data Networks

State of Montana participates in an annual tabletop exercise with scenarios involving multiple industry sectors that include both State and Private entities. The tabletop exercise encourages continuity plans that extend beyond a single entity and to include items like alternative communication networks for major disasters.

State of Montana Continuity of Operations Plan contains these key elements:

1. Contact information for key stakeholders.
2. Mission Essential Functions:
    a. Provide IT hosting, network connectivity, telephone service, and online security to government entities.
    b. Provide software development services to government entities.
    c. Provide project management services to government entities.
    d. Provide records management services to government entities.
    e. Provide data center environment for state agencies.
3. Disaster Recovery Tiers defining recovery goals.
4. Incident response plan that addresses:
    a. Core security incident response team.
    b. Role's matrix identifying those responsible, accountable, consulted, and informed on incident response tasks.
    c. Incident reporting by staff or incidents detected and staff alerted by tools.
    d. Federal and State notifications.
    e. Continuous Improvement.

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

The approach to assess and mitigate cybersecurity risks and threats to critical infrastructure and key resources is to partner with various State and Local Government Entities to ensure that critical infrastructure and key resources across the state is identified and assessed. Any available training through the training investment as well as open-source training will be promoted and made available.

The state has made progress over the last few years including whole of government approach, new firewalls and edge devices, unification of state government, deployment of vulnerability analysis, increased deployment of XDR and cross functional teams to address high risk and emerging threats. A cyber risk management team helps to mitigate risks proactively by:

1. Implementing a third-party risk management program, which provides due diligence assessments of vendor security controls to ensure State citizen data is safeguarded.

2. Implementing NIST 800-37r2 Risk Management Framework for new systems, ensuring risk is assessed throughout the system development life cycle.
3. Creating internal audit functions to continuously monitor security controls and ensure control effectiveness.

Cyber Threat Indicator Information Sharing

The State of Montana Fusion Center (the MATIC) is the central information sharing hub for the state. The Montana Information Security Advisory Council is a public/private collaborative group that shares information and best practices.

Montana participates and shares indicators and threat information with instate partners. This information is used to bolster defenses and distribute information within Montana for the protection of the network and endpoints.

Montana CISO Office holds a weekly threat brief with all state and federal partners. We also work with CISA to understand threats and communicate what is allowable to our partners throughout the state.

Leverage CISA Services

The State of Montana and its various entities and committees utilizes services from CISA to assess and enhance their cybersecurity posture. The State encourages all State and Local Government Entities to utilize CISA and MS-ISAC free and low-cost services first, then build upon with additional layers of security.

Montana fully appreciates the help and support from CISA. Information provided through CISA is used to help bolster our defenses in preemptive blocking while also being used to help guide threat hunting, threat intelligence, and threat sharing throughout the state of Montana. Information from CISA is ingested through a multitude of ways from automatic playbooks, threat intelligence team and more.

As a condition of receiving SLCGP funding, the grant recipients will sign up for and maintain CISA's no cost Vulnerability Scanning(CyHy) and Web Application Scanning services as well as complete annually the no cost Nationwide Cybersecurity Review (NCSR) assessment administered by MS-ISAC. The NCSR is open to complete in October through late February, check with MS-ISAC on availably.

Information Technology and Operational Technology Modernization Review

Montana's SITSD team uses a project intake process to evaluate all new projects and their impact to informational and operational technology. During this review process, the project management, customer success, architects, and the security team are consulted before projects are initiated. Major projects receiving approval to proceed follow the NIST 800-37r2 Risk Management Framework process to ensure all aspects of risk, security, architectural review, and business are aligned, addressed, and assessed.

Cybersecurity Risk and Threat Strategies

The State of Montana Fusion Center (the MATIC) is the central information sharing hub for the state.

State of Montana conducts Cyber Assessments in coordination with all State of Montana entities. Based off the NIST, Cybersecurity Framework and the Nationwide Cybersecurity Review (NCSR) these questions assess each entity equally providing consistent insight into the entity and the State of Montana's overall cyber security posture. Assessment results are analyzed, and areas of common concern are identified in order to prioritize strategic efforts for making statewide improvements to network security.

Rural Communities

Because of the services provided approach to this plan, the Committee can ensure that all licenses and services are tracked and managed to make sure that rural areas are represented in the services provided and meet or exceed the 25% minimum.

More than 80% of Montana Counties are rural areas. With such a large makeup, rural communities are the core recipients of state cyber security tools and services.

Rural communities also have representation on the Committee.

FUNDING & SERVICES

The Committee intends to focus on 8 key efforts to strengthen cybersecurity across the State. These efforts include the goals and objectives section above and are detailed in Appendix B: Project Summary Worksheet. Sustainable funding is required to ensure that projects enabled by grant funding can continue to be successful. Funding sources can include local, state and federal organizations.

Distribution to Local Governments

To ensure 80% of the SLCGP funds are distributed to local units of government, it is the intent of the committee to have the Montana Department of Administration or the MT SLCGP State Administrative Agency (SAA), contract for services directly on behalf of local units of government with their consent. The SAA may issue direct subawards to local units of government based on the applications received and project prioritization by the committee. The SAA will ensure that 25% of the funds are directed to rural communities or utilized with their consent. All project applications must align with the projects listed in Appendix B.

As a condition of receiving SLCGP funding, the grant recipients will sign up for and maintain CISA's no cost Vulnerability Scanning(CyHy) and Web Application Scanning services as well as complete annually the no cost Nationwide Cybersecurity Review (NCSR) assessment administered by MS-ISAC. The NCSR is open to complete in October through late February, check with MS-ISAC on availably.

ASSESS CAPABILITIES

Montana's strategic approach will be to use the Nationwide Cybersecurity Review (NCSR) for annual assessments. NSCR is a free service from MS-ISAC and the question set is built off the NIST Cybersecurity Framework. Additional council approved NIST based assessments such as CISAs CPGs, CRE, CRR, CIS Controls, and various Vulnerability assessments will also be used as supplemental assessments to help further determine security current security posture.

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

The State Chief Information Officer is responsible for managing and protecting the State network. The State Chief Information Security Officer is responsible for advising and overseeing security strategy for Executive Branch agencies without elected officials; for advising and consulting security strategy for Executive Branch agencies with elected officials and the Judicial and Legislative Branches; and for advising security strategy for all other local and municipal governments in the state. Both the State CIO and the State CISO are members of the Montana Information Security Advisory Council (MT-ISAC).

The Montana Disaster and Emergency Services (MTDES) serves as the SAA for the State. The MTDES will manage and administer the financial and programmatic responsibilities of the program, whereas State CIO and the State CISO will serve in the role as project manager responsible for the Committee and their assigned roles and responsibilities under the approved committee charter and per the SLCGP requirements.

Resource Overview and Timeline Summary

The following information is provided to meet the requirement in the State and Local Cybersecurity Improvement Act: e.2.E. This information represents the best estimation based on current reference material. It is subject to revision over time.

When funding is approved, the first step is to develop a project plan. The project plan will be managed by State CIO and State CISO, MTDES, and the IIJA committee members. Project plan will outline scope, time and cost. The objective is to allocate and use funds within the allotted time provided via IIJA specifications. Depending on availability of resources, funding could be utilized over multiple years, not to exceed the guideline within the IIJA specifications. The guidelines will follow the item below:

- **People** – funding to be approved to hire appropriate contract staff to help the State & Local Governments and K-12 school districts implement projects agreed upon per year one.
- **Process** – MTDES will set up a process to allow State & Local Governments and K-12 school districts to request funding for the committee approved projects to be implemented in their areas. The funding amounts requested via projects will be voted on to be approved by the committee.
- **Technology** – Decision for technologies will be based on the decision by the committee. It is the intent of the committee to have the Montana Department of Administration or the MT SLCGP State Administrative Agency (SAA), contract for services directly on behalf of local units of government to aggregate requests and purchase in bulk for cost advantage.

Upon approval of the Plan and distribution of the funds, the key initiatives will begin.

METRICS

The below table should reflect the goals and objectives the Committee establishes.

State of Montana – Cybersecurity Program Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1. Asset Management	**1.1** Leverage the Montana Information Security Advisory Council (MT-ISAC) to create a workgroup focused on increased cybersecurity apprenticeships and internships opportunities in Montana (CSF ID.AM-6)	# of Workgroup meetings # of apprenticeships and internships # of entities using either apprenticeships and internships based off of program	Reports from State CISO office, MT-ISAC quarterly CSF ID.AM-6
2. Governance	**1.2** Leverage MT-ISAC for monthly sharing of cyber threat information and industry best practices to all Montana's Governments, Critical Infrastructure, and Small Businesses (CSF ID.GV-4)	# of meetings # in attendance # of individual entities	Reports from State CISO office, MT-ISAC quarterly CSF ID.GV-4
3. Risk Management Strategy	**1.3** Leverage MT-ISAC and industry best practices to support and standardize on NCSR as annual risk assessment. Additionally providing support for 3rd party on site standardized assessments as MT-ISAC determines per timeline determined. (CSF ID.RM-1) **1.4** Deliver support for State and Local governments and K-12 to move to .GOV domain for email and websites (CSF ID.RM-1) **1.5** Leverage MT-ISAC and industry best practices to create a standard naming convention for government entities moving to .GOV (CSF ID.RM-1)	- Completion of standardization of Risk Assessment and guidance % of State Agencies, Counties, Cities, K-12 that have taken NCSR - Gap numbers from annual Risk Assessment guidance # of State Agencies, Counties, Cities, K-12 that have taken 3rd Party Risk Assessments # of SLTT to move to .GOV % of State Agencies, Counties, Cities, on.GOV -Completion of Standard naming convention for MT SLTT entities moving to .GOV	Reports from State CISO office, MT-ISAC quarterly CSF ID.RM-1 Critical, High, Moderate, Low gaps identified from annual assessments. Source: NCSR, CISA Assessments (CPGs/CRE), CIS Controls or other approved by the Committee. Annual

4. Identity Management, Authentication and Access Control	**2.1** Leverage MT-ISAC to create a guideline or reference an established industry best practice on Multifactor Authentication with options to use current state services and contracts. Create an statewide action plan for funding improving the use. (CSF PR.AC-7, CIS Control 6.3, 6.4, 6.5) **2.2** Deliver solutions to Local Governments and K-12 to help protect network integrity with proper network segmentation (CSF PR.AC-5, CIS Control 12.2) **2.3** Leverage MT-ISAC to create a guideline or reference an established industry best practice on prohibiting use of known/fixed/ default passwords and credentials with options to use current state services and contracts (CSF PR.AC-1, CIS Control 4.7)	- Completion of guideline or industry best practice referenced on publicly accessible site on MFA. % of State Agencies, Counties, Cities, K-12 using MFA for remote access % of State Agencies, Counties, Cities, K-12 using MFA for accessing critical systems # of reviews of network for proper segmentation with documented guidance with roadmap to address - Completion of guideline or industry best practice referenced on publicly accessible site on prohibiting use of known/fixed/default passwords and credentials.	Reports from State CISO office, MT-ISAC quarterly CSF Controls PR.AC-1 & 5 & 7 CIS Controls 4.7 & 6.3 & 6.4 & 6.5 & 12.2 Annual assessments. Source: NCSR, CISA Assessments (CPGs/CRE), CIS Controls or other approved by the Committee. Annual
5. Awareness and Training	**2.4** Deliver basic end user security awareness training for Montana State & Local governments and K-12 (CSF PR-AT-1, CIS Control 14) **2.5** Deliver cyber education to privileged users and cyber professionals within Montana State & Local governments and K-12 (CSF PR-AT-2, CIS Control 14.9) **2.6** Deliver access for Montana State & Local governments and K-12 privileged users and cyber professionals to cyber ranges (CSF PR-AT-2, CIS Control 14.9)	# of State Agencies, Counties, Cities, K-12 taking annual security awareness training % of State Agencies, Counties, Cities, K-12 users fully completing annual security awareness training # of State Agencies, Counties, Cities, K-12 users taking cyber education # of State Agencies, Counties, Cities, K-12 users using cyber ranges for learning how to better defend their networks	Reports from State CISO office, MT-ISAC quarterly CSF PR-AT-1 & 2 CIS Control 14

6. Data Security	**2.7** Leverage MT-ISAC to create a guideline or reference an established industry best practice on encryption for data at rest and in transit with options to use current state services and contracts. Create a statewide action plan for funding improving the use. (CSF PR.DS-1 & 2, CIS Control 3.6 & 3.9 & 3.10 & 3.11)	- Completion of guideline or industry best practice referenced on encryption for data at rest and in transit. # of State Agencies, Counties, Cities, K-12 using fully using encryption at desktop # of State Agencies, Counties, Cities, K-12 using fully using encryption at server level	Reports from State CISO office, MT-ISAC quarterly CSF PR-DS-1 & 2 CIS Control 3.6 & 3.9 & 3.10 & 3.11 Annual assessments and reports. Source: NCSR, CISA Assessments (CPGs/CRE), CIS Controls or other approved by the Committee. Annual
7. Information Protection Processes and Procedures	**2.8** Leverage MT-ISAC to create a guideline or reference an established industry best practice on limiting use of unsupported/end of life (EOL) software and hardware and ending the use of EOL on systems that are accessible from the internet with options to use current state services and contracts. (CSF PR-IP-2, CIS Control 12.1 & 13.5 & 16.5) **2.9** Leverage MT-ISAC to create a guideline or reference an established industry best practice on backup and recovery with options to use current state services and contracts. Create a statewide action plan for funding improving the use. (CSF PR-IP-4, CIS Control 11)	- Completion of guideline or industry best practice referenced on limiting use of unsupported/end of life software and hardware. - Completion of guideline or industry best practice referenced on backup and recovery. # of State Agencies, Counties, Cities, K-12 having offline, encrypted backups of critical data % of State Agencies, Counties, Cities, K-12 having offline, encrypted backups of critical data # of State Agencies, Counties, Cities, K-12 using CISA Vulnerability Scanning Service % of State Agencies, Counties, Cities, K-12 using CISA Vulnerability scanning service	Reports from State CISO office, MT-ISAC quarterly CSF PR-IP-2 & 4 CIS Control 11 & 12.1 & 13.5 & 16.5 Annual assessments & Reports. Source: NCSR, CISA Assessments (CPGs/CRE/Vuln Scans), CIS Controls or other approved by the Committee. Annual

8. Protective Technology	**2.10** Leverage MT-ISAC to create a guideline or reference an established industry best practice on audit/log records with options to use current state services and contracts. Create an statewide action plan for funding improving the use. (CSF PR.PT-1, CIS Control 8)	- Completion of guideline or industry best practice referenced on audit/log records. # of State Agencies, Counties, Cities, K-12 using centralized logging server or SIEM tool % of State Agencies, Counties, Cities, K-12 using centralized logging server or SIEM tool	Reports from State CISO office, MT-ISAC quarterly CSF PR.PT-1 CIS Control 8 Annual assessments. Source: NCSR, CISA Assessments (CPGs/CRE), CIS Controls or other approved by the Committee. Annual
9. Anomalies and Events	**3.1** Deliver Network Monitoring and Management Intrusion Detection Systems (IDS) solutions for County Governments for additional layer of alerting and visibility for Election Offices, Emergency Services Offices, and Public Water System Municipalities. (CSF DE.CM-1, CIS Control 13.3) **3.2** Deliver support for State & Local governments and K-12 to utilize MS-ISAC's no cost Malicious Domain Blocking and Reporting (MDBR) service or similar service (CSF DE.CM-1 & PR.AC-5, CIS Control 9.2)	# of State Agencies, Counties, Cities, K-12 using MS-ISAC Albert Sensor or like service (determined by State CISO Office) % of State Agencies, Counties, Cities, K-12 using Albert Sensor or like service (determined by State CISO Office) # of State Agencies, Counties, Cities, K-12 using MS-ISAC MDBR or like service (determined by State CISO Office) % of State Agencies, Counties, Cities, K-12 using MDBR or like service (determined by State CISO Office)	Reports from State CISO office, MT-ISAC quarterly CSF DE.CM-1 & PR.AC-5 CIS Control 9.2 & 13.3 Annual assessments and reports. Source: NCSR, CISA Assessments (CPGs/CRE), CIS Controls or other approved by the Committee. Annual

10. Security Continuous Monitoring	**3.3** Deliver Endpoint Detection and Response solution for Montana Local Governments and K-12 (CSF DE.CM-4, CIS Control 10) **3.4** Deliver support for all State & Local governments and K-12 Schools Districts public facing IPs to have external vulnerability scanning with weekly report to entity. Create a statewide action plan for improving the use. (CSF DE.CM-8, CIS Control 7.6) **3.5** Deliver support for identified State & Local governments and K-12 School Districts to have internal vulnerability scan.	# and % of State Agencies, Counties, Cities, K-12 using a EDR solution that is approved by State CISO Office # and % of State Agencies, Counties, Cities, K-12 using CISA Vulnerability Scanning Service # and % of State Agencies, Counties, Cities, K-12 conducting at a minimum monthly Internal Vulnerability Scanning Service	Reports from State CISO office, MT-ISAC quarterly CSF DE.CM-4 & 8 CIS Control 7.6 & 10 Annual assessments & reports. Source: NCSR, CISA Assessments (CPGs/CRE/Vulnerability Scanning), CIS Controls or other approved by the Committee. Annual
11. Response Planning	**4.1** Leverage MT-ISAC and industry best practices to create a statewide incident response reporting process (CSF RS.RP-1 & PR.IP-9, CIS Control 17)	- Completion of guideline or industry best practice referenced on incident response reporting # of State Agencies, Counties, Cities, K-12 reported possible cyber incidents	Reports from State CISO office, MT-ISAC quarterly CSF RS.RP1 & PR.IP-9 CIS Control 17 Annual assessments. Source: NCSR, CISA Assessments (CPGs/CRE), CIS Controls or other approved by the Committee. Annual
12. Recovery Planning	**5.1** Leverage MT-ISAC and industry best practices by delivering training, workshops, exercises on incident response and recovery planning (CSF RC.RP-1 & PR.IP-10, CIS Control 17)	# of State Agencies, Counties, Cities, K-12 attending workshops or exercises on incident response and recovery planning % of State Agencies, Counties, Cities, K-12 attending workshops or exercises on incident response and recovery planning	Reports from State CISO office, MT-ISAC quarterly CSF RC.RP1 & PR.IP-10 CIS Control 17 Annual assessments, Reports. Source: NCSR, CISA Assessments (CPGs/CRE/Exercises), CIS Controls or other approved by the Committee. Annual

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY State of Montana				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Advanced		
2. Monitor, audit, and track network traffic and activity	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Advanced	8,	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Fundamental State - Advanced	1, 2, 3, 7	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	2, 3,	
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)			1	
a. Implement multi-factor authentication	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Advanced	1,	
b. Implement enhanced logging	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Advanced	1,	

c. Data encryption for data at rest and in transit	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	1,	
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	1,	
e. Prohibit use of known/fixed/default passwords and credentials	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	1,	
f. Ensure the ability to reconstitute systems (backups)	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	1,	
g. Migration to the .gov internet domain	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Fundamental State - Intermediary	5,	
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Fundamental State - Intermediary	1, 6	
7. Ensure continuity of operations including by conducting exercises	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Fundamental State - Intermediary	1,	
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Fundamental State - Intermediary	1, 4	
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Fundamental State - Intermediary	1, 7, 8	
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Fundamental	1, 2, 3,	

resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity				
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	1, 7, 8	
12. Leverage cybersecurity services offered by the Department	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Intermediary	1, 3	
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Fundamental	1, 2	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Local & K-12 Foundational State - Fundamental	1, 2, 3	
15. Ensure rural communities have adequate access to, and participation in plan activities	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Intermediary	1, 2	
16. Distribute funds, items, services, capabilities, or activities to local governments	State capability: Local and K-12 capabilities are unknown at this time, and will be determined via assessment	Intermediary	1,	

APPENDIX B: PROJECT SUMMARY WORKSHEET

Purpose: The Project Summary Worksheet is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in Appendix A: Sample Cybersecurity Plan Capabilities Assessment.

- Column 1. Project number assigned by the entity
- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Element the project addresses
- Column 5. Estimated project cost
- Column 6. Status of project (future, ongoing, complete)
- Column 7. Project priority listing (high, medium, low)
- Column 8. Project Type (Plan, Organize, Equip, Train, Exercise)

Column 1 Project #	Column 2. Project Name	Column 3. Project Description	Column 4. Related Required Element #	Column 5. Cost	Column 6. Status	Column 7. Priority	Column 8. Project Type
1	Whole of State Cyber Security Initiatives	Repurpose existing resources and/or hire additional resources to support the Committee and the Plan. This includes updating the Plan; and developing the Operations Plan, Communications Plan, and Organizational Change Management Plan to ensure state and local awareness and participation in Montana's whole-of-state projects. This also includes providing administrative tasks such as weekly website updates, monthly meetings, meeting minutes, support outreach program, promotional materials, exercises (to include workshops, meetings, and logistics) and initiatives as outlined in the Plan objectives. Educate on the Plan and market services already offered by State, MT National Guard, CISA, MS-ISAC. Includes two half time staff for management of activities and meetings.	3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	$125,000 FY23 adjust as needed. In FY24 and budget for 2 additional years.	future	High	Plan
2	Perform security strategic assessments	Provide support to all State, Local and Tribal Governments and K-12 School Districts for completing NCSR, help with interpreting reporting, and to develop a plan based from assessment.	3, 4, 10, 13, 14, 15	$25,000 for FY23. In FY24 and budget for 2 additional years.	Future	High	Organize

3	Perform security technical assessments	Provide support for signing up for CISA's free external Vulnerability Scans and interpreting the results. Provide support for signing up for MS-ISAC Malicious Domain Blocking and Reporting (MDBR) service. Provide support for additional technical assessments based on strategic plans and risk to State.	3, 4, 10, 12, 14	$25,000 for FY23. In FY24 and budget for 2 additional years.	Future	medium	Exercise
4	Build security awareness	Provide support to all State, Local and Tribal Governments and K-12 School Districts by offering basic end user security awareness training to their employees	8	$165,000 for FY23. In FY24 and budget for 2 additional years.	ongoing	High	Train
5	Migrate to .GOV domains	Provides support to all SLTT entities for migrating their domain to .GOV	5g, 6	$25,000 for FY23. In FY24 and budget for 2 additional years.	Future	Medium	Organize
6	Build a cybersecurity workforce	Provides support via MT-ISAC to all entities for implementing NICE Workforce Framework practices for Cybersecurity. Provide cyber education and access to cyber ranges to IT privileged users and cyber professionals	8	$50,000 for FY23. In FY24 and budget for 2 additional years.	Future	Medium	Organize & Train
7	Server and Workstation Behavior-based Endpoint Protection	Provide behavior-based endpoint detection and response solution for servers and workstations to Montana Local Governments and K-12 school districts	3, 9, 11	1,425,000 for FY23. In FY24 and budget for 2 additional years.	Future	Medium	Equipment
8	Network Monitoring and Management Intrusion Detection Systems for County Networks	Provide Network Monitoring and Management Intrusion Detection Systems for additional layer of alerting and visibility to County Governments for Election and Emergency Service, and Public Water System Municipalities. Review success and look into expanding into Cities, Towns, K-12.	2, 9, 11	$560,000 for FY23. In FY24 and budget for 2 additional years.	Future	Medium	Equipment