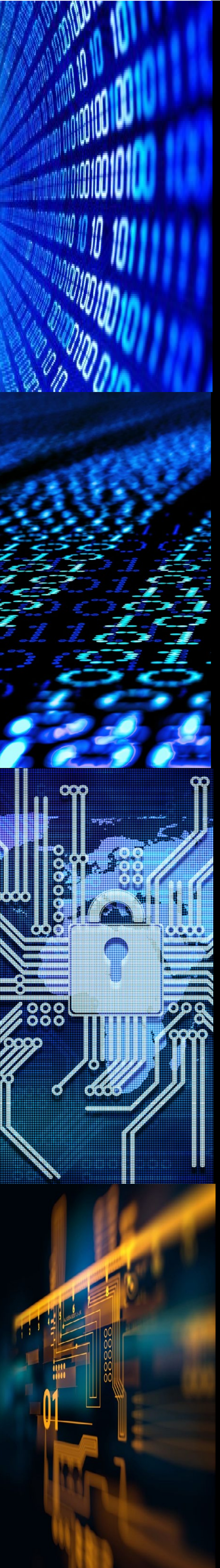


OREGON CYBERSECURITY PLAN

2023

Approved by State of Oregon Planning Committee on 7/31/23

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

Letter from Oregon Planning Committee 1

Introduction 2

Vision, Mission, and Values 4

Cybersecurity Strategic Plan Goals, Objectives, and Actionable Items 5

Strategic Goal 1: Cybersecurity Governance 5

Strategic Goal 2: Risk Management 6

Strategic Goal 3: Mature Cybersecurity Capabilities 7

Strategic Goal 4: Build a Culture of Cyber Awareness 8

Strategic Goal 5: Prepare and Plan for Cyber Incidents 9

Strategic Goal 6: Collaborate and Share Information 9

Strategic Goal 7: Build a Cyber Workforce 9

Cybersecurity Plan Elements 11

Manage, Monitor, and Track 11

Monitor, Audit, and Track 11

Enhance Preparedness 12

Assessment and Mitigation 12

Best Practices and Methodologies 12

Safe Online Services 13

Continuity of Operations 13

Workforce 13

Continuity of Communications and Data Networks 14

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources 14

Cyber Threat Indicator Information Sharing 14

Leverage CISA Services 14

Information Technology and Operational Technology Modernization Review 14

Cybersecurity Risk and Threat Strategies 15

Rural Communities 15

Funding & Services 16

Distribution to Local Governments 16

Assess Capabilities 16

Implementation Plan 16

Organization, Roles and Responsibilities ... 17
Resource Overview and Timeline Summary ... 17
SLCGP Goals ... 20
SLCGP Objectives ... 20
Associated Metric ... 20
Metric Description ... 20
Success Factors ... 22
Appendix A: SAMPLE Cybersecurity Plan Capabilities Assessment ... 23
Appendix B: Project Summary Worksheet ... 27
Appendix C: Service Catalog ... 30
Appendix D: CIS and MS-ISAC Offerings ... 35
Appendix E: Roadmap ... 37
Appendix F: Implementation Timeline ... 38
Appendix G: Draft Project Application ... 39

LETTER FROM OREGON PLANNING COMMITTEE

Greetings,

The Cybersecurity Planning Committee for Oregon is pleased to present to you with the 2022-2027 state Cybersecurity Plan. The Cybersecurity Plan represents the State of Oregon’s continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, the plan meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from cities, counties, special districts, rural, urban, and suburban; public schools; public health; public safety; and critical infrastructure are members of Oregon’s SLCGP Planning Committee and collaborated to develop Oregon’s Cybersecurity Plan with actionable goals and objectives to ensure successful implementation. These goals and objectives focus on leveraging economies of scale, utilizing no cost and low-cost services and programs, to implement sustainable solutions that enhance cyber security posture of Oregon. They also incorporate the SLCGP required plan elements.

Oregon will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Sincerely,

Ben Gherezgiher

Ben Gherezgiher, Committee Chair

Chief Information Security Officer

State of Oregon

Enterprise Information Services

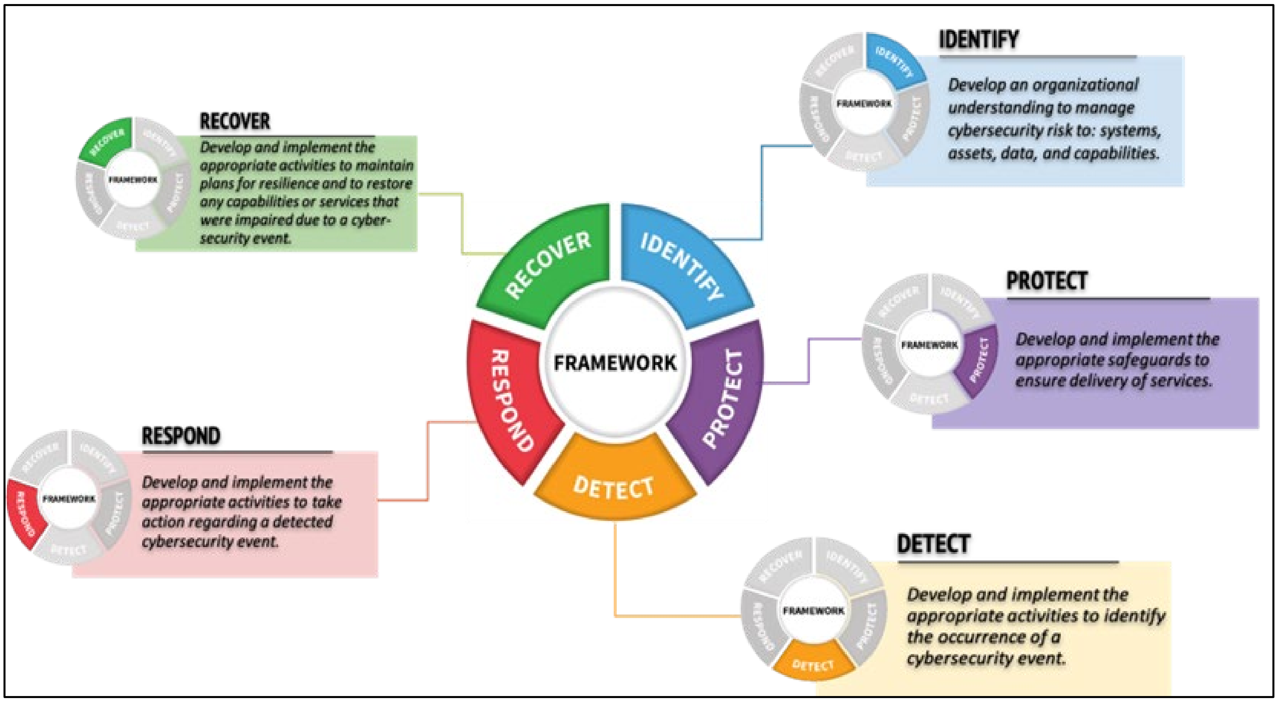
INTRODUCTION

The Cybersecurity Plan is a five-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 five years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within Oregon 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 Oregon cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of Oregon or 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.
- **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 Oregon along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes Oregon’s plan to implement, maintain, and update the Cybersecurity Plan to enable the continued evolution of, and progress toward, the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how Oregon 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, 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.

- **Identify**: Identify cybersecurity risk management measures and risk management processes to reduce cybersecurity risks across the enterprise.
- **Protect**: Develop and implement enterprise safeguards to reduce risk and increase awareness and resiliency.
- **Detect**: Develop tools and processes to accelerate notification of cybersecurity threats, defeat threat actors before they have impact on state information assets.
- **Respond**: Consistently respond to anomalies and suspected events.
- **Recover:** Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.


FRAMEWORK
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.
IDENTIFY
Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities.
PROTECT
Develop and implement the appropriate safeguards to ensure delivery of services.
RESPOND
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
DETECT
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Vision, Mission, and Values

Vision:

A cyber safe, secure, and resilient Oregon.

Mission:

Protect Oregon by collaborative development and implementation of solutions and best practice to cybersecurity challenges.

Core Values:

Service:

We put Oregon and its citizens first, to ensure a cyber safe, secure, and resilient environment. We aim to be timely, supportive, and current.

Teamwork:

We recognize that a mission cannot be upheld alone, and value our partners, both internal and external, who help us to uphold our mission and vision.

Excellence:

We take pride in the work we do to better Oregon. We work to do every task, project, initiative, and service to the best of our ability and for the betterment of our state.

Diversity:

We strive to build a workforce that is diverse and inclusive. We encourage our workforce to have diversity of thought, perspective, and problem solving so that all voices are heard.

Integrity:

We hold ourselves accountable to the highest ethical and moral standards in both our personal and professional conduct. We will act with honor and truthfulness in all situations. We take great pride in our stewardship and fiscal responsibility of grant funds.

Cybersecurity Strategic Plan Goals, Objectives, and Actionable Items

This strategic cybersecurity plan embodies a pathway to reaching improved cyber resilience through a set of interconnected goals, objectives, and actionable items, that will help Oregon protect our institutions, businesses, and individuals. This plan outlines statewide goals and objectives set to be pertinent to all public and private sector institutions and individuals, as well as those specifically tailored for public entities. These goals, objectives, and actionable items will be addressed in years two through five of the grant programs, and as progress is achieved, this plan will be revised and resubmitted to reflect the updated objectives in years three through five.

Strategic Goal 1: Cybersecurity Governance

Objective 1.1: *Establish, implement, and maintain management frameworks that promote and oversee the implementation of security controls and the performance of information security within Oregon state and local government organizations.*

Action Items:

- Establish management structures and roles along with their associated authorities and responsibilities for centrally managing, coordinating, developing, implementing, and maintaining the organization's cybersecurity program.
- Develop and implement trainings and workshops aimed at developing cybersecurity program managers.
- Develop and coordinate strategies to identify and address cybersecurity risks and cybersecurity threats.
- Establish and institutionalize contacts with relevant groups and associations within the security and privacy communities, including law enforcement authorities, state and federal cybersecurity organizations, information sharing and analysis organizations and centers, incident response service providers, information security professional organizations, information technology and telecommunications service providers, and others as necessary to protect organizational information assets.
- Institute continuous improvement to the Statewide Information and Cyber Security Standards as well as implement and improve policies, processes, standards, and technologies necessary to meeting cybersecurity standards for systems and program maturity.

Objective 1.2: *Establish a risk–based approach to information security while establishing the required behaviors and controls necessary to protect information technology resources, secure personal information, safeguard privacy, and maintain the physical safety of individuals.*

Action Items:

- Adopt and implement information security programs at the state and local government levels that reasonably conform to an applicable industry-recognized cybersecurity framework such as the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of

Standards and Technology (NIST), the Center for Internet Security (CIS) Critical Security Controls (CSC) for Effective Cyber Defense, etc., that contain prioritized sets of best practices to help defend against the most pervasive and dangerous cyber threats.

- Implement policies and standards to securely protect organizational information and information systems while maintaining compliance with applicable statutory and regulatory requirements pertaining to confidentiality, integrity, availability, privacy, and safety.
- Implement administrative, technical, and physical controls necessary to safeguard information assets in all their forms from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate, or accidental.
- Establish procedures and implement tools and technologies to identify and maintain an accurate inventory of all organizationally owned, leased, licensed, or managed information assets.
- Establish processes to categorize assets and information according to their sensitivity and criticality and require that protection mechanisms be implemented commensurate with the impact should there be a loss of confidentiality, integrity, or availability of the asset or information.

Strategic Goal 2: Risk Management

Objective 2.1: *Develop and implement a cybersecurity risk management program.*

Action Items:

- Build the necessary structures and processes to identify, assess, and mitigate cyber risks within and across Oregon state and local government organizations.
- Implement continuous risk management processes and tools that account for the identification, assessment, and treatment of risks that can adversely impact state and local government operations, information, or information systems.
- Develop and grow the capability to conduct cybersecurity surveys and assessments of systems connected to or sharing data with Oregon public-sector cybersecurity programs and systems.
- Develop statewide and individual organization capabilities to continually test state and local government networks, systems, and applications to identify vulnerabilities, gaps in cyber defenses, and configuration weaknesses.

Objective 2.2: *Measure, assess and mitigate cyber risk and threats which may degrade or impact information systems within Oregon.*

Action Items:

- Establish uniformity of cybersecurity framework, controls, technologies, and procedures across state government, and give guidance to other public entities so they may follow suit.
- Increase coordination and collaboration between federal, state, and local government for cybersecurity incident handling, including emergency management entities and critical infrastructure.
- Routinely test state networks, systems, applications, and other connected systems to identify vulnerabilities, gaps, and threats.
- Identify, 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.

- Continually assess state and local government networks, systems, and applications to identify vulnerabilities, misconfigurations, gaps in cyber defenses, and emerging threats and prioritize remediation efforts and resources based on risk.

Objective 2.3: *Drive improvements to Oregon's cybersecurity posture.*

Action Items:

- Support, promote, and utilize Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) risk and vulnerability services.
- Support, promote, and utilize the Multi-State Information Sharing and Analysis Center's (MS-ISAC) National Cyber Security Review (NCSR) service.
- Support, promote, and utilize CISA's Cross Sector Cybersecurity Performance Goals to evaluate and establish baseline configurations for IT and OT systems.
- Support, promote, and utilize CISA's Known Exploited Vulnerabilities Catalog in prioritizing patching decisions.
- Support, promote, and utilize the Multi-State Information Sharing and Analysis Center's (MS-ISAC) National Cyber Security Review (NCSR) service.
- Support the use of and engage independent third parties to review and assess the appropriateness of the cybersecurity programs and controls that safeguard state and local government organizations and their networks and systems.
- Lead and support efforts to modernize and harden state and local government information and operational technology infrastructure, prioritizing updates and upgrades of software and hardware including end-of-life software. Develop and produce cybersecurity progress reports to key stakeholders that identify trends, risks, emerging threats, and key performance indicators.

Strategic Goal 3: Mature Cybersecurity Capabilities

Objective 3.1: *Enhance public sector entities incident reporting capabilities.*

Action Items:

- Ensure that cybersecurity best practices, standards, and frameworks are available to state, city, county, and special districts.
- Prioritized cybersecurity investments are risk-based and provide up-to-date protection for the most critical and sensitive assets.
- Refine our Incident Response Plan to include defined methodology and individual playbooks necessary to ensure that incident responses are constant.

Objective 3.2: *Promote delivery of safe, recognizable, and trusted online services, including the use of .gov domain.*

Action Items:

- Leverage existing relationships to create a state-wide cyber contact network that can be used to reach out to other public entities and begin working on risk assessments of the 18 Center for Internet Security Critical Security Controls, which will address critical items such as: MFA, logging, encryption, unsupported and unpatched software, password management, and offline backups.

- Assist organizations with best practices when they are asked to move to a .gov domain.

- Encourage all organizations to join MS-ISAC, as their joining will help expand the state-wide cyber contact network.

Objective 3.3: *Enhance preparation, response and resilience of information systems, applications, and user accounts against cyber risk and threats.*

Action Items:

- Offer direct and indirect support to state and local entities in implementing cybersecurity best practices.

- Increase security posture for Oregon's remote workforce environment.

- Research, obtain, deploy, and monitor effective detective and preventative security services and technologies.

Strategic Goal 4: Build a Culture of Cyber Awareness

Objective 4.1: *Create and extend access to public sector entities for awareness-level training.*

Action Items:

- Implement cybersecurity trainings for state and local entities.

- Create and distribute relevant security awareness materials, alerts, and advisories, and notify key stakeholders of new or updated statutes, regulatory requirements, and policies.

Objective 4.2: *Provide outreach avenues for sharing free and low-cost resources.*

Action Items:

- Enable and encourage local governments access to free and low-cost offerings for cybersecurity services, see Appendix D for details.

Strategic Goal 5: Prepare and Plan for Cyber Incidents

Objective 5.1: *Encourage incident reporting through the MS-ISAC Security Operations Center.*

Action Items:

- Ensure that state and local entities are aware of the resources provided by MS-ISAC, see Appendix D for details.

Objective 5.2: *Improve capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity.*

Action Items:

- Initiate regular cybersecurity exercises to increase and improve the ability of public sector organizations to detect and mitigate risks.
- Provide and encourage state cybersecurity employees with opportunities and resources to continually advance and progress their knowledge, skills, and abilities that are required to stay current with evolving cybersecurity challenges.
- Create and grow the ability to conduct cybersecurity surveys and assessments of public and private sector cybersecurity systems.
- Develop and implement a supply chain cybersecurity baseline that establishes requirements for vendors and institutes an assessment platform for security due diligence to be standardized and reported.

Strategic Goal 6: Collaborate and Share Information

Objective 6.1: *Create a collaborative environment to share, identify, and evaluate information for members to discuss threats and vulnerabilities impacting Oregon.*

Action Items:

- Establish and improve engagement programs and partnerships with public and private sector organizations, Information Sharing Analysis Centers and Organizations (e.g., MS-ISAC), as well as other non-government cybersecurity organizations.
- Foster partnerships with federal, state, local, and Oregon National Guard to increase collaboration and communication, and improve the capability and capacity to respond and prevent cyberattacks.
- Attend and participate in industry and government conferences and events as a cybersecurity subject matter expert.

Strategic Goal 7: Build a Cyber Workforce

Objective 7.1: *Provide tailored security training for public sector entities to improve and mature their cybersecurity posture.*

Action Items:

- Support and establish cybersecurity training and education programs for professional development and ensuring access for the current staff.

- Develop and provide current and pertinent cybersecurity news, updates, and information to staff to encourage awareness of the current cybersecurity climate.

Objective 7.2: *Build a network of cyber contacts across Oregon.*

Action Items:

- Integrate public and private sector cyber defense and response efforts to enhance the knowledge base of activity within the state.
- Create and incorporate platforms or web portals for cybersecurity communications and information sharing within the state and local government.

CYBERSECURITY PLAN ELEMENTS

This plan incorporates the following plans:

State of Oregon Enterprise Information Services Strategic Framework 2023-2026 This strategy establishes a framework for advancing the State of Oregon's mission through the collaborative development and adoption of enterprise-wide cybersecurity policies matched by prioritized risk management-based implementation of cybersecurity defenses.

Oregon Cyber Disruption Response and Recovery (OCDR) - Voluntary Resource Guide for Local Government – This Guide provides a common framework for responding to cyber threats impacting Oregon government and enables all levels of Oregon government to rapidly coordinate a cyber disruption response, minimizing the impact in Oregon.

State of Oregon Information Security Incident Response Plan – This Plan guides response to information security incidents. This plan is built on the premises that incidents vary in severity and require a flexible scale of response efforts to mitigate, and that response efforts must be adequate, uniform and coordinated regardless of the size.

Manage, Monitor, and Track

At the State and Local Government levels, organizations should establish procedures that effectively control and restrict access to information assets to authorized users based on need-to-know. Access is defined by business, legal, regulatory, and compliance requirements. Controls must be implemented for protection of information assets. The State Executive Branch sets policies and IT Control Standards that document the minimum baseline requirements for state agencies and is available for use by other branches of State Government and Local Government entities.

Organizations should:

1. Establish a representative or governing body accountable and appropriately resources with authority over the management of information assets.
2. Ensure the information assets under their purview are assessed for security risks and configured such that event logging is enabled to ensure an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, and availability of agency information and information systems are identified and managed; and
3. Review and retain event logs in compliance with all applicable Local, State and Federal laws, regulations, executive orders, circulars, directives, internal agency and State of Oregon policies, and contractual requirements.

Monitor, Audit, and Track

Monitoring, auditing, and tracking of network traffic will be strengthened by increasing the visibility at multiple local levels. The state and county partners have deployed Albert Sensors in 32 of Oregon's 36 counties. Increasing the number of counties and expanding the public-sector to include more local governments utilizing Albert Sensors will increase the ability to monitor, audit, and track network traffic.

Enhance Preparedness

State and Local Government organizations 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 and Continuity of Operations Plans. Lessons Learned from these exercises will be incorporated into future planning, inform organizational decisions, and demonstrate additional equipment and training needs.

The State regularly conducts exercises and participates in Local Government and other partner cyber exercises.

Assessment and Mitigation

All major systems and applications, and general support systems operated by or on behalf of State and Local Government organizations should undergo security assessments to ensure adequate security controls. Executive Branch State agencies are assessed against the CIS top 18 controls every 2 years. Local governments are encouraged to adopt this approach.

Implementing a process of continuous cybersecurity vulnerability assessment and threat mitigation practices prioritized by degree of risk will be addressed by increasing outreach with Local Governments. By increasing outreach, it creates more awareness and access to the resources provided by CISA, CIS/MS-ISAC, and State Government. Threat mitigation will be addressed by increasing access to facilitated self-assessments that will help local entities determine their risk level and provide guidance on which CIS top 18 controls are appropriate for that specific entity, creating a more customizable and tailored approach to each specific entity’s needs.

Best Practices and Methodologies

The approach for adopting and using best practices and methodologies to enhance cybersecurity will be accomplished through outreach to Local Governments. By tapping into established relationships, the SLCGP will be able to create, and foster a collaborative state-wide cyber contact network, and can begin to reach out to other public-sector entities to work on risk assessments of the CIS Top 18 controls which addresses MFA, logging, encryption, unsupported and unpatched software, password management, and offline backups. The CIS controls map to the NIST cybersecurity framework, and the State of Oregon already has contracts in place that are available to Local Government to access these types of assessments. This also gives the opportunity to point Local Government to the free and low-cost offerings for cybersecurity services. All organizations will be asked to move to a .gov email address and encouraged to join to MS-ISAC which will help build the cyber contact network addressed earlier in this plan.

State Government has established IT Control Standards which align to NIST 800-53 Revision 5 Moderate Controls and map to the NIST cybersecurity framework. The standards are a baseline for all Executive Branch State Government agencies. State Government has various legal, regulatory, and contractual compliance requirements based on their business services and operations, and the information they collect, store, process, and transmit. State Government agencies must implement controls to meet all compliance requirements. Some commonly applicable statutory and regulatory requirements include IRS Publication 1075, Safeguards for Protecting Federal Tax Returns and Return Information (FTI), Health Insurance Portability and Accountability Act (HIPAA), Minimum Acceptable Risk Standards for Exchanges, version 2.0 (MARS-E), Family Education Rights Privacy Act (FERPA), Payment Card Industry – Data Security Standards (PCI-DSS), and Criminal Justice Information Services (CJIS.)

At the Local Government level, controls are implemented based on differing frameworks such as NIST or the CIS Top 18 controls. Local Government also have various legal, regulatory, and contractual compliance requirements based on their business services and operations, and the information they collect, store, process, and transmit. Regardless of the framework, the following best practices are included and projects to implement will be considered over the life of the SLCGP: (a) implementation of multi-factor authentication, (b) implementation of enhanced logging, (c) encryption for data at rest and in transit, (d) eliminating use of unsupported/end of life software and hardware that are accessible from the Internet, (e) prohibition of use of known/fixed/default passwords and credentials, and (f) enabling the ability to reconstitute systems (backups).

NIST Principles

A detailed description of the application of NIST Principles and the CIS Critical Security Controls is provided in the preceding paragraph.

Supply Chain Risk Management

State Government requires third parties that do business with the State of Oregon Executive Branch to implement NIST 800-53r5 Moderate Controls that align with the State IT Control Standards. All State IT Investments must follow an IT Governance Framework which includes oversight and portfolio management of all major IT investments as well as cybersecurity vetting. All IT contracts include cybersecurity terms and conditions. Procurement of products and services under the SLCGP will be achieved through Executive Branch Processes.

Tools and Tactics

Local Government is encouraged to join to MS-ISAC and engage with CISA to gain access to knowledge bases of adversary tools and tactics to improve your cybersecurity efforts.

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. See the Projects Summary Worksheet in Appendix B for details.

Continuity of Operations

State and Local Government organizations 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 on behalf of State Government or their respective Local Government organization. Contingency planning is an important aspect of risk management. Ensuring availability of 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.

Lessons learned from exercises will be incorporated into future planning, inform organizational decisions, and demonstrate additional equipment and training needs.

Workforce

Workforce recruitment and retention is a well-documented problem across the Nation in both the Public and Private Sector. The National Initiative for Cybersecurity Education (NICE) Workforce Framework will be utilized to identify and mitigate any gaps in the cybersecurity workforce across the State. SLCGP will provide more access to training for Local Government. The training will come from various sources that map to the NICE

Workforce Framework. The delivery of the course will vary and could range from online training platforms to in-person trainings.

Continuity of Communications and Data Networks

The State of Oregon has partnered with CISA to conduct a Regional Resiliency Assessment Program (RRAP) of the State's IT infrastructure to include telephony-based communications applications, network security architecture, network backbone, cloud connectivity, remote data center architecture, emergency response capacity supporting selected executive agencies residing in the State Data Center and critical agencies that are not located in the state data center. Continuity of communication and data networks will be addressed once the RRAP is complete.

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

State and Local Government organizations should assess and mitigate cybersecurity risks and threats to Critical Infrastructure and Key Resources (CIKR). SLCGP will foster partnerships with Oregon Department of Emergency Management and Oregon TITAN Fusion Center to ensure that CIKR is identified across the state. Trainings through the training investment, as well as open-source training, will be promoted and made available to local entities.

Cyber Threat Indicator Information Sharing

Department Agreements

State Government, in coordination with the MS-ISAC and CISA monitor information from a variety of open and classified sources, analyzes that information, and distributes information across State and Local Government organizations. The SLCGP will explore avenues to expand information sharing including the potential for establishing a Federated Security Operations Center (SOC). Benefits of a Federate SOC at a minimum would be: 1) small organizations would benefit from larger organizations, 2) organizations would see different types of malicious activity and be able to better prepare and plan, 3) organizations would be able to leverage federated resources in the event of a cyber incident.

Leverage CISA Services

The State has established partnerships and existing networks in the State to leverage the cybersecurity services that are offered by CISA. Many Local Government entities also take advantage of cybersecurity services offered by CISA. This should continue and expand in the future. The Local/Regional CISA representative is very collaborative and accessible to State and Local Government organizations and routinely coordinates other associations and entities across the State. Additionally, the SLCGP recipients should enroll in Vulnerability Scanning and Web-Application Scanning as appropriate.

Information Technology and Operational Technology Modernization Review

Alignment of controls for information technology and operational technology cybersecurity objectives is necessary. Cybersecurity must include systems that process data and those that ensure safety. SLCGP participants may replace end of life/outdated equipment if equipment purchases are approved by the SLCGP Planning Committee at some point in the future. This is not addressed in year one or two of the grant.

Cybersecurity Risk and Threat Strategies

The SLCGP Planning Committee should use this plan and operate under their approved charter to develop and coordinate strategies and projects to address cybersecurity risks and cybersecurity threats with other organizations, including consultation with Local Governments and associations of Local Governments. The SLCGP Planning Committee will coordinate with MS-ISAC on best practices, and to use the CIS top 18 controls to scale various implementation efforts to best suit the local entities based on size and ability and help them mature at a sustainable pace.

Rural Communities

Rural communities are assured adequate access to projects under the SLCGP by virtue of their representation on the SLCGP planning committee and outreach activities that will be done by the Planning Committee as a whole and individual members of the Planning Committee. The SLCGP Planning Committee will 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.

FUNDING & SERVICES

The SLCGP initiatives will leverage existing state programs as well as Homeland Security investments to help local governments mature their cybersecurity efforts. The initiatives invested in will give the most value to entities with the limited amount of funds available.

Understanding the current cybersecurity posture for State and Local Government and areas for improvement based on assessments, testing, and evaluations will be an initial initiative. Providing resources for these services to Local Government will provide quantifiable data for decision making, alignment of services, and a clearer assessment of risk to Oregon.

The framework used to allocate funds equitably will be to prioritize awards to sub-applicants by their correlation to the tiers laid out in the service catalog, with priority going to tier one service. Sub-applicants will also be informed that funds distributed are to be seen as a one-time grant, and sustainability of the service going forward will need to be accounted for in their proposals. Sub-applicants will have the ability to re-apply for funds in later years of the grant program, but priority will be given to first time sub-applicants.

Distribution to Local Governments

The grant will be used for the benefit of local governments and distributed as services available to the local entities. The State Administrative Agency (SAA) will retain 5% of the grant for management and administration. SLCGP projects will be monitored to ensure that 25% of cybersecurity grant funding goes to rural areas.

ASSESS CAPABILITIES

Assessing cybersecurity maturity and capabilities at the Local Government level is a challenge. The challenge is complex and varies by the number who participate, their resources, and maturity level. Some organizations may choose not to participate due to lack of trust to share information, adding to the complexity and challenge of forming a comprehensive representation of Oregon.

State Government Executive Branch agencies are assessed against the CIS top 18 controls every 2 years per statute.

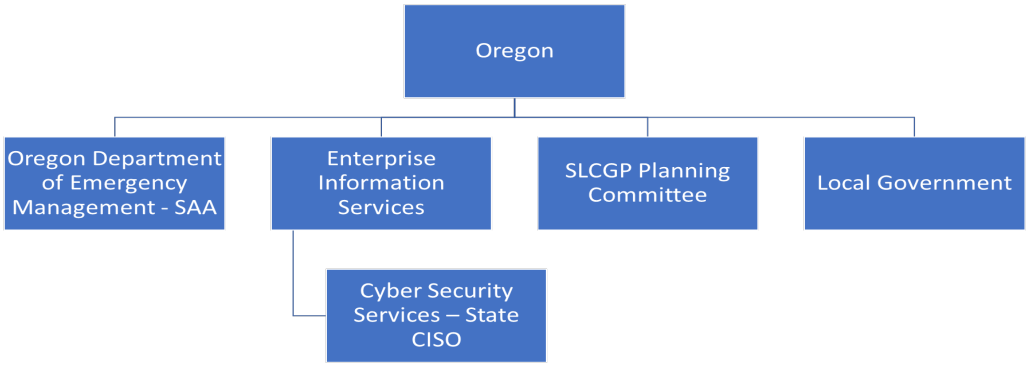
Increasing outreach to Local Government will increase access to CISA and CIS/MS-ISAC assessment resources. Increasing access to facilitated self-assessments will help Local Government organizations determine their capabilities and provide guidance on best practices.

IMPLEMENTATION PLAN

Implementing the SLCGP Cybersecurity Plan has multiple facets and relies on multiple organizations. Once the plan is submitted for approval, vendors and procurement pathways need to be established in accordance with the service catalog, and different offerings may be available through multiple sources e.g., private vendors, CISA, etc. Once the procurement methods have been determined, sub-applicants can start submitting proposals. Sub-applicants will need to be an Oregon Cooperative Procurement Program (ORCPP) member to procure off of State contracts but are not limited to use only State-contracts. The proposals will be reviewed internally by a sub-committee formed out of the SLCGP Planning Committee, having members review proposals from their governmental body, e.g., members from cities would review proposals from cities, members from counties would review proposals from counties, unless the proposal is from their organization, in which case they would be asked to recuse themselves from that review. Reviewed proposals will then be brought back to the SLCGP Planning Committee for consensus, and prioritization in accordance with the service tiers laid out in the service catalog. The funds are meant to be a one-time opportunity, not a year-over-year funding opportunity.

Organization, Roles and Responsibilities

The implementation of the SLCGP Cybersecurity Plan depends on multiple organizations. Each organization has a role in carrying out the cybersecurity plan and associated responsibilities.


Oregon
Oregon Department of Emergency Management - SAA
Enterprise Information Services
SLCGP Planning Committee
Local Government
Cyber Security Services – State CISO

The Oregon Department of Emergency Management (ODEM) is the State Administrative Agency (SAA) for Oregon. ODEM is the SLCGP grant administrator and will be responsible for ensuring grant management processes.

Enterprise Information Services through Cyber Security Service (CSS) is the SLCGP program administrator for Oregon. The State Chief Information Security Officer (CISO) is the chair of the SLCGP Planning Committee and leads the SLCGP program administration.

The SLCGP Planning Committee is chartered to provide strategic guidance and recommendations to EIS to inform and support the development and implementation of the Oregon Cybersecurity Plan. They will approve the Cybersecurity Plan before submitting for CISA/FEMA approval.

Local Government is the beneficiaries of the SLCGP Plan projects. Their role is to partner with the SLCGP Planning Committee to mature Oregon's cybersecurity posture.

Resource Overview and Timeline Summary

Below is an overview of the resources and projected timeline needed to implement the projects proposed

in Appendix B: Project Summary Worksheet.

#	Gov. Entity	Gov. Entity Type	Location Type	Representative Name	Title	Role

1	EIS-CSS	State	N/A	Ben Gherezgiher	State CISO, Chair	IT, Cyber
2	Multnomah County	County	Urban	Dennis Tomlin	CISO	IT, Cyber
3	Portland Public Schools	Public Education	Urban	Derrick Brown	Sr. Director of Technology	IT, Cyber
4	Special Districts Association of Oregon	Special District	Rural	Frank Stratton	Executive Director	IT, Cyber, Business
5	Lane Council of Governments	Regional Government	Urban, Rural	Heidi Leyba	CTO	IT, Cyber, Business
6	Klamath County	County	Urban, Rural	Jessica Chastain	IT Director	IT, Cyber
7	DHSOHA	State, Public Health	N/A	Kathryn Kopania	Preparedness Field Assignee	Business
8	City of Grants Pass	City	Rural	Ken Selland	IT Manager	IT
9	Clackamas County	County	Urban	Kevin Galusha	Security Advisor	Cyber
10	Medford Water Commission	Special District - Water	Urban/Rural	Kris Stitt	IT Manager	IT
11	Jackson County	County	Urban, Rural	Mark Decker	Technology Director and CISO	IT, Cyber
12	Linn Benton Lincoln Education Service District	Special District, Public Education	Urban	Richard Thomas	Security Engineer	Cyber
13	OEM	State	N/A	Sarah Puls	Emergency Preparedness Planner	Business
14	City of Albany	City	Urban	Sean Park	CIO	IT, Cyber
15	City of Happy Valley	City	Urban	Will Wilson	IS Manager	IT, Cyber

	Gov. Entity	Support Staff Name	Title
1	EIS-CSS	Cinnamon Albin	Interim Deputy State CISO
2	EIS -CSS	Sherri Yoakum	Business Enablement Manager
3	EIS-CSS	Bryan Decker	Business Security Advisor
4	EIS-CSS	Mariah O'Seanecy	Business Security Advisor
5	EIS-PMO	Nychal McClain	Project Manager

SLCGP Goals	SLCGP Objectives	Associated Metric	Metric Description
Cybersecurity Governance	Establish, implement, and maintain management frameworks that promote and oversee the implementation of security controls and the performance of information security within Oregon state and local government organizations. Establish a risk–based approach to information security while establishing the required behaviors and controls necessary to protect information technology resources, secure personal information, safeguard privacy, and maintain the physical safety of individuals.	• Approved signed Governance charter • Percent of Planning Committee members attending monthly meetings • Decision log and meeting minutes	Member Percentage, Planning Committee, Monthly, decisions approved by votes.
Risk Management	Develop and implement a cybersecurity risk management program. Measure, assess and mitigate cyber risk and threats which may degrade or impact information systems within Oregon. Drive improvements to Oregon's cybersecurity posture.	• 100% of Oregon grant awardees completing the NCSR	Number, NCSR data, Annual
Mature Cybersecurity Capabilities	Enhance public sector entities incident response capabilities. Promote delivery of safe, recognizable, and trusted online services, including the use of .gov domain. Enhance preparation, response and resilience of information systems, applications, and user accounts against cyber risk and threats.	• Number of entities requesting incident response resources • Number of entities moving to .gov annually	Number, reporting, Annual

Build a Culture of Cyber Awareness	Create and extend access to public sector entities for awareness-level training. Provide outreach avenues for sharing free and low-cost resources.	• Number of public sector entities utilizing awareness-level training annually	Number, Sub-applicant reporting, Quarterly
Prepare and Plan for Cyber Incidents	Encourage incident reporting through the MS-ISAC Security Operations Center. Improve capability and capacity to adopt and use best practices and methodologies to enhance cybersecurity.	• Number of incidents reported • Number of entities participating in MS-ISAC free services • Number of entities participating in CISA free services	Number, reporting, quarterly
Collaborate and Share Information	Create a collaborative environment to share, identify, and evaluate information for members to discuss threats and vulnerabilities impacting Oregon.	• Percentage of Planning Committee members engaged in monthly meetings • Entities signup to participate in Oregon Federated SOC	Member Percentage, Planning Committee, Monthly
Build a Cyber Workforce	Provide tailored security training for public sector entities to improve and mature their cybersecurity posture. Build a network of cyber contacts across Oregon.	• Number of entity staff trained • Number of sub-applicants submitting quarterly reports for services procured	Number, Sub-applicant reporting, Quarterly

Success Factors

The successful execution of this strategic plan will broadly depend on or be influenced by the following considerations:

Management Endorsement - It is essential that this strategic plan is endorsed and driven at the highest levels of the executive branch of Oregon State Government and that it receives the full support of the Oregon State Chief Information Officer, as well as the Oregon State Chief Information Security Officer. The Oregon State Chief Information Officer and Oregon State Chief Information Security Officer should identify and establish State cybersecurity priorities and provide budgetary and human resources needed to implement the strategy.

Resource Prioritization - As the threat landscape is both evolving and expanding, it is critical to continuously advance Oregon’s security, resilience, and operational capacities. The prioritization and fluid allocation of key resources is necessary to maintain currency and effectively protect against and respond to significant cybersecurity incidents.

Shared Responsibility - Cybersecurity is a shared responsibility beyond Oregon State Government alone. As cyberspace consists of a hyper-connected array of networks, systems, and devices, the cooperation of all key stakeholders – government, industry, non-government organizations, and academia – is essential to not only the success of this strategic plan, but also the public health, welfare, and safety of the citizens, economy, and public interests of the State of Oregon and national security.

Human Capital - As cybersecurity is a highly technical and complex discipline that requires qualified and skilled human resources at sufficient staffing levels, the ability of the State to recruit, develop, and retain talented and mission-focused personnel is critical to carrying out this strategic plan.

Funding - This strategic plan was drafted assuming that funding levels for cybersecurity would remain stable and additional investments would be made over time to address the growing threat environment and to protect the public and private institutions, critical infrastructure assets, and the citizens of Oregon from the threat of cyberattacks.

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

COMPLETED BY State of Oregon SLCGP Planning Committee				**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	**Objectives # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	1.2, 3.3	
2. Monitor, audit, and track network traffic and activity	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	1.2, 5.2	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	1.1, 1.2, 2.2, 3.3	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	1.2, 2	
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)			1.2, 2, 3.2, 3.3	
a. Implement multi-factor authentication	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. Allowable project under this plan.	Fundamental		

b. Implement enhanced logging	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. Allowable project under this plan.	Fundamental		🟥
c. Data encryption for data at rest and in transit	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. Allowable project under this plan.	Fundamental		🟥
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. Allowable project under this plan.	Fundamental		🟥
e. Prohibit use of known/fixed/default passwords and credentials	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. Allowable project under this plan.	Fundamental		🟥
f. Ensure the ability to reconstitute systems (backups)	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. Allowable project under this plan.	Fundamental		🟥
g. Migration to the .gov internet domain	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental		🟥

	Allowable project under this plan.			🟥
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. This is the objective of this plan.	Fundamental	3.2	🟥
7. Ensure continuity of operations including by conducting exercises	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	5	🟥
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)	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	7	🟥
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	3	🟥
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	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	2, 3	🟥
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	6	🟥

	This is the objective of this plan.			🟥
12. Leverage cybersecurity services offered by the Department	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. This is the objective of this plan.	Fundamental	3	🟥
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations.	Fundamental	1, 2	🟥
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. This is the objective of this plan.	Fundamental	2	🟥
15. Ensure rural communities have adequate access to, and participation in plan activities	Incomplete implementation across the totality of the State and Local Government organizations. Different processes used by State Government organizations other Local Government Organizations. This is the objective of this plan.	Fundamental	4, 6	🟥
16. Distribute funds, items, services, capabilities, or activities to local governments	Oregon SAA routinely manages grant programs and has process in place.	Advanced		🟥

APPENDIX B: PROJECT SUMMARY WORKSHEET

The projects listed below are proposed sample projects for year one of the grant and will be based on consumption by local government. Planning time will need to be allocated for.

	1. Project Name	2. Project Description	3. Related Required Element #	4. Cost	5. Status	6. Priority	7. Project Type
	Federated SOC	A framework that facilitates the sharing of information across participating entities from the perspective of cyber-based threats and activities. This federation also allows for the sharing of feeds of information to be used by eligible participants, both with the State of Oregon and potentially with other peer organizations.	1, 2, 3, 6	unknown	Future	High	Organization
	Multifactor Authentication Capability (MFA)	An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. This additional protection can be applied to internal or external resources, or both.	1, 3	varies	Future	High	Equipment
	Migration to .gov Domain	Domain migration is the process of moving an entity registered domain from one root to the other. Movement of domain names services to another and involves a transition plan depending on complexity of the entity's operation. There are several things that need to be considered to ensure the migration is successful and doesn't affect a business performance internet-based service.	3	varies	Future	High	Equipment
	Information Security Awareness Training	Reveal your organization's employees' strengths and weaknesses and empower them against cyber criminals. Employees are part of an organization's attack surface, and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a healthy security program. If an organization needs to comply with different government and industry regulations, it must provide security awareness training to employees to meet regulatory requirements.	4	varies	Future	High	Train

	End use of unsupported/end of life software and hardware	Procure Professional Services or IT solutions for use by local entities to end use of unsupported/end of life software and hardware.	3	varies	Future	High	Organization
	Data encryption	Procure Professional Services or IT solutions for use by local entities to encrypt data and rest and in transit.	3	varies	Future	High	Equipment
	Logging	Procure Professional Services or IT solutions for use by local entities to enhance logging capabilities.	3	varies	Future	High	Organization
	Vulnerability Management Services and Scanning	Reveal your organization's employees' strengths and weaknesses and empower them against cyber criminals. Employees are part of an organization's attack surface, and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a healthy security program. If an organization needs to comply with different government and industry regulations, it must provide security awareness training to employees to meet regulatory requirements.	**2**	varies	Future	High	Equipment
	URL/ Web/ Content Filtering	An IT service, provided as an appliance or an add-on to a next-generation firewall, that allows for the blocking of web content based on categorical classification. This service generally allows for exceptions, based on role, as well as logging information for those exceptions or potential policy violations. Some also provide additional protections for files downloaded from or by websites.	**3**	varies	Future	High	Equipment
	Albert Sensors	An IDS (Intrusion Detection System) solution from the Center for Internet Security that can provide a second layer of detection as well as incident response and around-the-clock support.	**3**	varies	Future	High	Equipment
	Advanced Endpoint Protection (AEP)	This is an IT product that offers endpoint protection with the enhancements of machine learning, and may include cloud computing, email and other solutions. The products are generally offered as either Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR).	**3**	varies	Future	High	Equipment
	Immutable Data Backup and Recovery Testing	Data backup as a service that meets or exceeds business expectations. Data resilience refers to the ability of any data storage facility and system to	**3**	varies	Future	High	Equipment

		bounce back despite service disruptions, such as power outages, data corruption, natural disasters, and equipment failure. It is often part of an organization's disaster recovery plan.					

APPENDIX C: SERVICE CATALOG

The following tables represent the service catalog for the grant program. Table 1 represents Year 1 focus areas, targeting both the requirements for funding as well as basic cyber-hygiene. For Table 1, items that are italicized are those services or products that are required for funding. The tables are organized by tier, and then alphabetically. Where appropriate, the CIS control addressed by the solution is listed.

Table 1

	CYBER Services	**CYBER Services Governance**	
CYBER Services	Description/Rationale	**CYBER Service Tier**	**CIS Control(s)**
Advanced Endpoint Protection (AEP)	*This is an IT product that offers endpoint protection with the enhancements of machine learning, and may include cloud computing, email, and other solutions. The products are generally offered as either Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR).*	*Tier 1*	*10*
Domain Migration Services (Migration to .gov)	*Domain migration is the process of moving an entity registered domain from one root to the other. Movement of domain names services to another and involves a transition plan depending on complexity of the entity's operation. There are several things that need to be considered to ensure the migration is successful and doesn't affect a business performance internet-based service.*	*Tier 1*	
Immutable Data Backup and Recovery Testing	*Data backup as a service that meets or exceeds business expectations. Data resilience refers to the ability of any data storage facility and system to bounce back despite service disruptions, such as power outages, data corruption, natural disasters, and equipment failure. It is often part of an organization's disaster recovery plan.*	*Tier 1*	*11*
Multifactor Authentication Capability (MFA)	*An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. This additional protection can be applied to internal or external resources, or both.*	*Tier 1*	*6*
Albert Sensors	*An IDS (Intrusion Detection System) solution from the Center for Internet Security that can provide a second layer of detection as well as incident response and around-the-clock support*	Tier 1	13

Information Security Awareness Training	*Reveal your organization's employees' strengths and weaknesses and empower them against cyber criminals. Employees are part of an organization's attack surface, and ensuring they have the know-how to defend themselves and the organization against threats is a critical part of a healthy security program. If an organization needs to comply with different government and industry regulations, it must provide security awareness training to employees to meet regulatory requirements.*	Tier 1	14
URL/Web/Content filtering	*An IT service, provided as an appliance or an add-on to a next-generation firewall, that allows for the blocking of web content based on categorical classification. This service generally allows for exceptions, based on role, as well as logging information for those exceptions or potential policy violations. Some also provide additional protections for files downloaded from or by websites.*	Tier 1	9
Vulnerability Management Services & Scanning	*Vulnerability management services are designed to identify security holes within an organization's IT infrastructure, specifically related to cyber threats. Vulnerability assessment services run a series of diagnostics on entity's devices, applications, and networks, and utilize this data to recommend areas for improvement based on urgency and scope.*	Tier 1	7
Consulting and Planning Services	*This service allows for eligible entities to procure assistance with the planning and implementation of other products and services in this catalog, along with other, general planning needs, such as those that would align GRC activities to business performance drivers, using frameworks such as NIST, PCI/DSS, ISO, GDPR, NYDFS, and others with our IT security service program.*	Tier 1	17

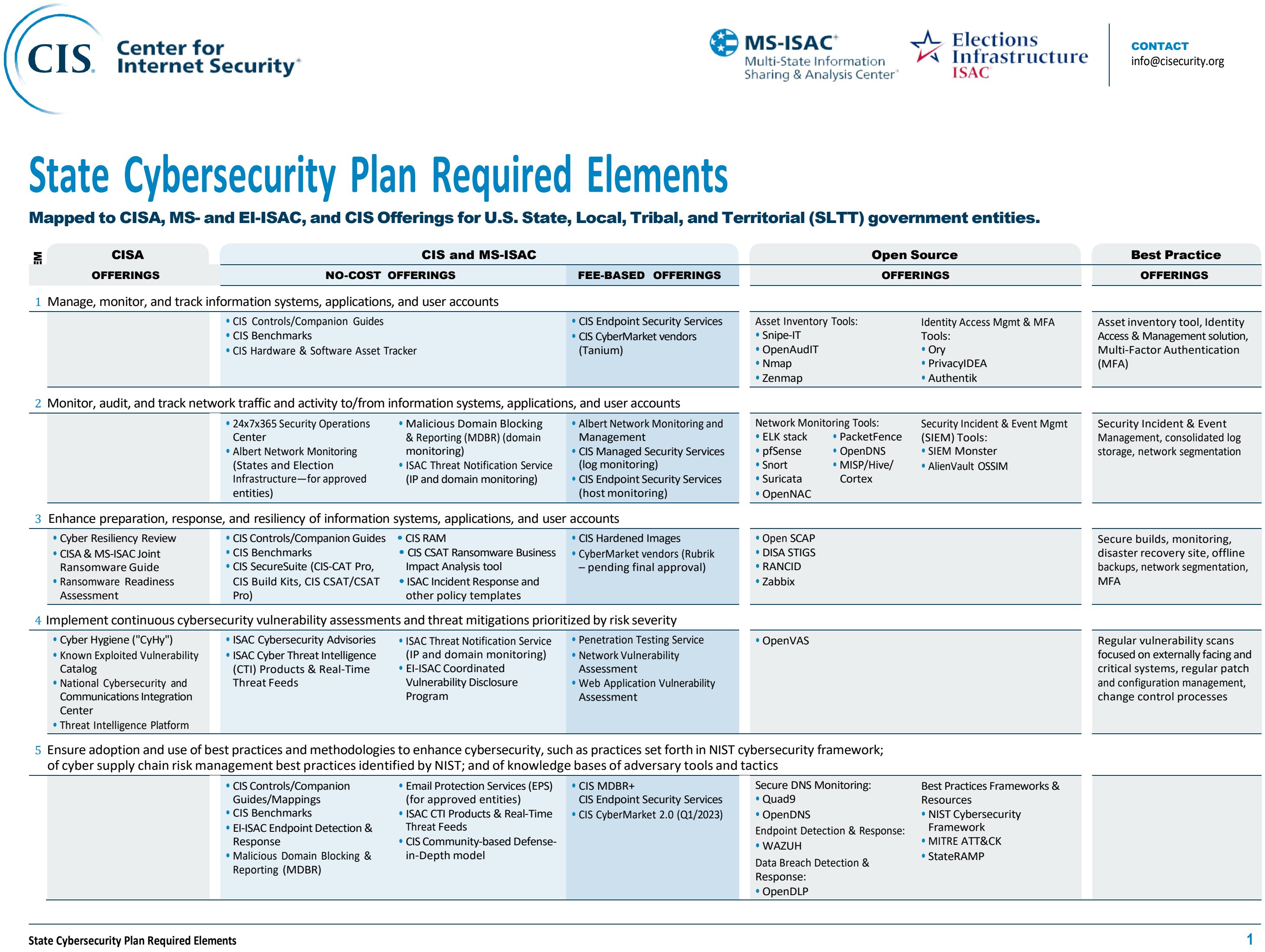
Table 2

CYBER Services	CYBER Services	CYBER Services Governance	
	Description/Rationale	CYBER Service Tier	CIS Control(s)
Converged Endpoint Management (XEM)	*This is an IT product that converges IT management of devices and security operations into a single solution to help provide better control in an environment. For smaller IT organizations, it can help with both endpoint security as well as management for things like patching. This solution would require both an XEM product as well as the expertise to size, select and deploy a product. Additional services for ongoing support may also be appropriate.*	Tier 2	10
Cyber Security Risk Assessment Services	*A cyber risk assessment is essential in building an information security program. Risk management and risk assessment activities will consider people, business processes (information handling), and technology.*	Tier 2	18
DNS Filtering	*An IT service or appliance that uses block lists to filter out known bad hosts, blocking DNS resolution to those hosts. This can be done as part of a next generation firewall deployment or as a subscription to a cloud-based service.*	Tier 2	13
Email security gateway	*An IT device or service that provides additional screening for potential malware attached to email. Traditionally this has been an appliance on-site, however there are cloud-based services. These services also provide URL screening for URLs sent via email. Often, they include email encryption options to provide additional email security.*	Tier 2	9
Enhanced Network Protection - Firewall Services	*A Network Firewall is a security device used to prevent or limit illegal access to private networks by using policies defining the only traffic allowed on the network; any other traffic seeking to connect is blocked.*	Tier 2	13
Identity & Access Management Solutions	*Identity and access management (IAM) ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs. Identity management and access systems enables your organization to manage employee access and credentials allowing the right credentials to have the right access to enterprise resources.*	Tier 2	5

Mobile Device Management (MDM) Solutions	*Mobile device management (MDM) solutions help businesses address the difficulties of managing mobile endpoints across a business. Employing device detection and integration, policy adherence rules, application deployment, and a variety of other features, companies can manage the mobile devices and applications needed to run their business.*	Tier 2	4
Penetration Testing Services	*This IT service is used to test a network for weaknesses and flaws in configurations or settings that could allow for intruders to infiltrate the network. Depending on the level of testing requested, the provider may also then attempt to compromise other devices on the network. This may be done with or without prior information being handed off to the testers.*	Tier 2	18
Privileged Access Management (PAM)	*An IT product that allows an organization to manage the privileges of users, with specific focus on those users whose role requires access beyond those of standard users. These products generally interact with directory services to allow for security groups to be granted those privileges. Audit logging is also provided, and in some cases, alerts may be set up for use of specific accounts or elevation types.*	Tier 2	5
Web Application Firewall (WAF)	*A web application firewall (WAF) protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. Attacks to apps are the leading cause of breaches—they are the gateway to your valuable data.*	Tier 2	16
Application Security Services	*Application security assessment services are designed to help your development and technical team to identify, understand risk, and threat to the application and take remedial action against critical and non-critical vulnerabilities. The goal is to transform the application security process into an on-going security governance managed process, establishing an application security gate to assess all applications before they go into production*	Tier 3	16
Security Information and Event Management (SIEM) Technology	*SIEM technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.*	Tier 3	13
MDR/XDR Solutions	*An IT solution that allows for the gathering of data from access an organizations existing security tools to provide analysis and automation to threat response.*	Tier 3	10

Statewide Federated SOCs	*A framework that facilitates the sharing of information across participating entities from the perspective of cyber-based threats and activities. This federation also allows for the sharing of feeds of information to be used by eligible participants, both with the State of Oregon and potentially with other peer organizations.*	Tier 3	

APPENDIX D: CIS AND MS-ISAC OFFERINGS



CIS Center for Internet Security

MS-ISAC Multi-State Information Sharing & Analysis Center

Elections Infrastructure ISAC

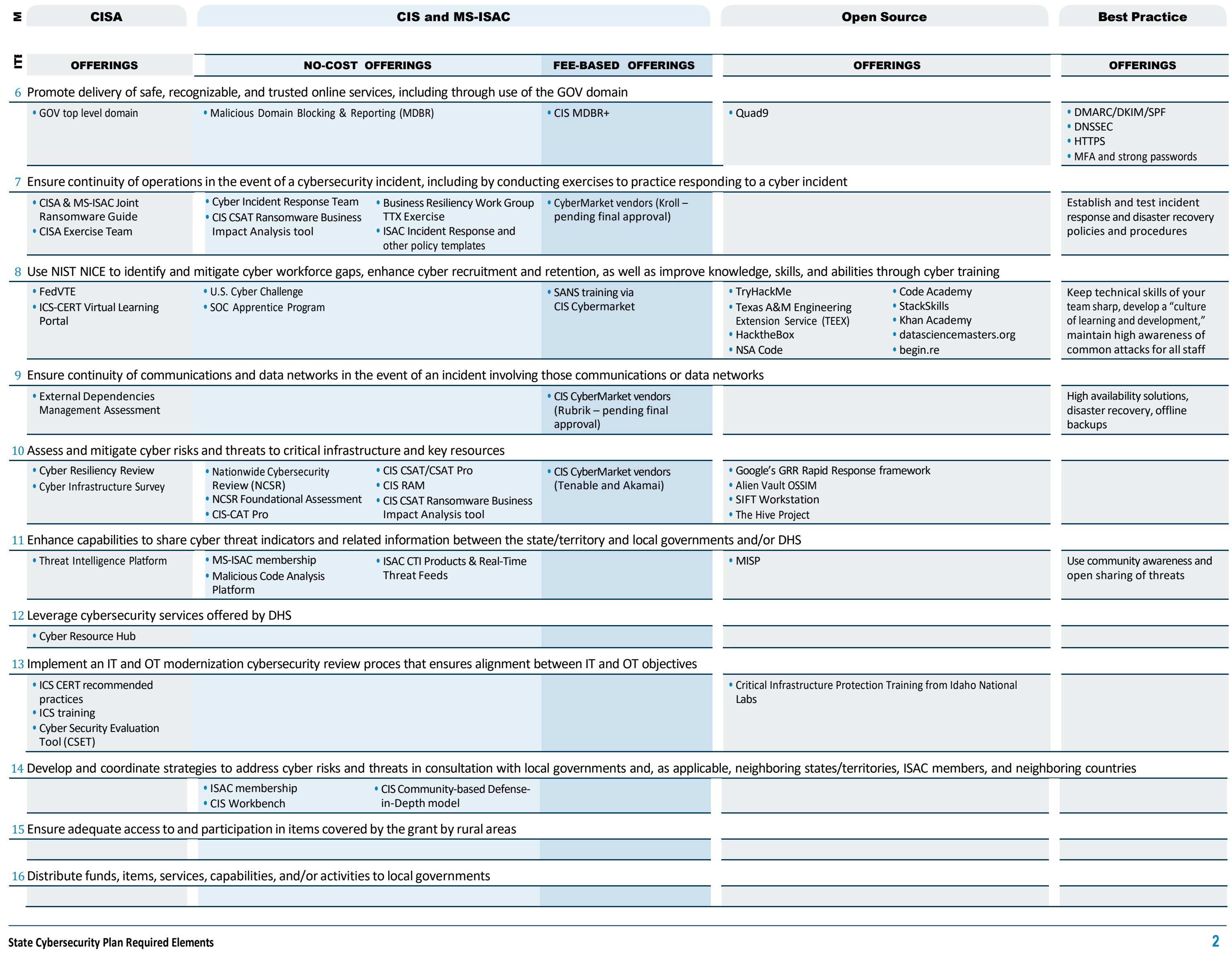
CONTACT
info@cisecurity.org

State Cybersecurity Plan Required Elements

Mapped to CISA, MS- and EI-ISAC, and CIS Offerings for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

EM	CISA	CIS and MS-ISAC			Open Source		Best Practice
	OFFERINGS	NO-COST OFFERINGS		FEE-BASED OFFERINGS	OFFERINGS		OFFERINGS
1 Manage, monitor, and track information systems, applications, and user accounts		• CIS Controls/Companion Guides • CIS Benchmarks • CIS Hardware & Software Asset Tracker		• CIS Endpoint Security Services • CIS CyberMarket vendors (Tanium)	Asset Inventory Tools: • Snipe-IT • OpenAudIT • Nmap • Zenmap	Identity Access Mgmt & MFA Tools: • Ory • PrivacyIDEA • Authentik	Asset inventory tool, Identity Access & Management solution, Multi-Factor Authentication (MFA)
2 Monitor, audit, and track network traffic and activity to/from information systems, applications, and user accounts		• 24x7x365 Security Operations Center • Albert Network Monitoring (States and Election Infrastructure—for approved entities)	• Malicious Domain Blocking & Reporting (MDBR) (domain monitoring) • ISAC Threat Notification Service (IP and domain monitoring)	• Albert Network Monitoring and Management • CIS Managed Security Services (log monitoring) • CIS Endpoint Security Services (host monitoring)	Network Monitoring Tools: • ELK stack • pfSense • Snort • Suricata • OpenNAC • PacketFence • OpenDNS • MISP/Hive/ Cortex	Security Incident & Event Mgmt (SIEM) Tools: • SIEM Monster • AlienVault OSSIM	Security Incident & Event Management, consolidated log storage, network segmentation
3 Enhance preparation, response, and resiliency of information systems, applications, and user accounts	• Cyber Resiliency Review • CISA & MS-ISAC Joint Ransomware Guide • Ransomware Readiness Assessment	• CIS Controls/Companion Guides • CIS Benchmarks • CIS SecureSuite (CIS-CAT Pro, CIS Build Kits, CIS CSAT/CSAT Pro)	• CIS RAM • CIS CSAT Ransomware Business Impact Analysis tool • ISAC Incident Response and other policy templates	• CIS Hardened Images • CyberMarket vendors (Rubrik – pending final approval)	• Open SCAP • DISA STIGS • RANCID • Zabbix		Secure builds, monitoring, disaster recovery site, offline backups, network segmentation, MFA
4 Implement continuous cybersecurity vulnerability assessments and threat mitigations prioritized by risk severity	• Cyber Hygiene ("CyHy") • Known Exploited Vulnerability Catalog • National Cybersecurity and Communications Integration Center • Threat Intelligence Platform	• ISAC Cybersecurity Advisories • ISAC Cyber Threat Intelligence (CTI) Products & Real-Time Threat Feeds	• ISAC Threat Notification Service (IP and domain monitoring) • EI-ISAC Coordinated Vulnerability Disclosure Program	• Penetration Testing Service • Network Vulnerability Assessment • Web Application Vulnerability Assessment	• OpenVAS		Regular vulnerability scans focused on externally facing and critical systems, regular patch and configuration management, change control processes
5 Ensure adoption and use of best practices and methodologies to enhance cybersecurity, such as practices set forth in NIST cybersecurity framework; of cyber supply chain risk management best practices identified by NIST; and of knowledge bases of adversary tools and tactics		• CIS Controls/Companion Guides/Mappings • CIS Benchmarks • EI-ISAC Endpoint Detection & Response • Malicious Domain Blocking & Reporting (MDBR)	• Email Protection Services (EPS) (for approved entities) • ISAC CTI Products & Real-Time Threat Feeds • CIS Community-based Defense-in-Depth model	• CIS MDBR+ CIS Endpoint Security Services • CIS CyberMarket 2.0 (Q1/2023)	Secure DNS Monitoring: • Quad9 • OpenDNS Endpoint Detection & Response: • WAZUH Data Breach Detection & Response: • OpenDLP	Best Practices Frameworks & Resources • NIST Cybersecurity Framework • MITRE ATT&CK • StateRAMP	

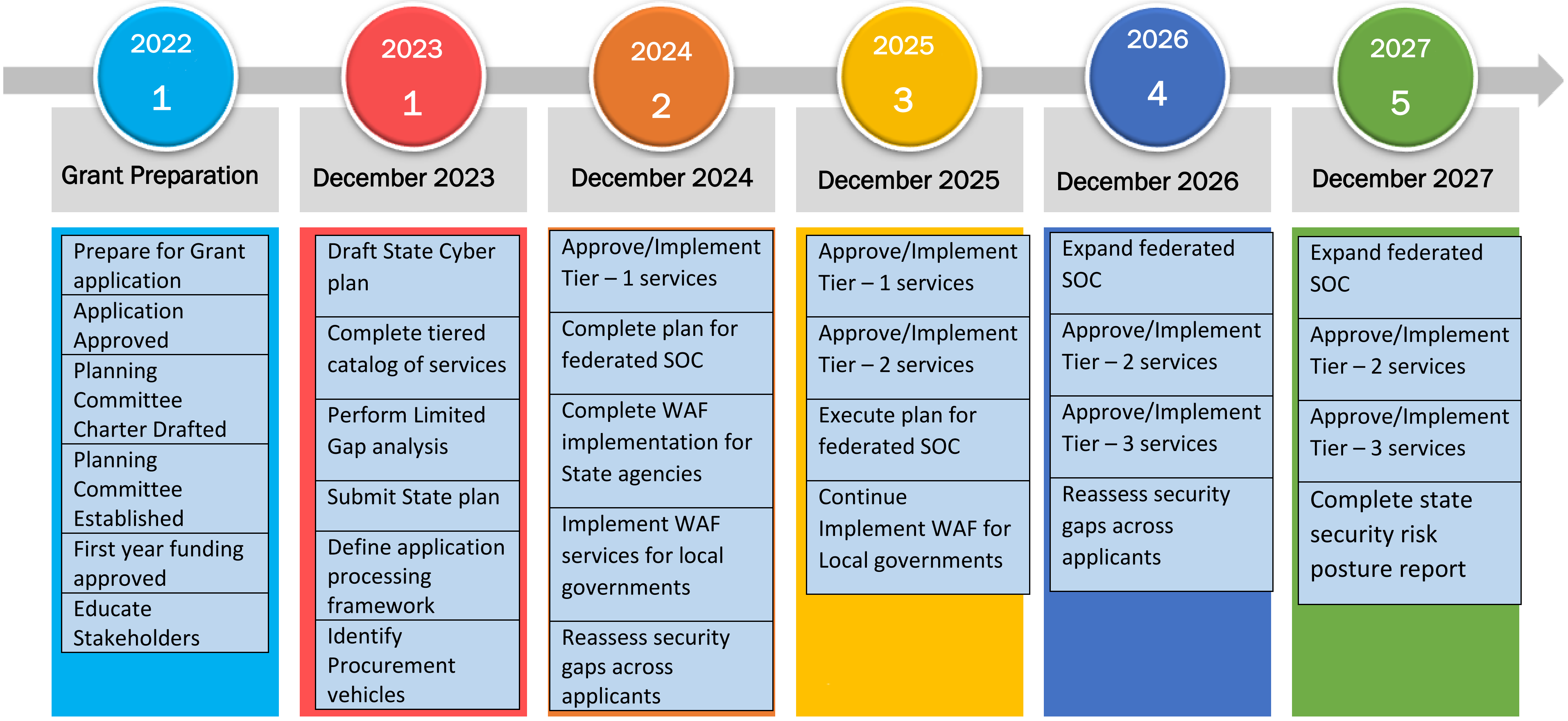
State Cybersecurity Plan Required Elements 1



M	CISA	CIS and MS-ISAC		Open Source	Best Practice
ITE	OFFERINGS	NO-COST OFFERINGS	FEE-BASED OFFERINGS	OFFERINGS	OFFERINGS
6 Promote delivery of safe, recognizable, and trusted online services, including through use of the GOV domain					
	• GOV top level domain	• Malicious Domain Blocking & Reporting (MDBR)	• CIS MDBR+	• Quad9	• DMARC/DKIM/SPF • DNSSEC • HTTPS • MFA and strong passwords
7 Ensure continuity of operations in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cyber incident					
	• CISA & MS-ISAC Joint Ransomware Guide • CISA Exercise Team	• Cyber Incident Response Team • CIS CSAT Ransomware Business Impact Analysis tool • Business Resiliency Work Group TTX Exercise • ISAC Incident Response and other policy templates	• CyberMarket vendors (Kroll – pending final approval)		Establish and test incident response and disaster recovery policies and procedures
8 Use NIST NICE to identify and mitigate cyber workforce gaps, enhance cyber recruitment and retention, as well as improve knowledge, skills, and abilities through cyber training					
	• FedVTE • ICS-CERT Virtual Learning Portal	• U.S. Cyber Challenge • SOC Apprentice Program	• SANS training via CIS Cybermarket	• TryHackMe • Texas A&M Engineering Extension Service (TEEX) • HacktheBox • NSA Code • Code Academy • StackSkills • Khan Academy • datasciencemasters.org • begin.re	Keep technical skills of your team sharp, develop a “culture of learning and development,” maintain high awareness of common attacks for all staff
9 Ensure continuity of communications and data networks in the event of an incident involving those communications or data networks					
	• External Dependencies Management Assessment		• CIS CyberMarket vendors (Rubrik – pending final approval)		High availability solutions, disaster recovery, offline backups
10 Assess and mitigate cyber risks and threats to critical infrastructure and key resources					
	• Cyber Resiliency Review • Cyber Infrastructure Survey	• Nationwide Cybersecurity Review (NCSR) • NCSR Foundational Assessment • CIS-CAT Pro • CIS CSAT/CSAT Pro • CIS RAM • CIS CSAT Ransomware Business Impact Analysis tool	• CIS CyberMarket vendors (Tenable and Akamai)	• Google’s GRR Rapid Response framework • Alien Vault OSSIM • SIFT Workstation • The Hive Project	
11 Enhance capabilities to share cyber threat indicators and related information between the state/territory and local governments and/or DHS					
	• Threat Intelligence Platform	• MS-ISAC membership • Malicious Code Analysis Platform • ISAC CTI Products & Real-Time Threat Feeds		• MISP	Use community awareness and open sharing of threats
12 Leverage cybersecurity services offered by DHS					
	• Cyber Resource Hub				
13 Implement an IT and OT modernization cybersecurity review proces that ensures alignment between IT and OT objectives					
	• ICS CERT recommended practices • ICS training • Cyber Security Evaluation Tool (CSET)			• Critical Infrastructure Protection Training from Idaho National Labs	
14 Develop and coordinate strategies to address cyber risks and threats in consultation with local governments and, as applicable, neighboring states/territories, ISAC members, and neighboring countries					
		• ISAC membership • CIS Workbench • CIS Community-based Defense-in-Depth model			
15 Ensure adequate access to and participation in items covered by the grant by rural areas					
16 Distribute funds, items, services, capabilities, and/or activities to local governments					

State Cybersecurity Plan Required Elements 2

APPENDIX E: ROADMAP



2022 – 1 – Grant Preparation

- Prepare for Grant application
- Application Approved
- Planning Committee Charter Drafted
- Planning Committee Established
- First year funding approved
- Educate Stakeholders

2023 – 1 – December 2023

- Draft State Cyber plan
- Complete tiered catalog of services
- Perform Limited Gap analysis
- Submit State plan
- Define application processing framework
- Identify Procurement vehicles

2024 – 2 – December 2024

- Approve/Implement Tier – 1 services
- Complete plan for federated SOC
- Complete WAF implementation for State agencies
- Implement WAF services for local governments
- Reassess security gaps across applicants

2025 – 3 – December 2025

- Approve/Implement Tier – 1 services
- Approve/Implement Tier – 2 services
- Execute plan for federated SOC
- Continue Implement WAF for Local governments

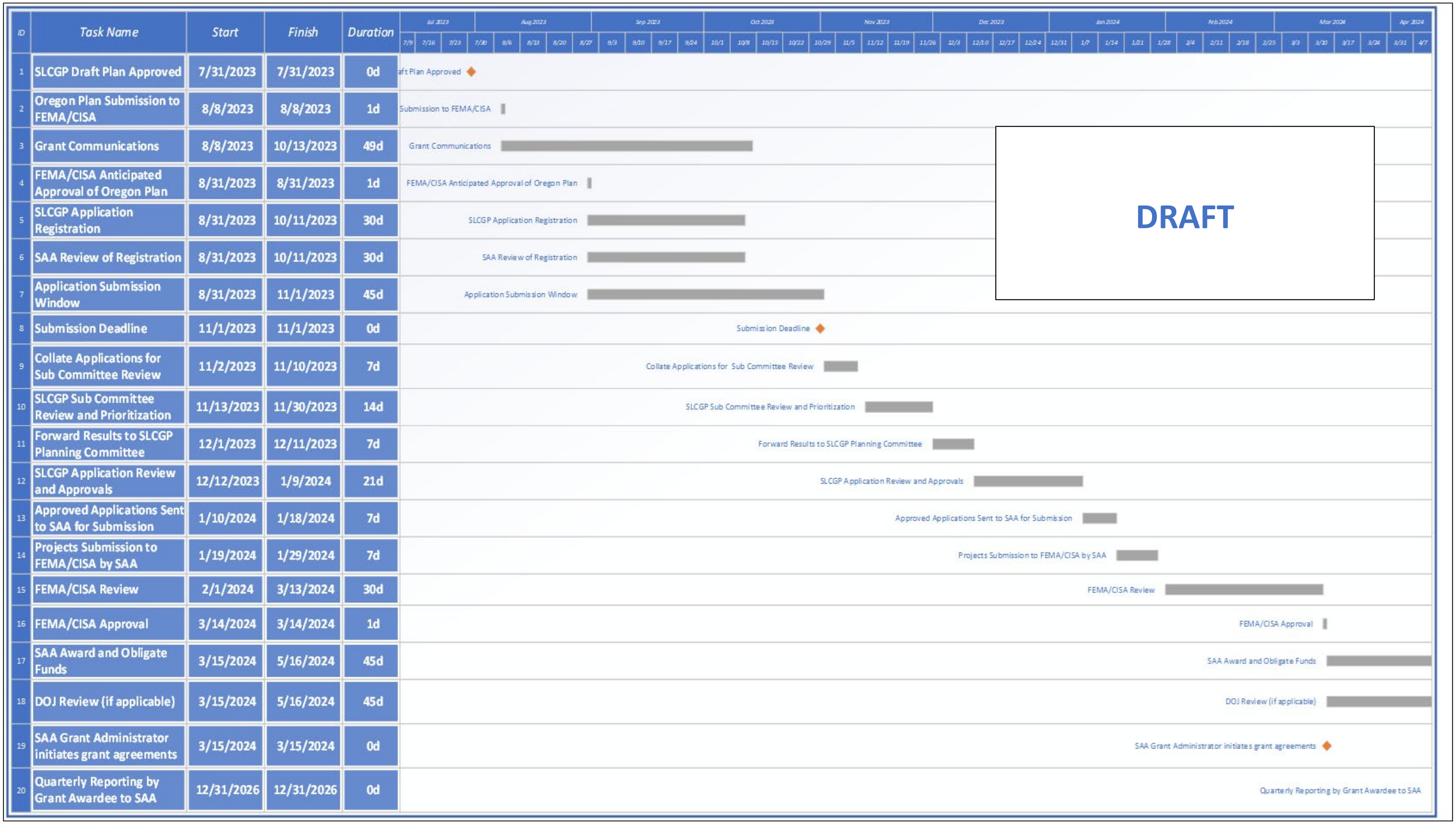
2026 – 4 – December 2026

- Expand federated SOC
- Approve/Implement Tier – 2 services
- Approve/Implement Tier – 3 services
- Reassess security gaps across applicants

2027 – 5 – December 2027

- Expand federated SOC
- Approve/Implement Tier – 2 services
- Approve/Implement Tier – 3 services
- Complete state security risk posture report

APPENDIX F: IMPLEMENTATION TIMELINE



ID	Task Name	Start	Finish	Duration
1	SLCGP Draft Plan Approved	7/31/2023	7/31/2023	0d
2	Oregon Plan Submission to FEMA/CISA	8/8/2023	8/8/2023	1d
3	Grant Communications	8/8/2023	10/13/2023	49d
4	FEMA/CISA Anticipated Approval of Oregon Plan	8/31/2023	8/31/2023	1d
5	SLCGP Application Registration	8/31/2023	10/11/2023	30d
6	SAA Review of Registration	8/31/2023	10/11/2023	30d
7	Application Submission Window	8/31/2023	11/1/2023	45d
8	Submission Deadline	11/1/2023	11/1/2023	0d
9	Collate Applications for Sub Committee Review	11/2/2023	11/10/2023	7d
10	SLCGP Sub Committee Review and Prioritization	11/13/2023	11/30/2023	14d
11	Forward Results to SLCGP Planning Committee	12/1/2023	12/11/2023	7d
12	SLCGP Application Review and Approvals	12/12/2023	1/9/2024	21d
13	Approved Applications Sent to SAA for Submission	1/10/2024	1/18/2024	7d
14	Projects Submission to FEMA/CISA by SAA	1/19/2024	1/29/2024	7d
15	FEMA/CISA Review	2/1/2024	3/13/2024	30d
16	FEMA/CISA Approval	3/14/2024	3/14/2024	1d
17	SAA Award and Obligate Funds	3/15/2024	5/16/2024	45d
18	DOJ Review (if applicable)	3/15/2024	5/16/2024	45d
19	SAA Grant Administrator initiates grant agreements	3/15/2024	3/15/2024	0d
20	Quarterly Reporting by Grant Awardee to SAA	12/31/2026	12/31/2026	0d

Jul 2023
Aug 2023
Sep 2023
Oct 2023
Nov 2023
Dec 2023
Jan 2024
Feb 2024
Mar 2024
Apr 2024
7/9
7/16
7/23
7/30
8/6
8/13
8/20
8/27
9/3
9/10
9/17
9/24
10/1
10/8
10/15
10/22
10/29
11/5
11/12
11/19
11/26
12/3
12/10
12/17
12/24
12/31
1/7
1/14
1/21
1/28
2/4
2/11
2/18
2/25
3/3
3/10
3/17
3/24
3/31
4/7
aft Plan Approved
Submission to FEMA/CISA
Grant Communications
FEMA/CISA Anticipated Approval of Oregon Plan
SLCGP Application Registration
SAA Review of Registration
Application Submission Window
Submission Deadline
Collate Applications for Sub Committee Review
SLCGP Sub Committee Review and Prioritization
Forward Results to SLCGP Planning Committee
SLCGP Application Review and Approvals
Approved Applications Sent to SAA for Submission
Projects Submission to FEMA/CISA by SAA
FEMA/CISA Review
FEMA/CISA Approval
SAA Award and Obligate Funds
DOJ Review (if applicable)
SAA Grant Administrator initiates grant agreements
Quarterly Reporting by Grant Awardee to SAA

APPENDIX G: DRAFT PROJECT APPLICATION

Fiscal Year 2022
State and Local Cybersecurity Grant Program
Project Application

Overview

This project application is for jurisdiction applying for the FY2022 State and Local Cybersecurity Grant Program (SLCGP). Every project submitted by a county, city, special district, or tribe must complete this application. No more than two project applications may be turned in per Applicant Agency.

I. General Project Information

Applicant Agency (agencies)

Project Title

Federal Funds Requested

$

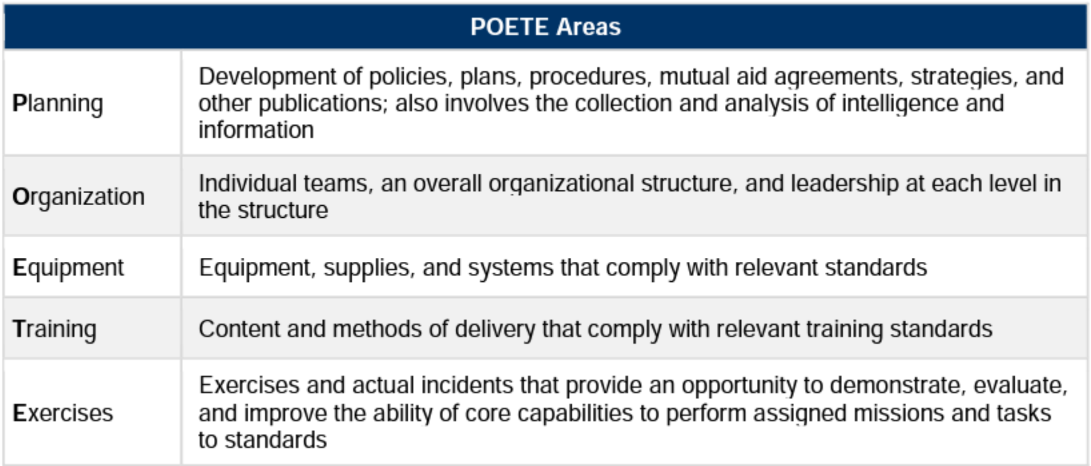
SLCGP Service Catalog

SLCGP Strategy **GOAL #**

SLCGP Strategy **OBJECTIVE #**

Project Budget Defined by POETE

Planning	$
Organization	$
Equipment	$
Training	$
Exercises	$



POETE Areas	
Planning	Development of policies, plans, procedures, mutual aid agreements, strategies, and other publications; also involves the collection and analysis of intelligence and information
Organization	Individual teams, an overall organizational structure, and leadership at each level in the structure
Equipment	Equipment, supplies, and systems that comply with relevant standards
Training	Content and methods of delivery that comply with relevant training standards
Exercises	Exercises and actual incidents that provide an opportunity to demonstrate, evaluate, and improve the ability of core capabilities to perform assigned missions and tasks to standards

II. Requirements

Clearly describe how this project will address a cybersecurity gap/gaps, and how that will allow you to improve your current cyber capability.

Clearly describe how the project ties to Oregon’s SLCGP Cybersecurity Plan.

III.IJ Specific Requirements

Cyber Security

Has the jurisdiction performed a formal cyber assessment?

If the jurisdiction has not performed a formal cyber assessment, does the jurisdiction have a formal cyber security plan/strategy?

IV.Project Details 25pts

Describe the project (Project business Case). What will this project do? Please be as clear and direct as possible in your first paragraph. Supporting details may be provided in 2nd or 3rd paragraphs.

Have you received quotes for the costs of the items, training, or services described above?

V.Project Impact 30pts

Describe who in the community will be directly impacted by this project and how.

Describe what impact this project will have on the whole community.

Describe how the project will enhance the cyber capability for the jurisdiction.

VI.Capability History 5pts

Describe the jurisdictions current functionality in the chosen cyber capability.

VII. Gap Information 15pts

Describe the current gap in the cyber capability.

Describe how the gap was identified (real event, exercise, assessment).

Describe what the agency/community has done to fill the gap so far.

Describe how the proposed project will fill the gap.

VIII. Sustainment 15pts

Describe the jurisdiction's plan to sustain the cyber capabilities built by this project.

IX. Milestones 10pts

Quarter 1

Quarter 2

Quarter 3

Quarter 4

Quarter 5

Quarter 6

Quarter 7

Quarter 8