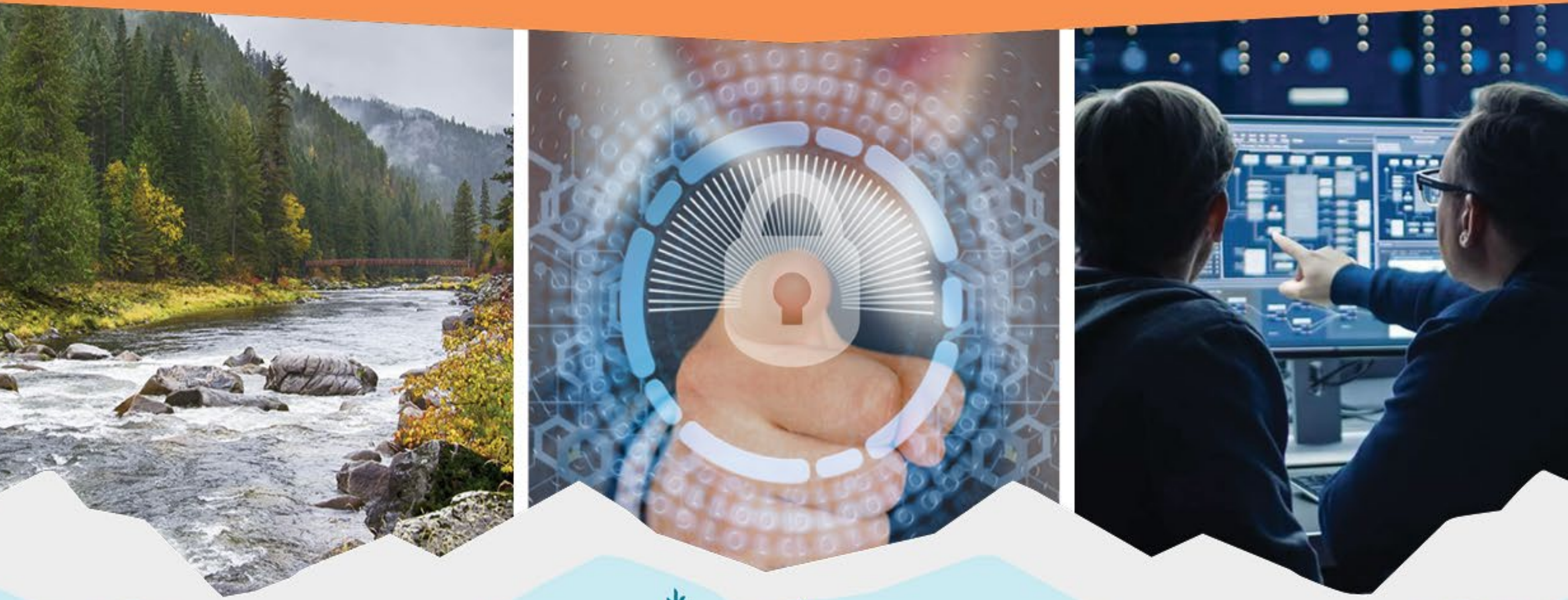
Idaho SLCGP Cybersecurity Plan
September 2023



Approved by the Idaho Cybersecurity Planning Committee on September 27, 2023
Version 1.0

Page Intentionally Left Blank

TABLE OF CONTENTS

LETTER FROM THE CYBERSECURITY PLANNING COMMITTEE & STATE CISO

Dear Sir/Madam:

The Cybersecurity Planning Committee for the State of Idaho is pleased to present the State's 2023 State and Local Cybersecurity Grant Program (SLCGP) Implementation Plan. It addresses Idaho's goals and objectives for improving cybersecurity readiness and capabilities in a whole-of-state approach that will be executed over the current and future SLCGP periods of performance.

The plan meets the requirements of the current U.S. Department of Homeland Security (DHS) guidelines for the SLCGP and outlines a security services approach that Idaho stakeholders have determined will best meet the needs of the State's diverse populations. This plan, which supports the "Planning" primary core capability, demonstrates Idaho's recognition that the State must make continued improvements to its cybersecurity posture - especially that of rural and frontier[1] counties, municipalities, and communities – while also addressing the cybersecurity posture of the State's considerable critical infrastructure and key resource providers.

Idaho's Cybersecurity Planning Committee is comprised of representatives from a wide mix of state agencies, local government jurisdictions, and other relevant organizations with need, knowledge, and expertise. Committee members have collaborated to develop this plan with actionable and measurable goals and objectives that will address Idaho's unique cybersecurity environment, gaps, and needs as they are accomplished.

Throughout the execution of this plan, one of Idaho's objectives is to begin forging the impressive "enabling asset environment" within the State – our cybersecurity expertise, activities and services provided by Idaho's public, private and educational organizations - into a cohesive, coordinated, and effective whole-of-state process. The plan will deconflict any overlap of effort among stakeholders, and result in each entity playing their optimal role in a unified approach to Idaho's long term cybersecurity resilience.

The focus of Idaho's plan is to utilize the extraordinary cybersecurity resources located in the State's more populated areas and employ innovative strategic thinking to help improve the cybersecurity capacity and readiness of rural and frontier jurisdictions, especially the sparsely populated communities that characterize much of Idaho. The plan incorporates the required SLCGP objectives by "right-sizing" our efforts to address gaps in the security of Idaho's jurisdictions at realistic levels that are understandable, accommodating, and achievable.

[1] Eighty percent (80%) of Idaho's 44 counties are rural and 96% of our 201 municipalities are classified as rural. Our 124 towns with populations less than 1,000 are a mix of rural and frontier communities with a median population of 371 residents often quite sparsely settled across their regions. **Frontier jurisdictions** are defined as those 15 counties with 5 or fewer residents per square mile.

The premise of Idaho's SLCGP Implementation Plan is the recognition that the unique diversity among stakeholders requires a sustained effort to serve our most vulnerable communities through effective education, outreach, and support. Idaho enjoys an exceptional level of support from the Governor's Office regarding whole of state cybersecurity, along with the interest and cooperation of the State's private sector, higher education, and industry leaders.

Sincerely,

John H Brown

John Brown
Chief Information Security Officer
Idaho Office of Information Technology Services

Brad Richy
Director, Homeland Security Advisor
Idaho Office of Emergency Management

INTRODUCTION

Idaho's SLCGP Cybersecurity Plan is a multi-year strategic planning document that anticipates further SLCGP funding allocations and includes the following components:

- **Vision and Mission:** Articulates our state's vision and mission for improving cybersecurity resilience and interoperability over the next three years and beyond, based on additionally expected SLCGP funding that Idaho expects to receive.
- **Organization, Roles, and Responsibilities:** Describes the current roles and responsibilities, and governance mechanisms for cybersecurity within Idaho as well as the successes and challenges the State has experienced to date and its corresponding priorities for improvement. This component also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is now and will be supported throughout the period of performance. This section additionally includes a governance model that identifies authorities and requirements of the State of Idaho and its county and municipal government jurisdictions for improved cybersecurity. The cybersecurity plan itself is a guiding document which does not formally create any authority or direction over any of Idaho's local systems or agencies.
- **Incorporation of Feedback and Input from Local Governments and Associations**: Describes how Idaho incorporated preliminary input and will schedule additional inputs from local governments to reduce overall cybersecurity risk across the state and each eligible entity within the state, as an especially important foundation in developing this whole-of-state cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape and close key gaps in the cybersecurity of all participating government jurisdictions.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within the State of Idaho along with methods and strategies for funding sustainment and enhancement to meet long-term goals.

- **Implementation Plan:** Describes Idaho's plan to execute, implement, sustain, and continually update and adapt the State's cybersecurity plan to enable continued evolution of and progress toward our identified goals and to keep up with the evolution of our threat, vulnerability, and gap environment. The implementation plan includes the resources to accomplish this and preliminary timelines where practicable.
- **Metrics:** Describes how Idaho will measure the outputs and outcomes of the program across the entity, period over period.

Idaho has adopted the NIST 800-171 standard as its official state cybersecurity framework. The simple, prescriptive nature of NIST 800-171 and its focus on protection is well suited to our foundational level of cybersecurity. The State intends to use this framework to improve local, rural and frontier cybersecurity and gauge and measure progress over time. Then as Idaho matures its cyber posture, the State may transition to using a more holistic framework, like NIST CSF, to address the full spectrum of capabilities.

Vision And Mission

This section describes Idaho's long-term vision for improving whole-of-state cybersecurity and the mission statement of the State to support our vision:

Vision

Establish the State of Idaho as a model of cybersecurity awareness, practice, and effectiveness to sustain our ongoing transformation to a technology-forward ecosystem and knowledge-based economy with technology innovation as our centerpiece of growth.

Mission

Support and enhance the resilience of Idaho's government, critical infrastructure, and local jurisdictions by addressing the pervasive cybersecurity risk to their operations, assets, and continuity, through a sustained approach to improving the cybersecurity posture of our most vulnerable local, rural and frontier jurisdictions.

Cybersecurity Program Goals and Objectives

Idaho has established the following cybersecurity goals and objectives for our long-term effort partially funded by 2022 and 2023 SLCGP Notices of Funding (NOFO) over a combined period of performance through 2027:

Cybersecurity Program	
Program Goal	**Program Objectives**
1. Develop a sustained internal capacity in Idaho to prevent cybersecurity events, reduce the impact of successful attacks, respond effectively, and recover with minimal long-term degradation of operational integrity, services delivery, and the confidentiality, integrity, and availability of our most important assets – data and information and control systems.	1.1 Establish cybersecurity as a whole-of-state long-term strategic initiative supported by a statewide cybersecurity strategy and roadmap, meeting Recommendation 1.1 of the March 2022 Governor's Cybersecurity Task Force Report and requirements of the SLCGP.
	1.2 Communicate cohesively and repetitively about cybersecurity risk awareness, literacy, and management so everyone in the state understands their responsibility for security.
	1.3 Provide the information, tools, and support to local governments – especially rural and frontier jurisdictions – necessary to protect their systems and information from most cybersecurity threats.
	1.4 Increase adoption of basic cybersecurity practices across the state.

Cybersecurity Program	
Program Goal	**Program Objectives**
2. Encourage and enhance extraordinary cooperation and collaboration among state agencies and departments, local government jurisdictions, critical infrastructure, educational institutions, and private industry that collectively are critical to state prominence and leadership in cybersecurity.	2.1 Ensure that all state agencies and local jurisdictions understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and assessments.
	2.2 Develop an information technology (IT) and security workforce and talent pipeline that has the requisite knowledge, skills, and capabilities to meet the demands of state and local government departments, agencies, and jurisdictions.
	2.3 Bring everyone into the room and foster a shared community of cyber information sharing and support through consideration of a best-of-breed Cybersecurity Fusion Center, meeting Recommendation 1.2 of the March 2022 Governor's Cybersecurity Task Force Report and improving outreach and information sharing with rural counties, meeting Recommendations 4.1 and 4.4 of the March 2022 Governor's Cybersecurity Task Force Report.
	2.4 Develop, maintain, and enhance an inventory of Idaho's critical infrastructure and key resources, meeting Recommendation 1.4 of the March 2022 Governor's Cybersecurity Task Force Report.
3.Support, maintain, and protect Idaho's unique mix of world-leading cybersecurity and engineering capacity and apply its extraordinary knowledge for broader statewide benefit as a key ingredient of our readiness for the cybersecurity challenges facing our state and nation.	3.1 Sustain Idaho's deeply collaborative and inclusive public/private partnerships.
	3.2 Encourage cross-sector participation and dialog in planning, decisioning, and execution.
	3.3 Develop a cyber workforce optimization strategy, considering programs to encourage cyber up-skilling of rural government employees and tribal members, incenting early career security employment and twilight career programs for older technically skilled workers to work in rural areas, and actively recruiting veterans, meeting Recommendation 2.5 of the March 2022 Governor's Cybersecurity Task Force Report.
4.Sustain the strong, decisive direction and tone from the top of state government.	4.1 Develop and establish an organizational and governance model that efficiently connects the cybersecurity program elements necessary for success and establishes clear missions, roles and responsibilities, and decision matrices among relevant state agencies, so Idaho de-conflicts any duplication of effort and authority.
	4.2 Encourage local government jurisdictions to fund reasonable budget requests from their IT or security departments or responsible persons, supporting the replacement of out of support hardware, software, and services with more securable infrastructure.
	4.3 Ensure that the State solicits expert policy perspectives, recommendations, and hands-on participation from our rich array of partner organizations throughout Idaho.

CYBERSECURITY PLAN ELEMENTS

Idaho's SLCGP Cybersecurity Plan incorporates the following existing plans by reference:

- **March 2022 Governor's Cybersecurity Task Force Report**
  - Identified statewide cybersecurity as a strategic imperative and established 18 recommendations to improve Idaho's resistance to cyber-attacks, many of which will become part of this plan.
- **2018 State of Idaho Hazard Mitigation Plan**
  - Chapter 3.10 - Risk Assessment: Cyber Disruption, as updated through this plan to align with plan elements.
- **Idaho Emergency Operations Plan - November 2021**
  - Incident Annex #7: Cybersecurity, as updated through this plan to align with plan elements.
- **Executive Order No. 2019-15**
  - Assignments of all-hazards prevention, protection, mitigation, response and recovery functions to State agencies in support of local and state government relating to emergencies and disasters.

Idaho's plan considers our remarkable cybersecurity enabling environment which includes:

- Governor's Cybersecurity Task Force – helping apply Idaho's world-leading cybersecurity capabilities to the cybersecurity challenges facing our citizens, businesses, critical infrastructure operators, and state and local governments.
- Idaho Cybersecurity Planning Committee – tasked with improving resilience and operationalizing the Task Force Report and SLCGP Cybersecurity Plan, allocating Idaho's State and Federal Cybersecurity Improvement Act funding.
- Idaho National Laboratories that bring expertise in operating technology security.
- Cybersecurity Infrastructure Security Agency (CISA) Region 10 representation to help us take advantage of its cybersecurity services and its U.S. - Computer Emergency Readiness Team (US-CERT)
- MS-ISAC and sector specific information sharing and analysis centers (ISAC) important to the state's critical infrastructure operators:
  - Aviation ISAC
  - Election Infrastructure ISAC
  - Electricity ISAC
  - Health ISAC
  - Information Technology ISAC
  - Oil and Natural Gas ISAC
  - Research and Education Networks ISAC
  - Transportation ISAC (surface, public, road)
  - Water ISAC
- Idaho Technology Council – the voice of Idaho's high tech private sector into the State's planning efforts.
- Idaho County Risk Management Program (ICRMP) – insures Idaho's jurisdictions for cyber and related risks.

- Idaho National Guard – a military organization with significant cybersecurity capabilities.
- Idaho Technology Authority (ITA) – able to focus its long-range technology work with state agencies on retiring out-of-service infrastructure with patchable replacements.
- Higher Education Institutions – eight schools that graduate technical and cybersecurity job candidates, and operate the Cyber Defense Center, and support science, technology, engineering, and math (STEM) programs.
- Associations that we will work with to support our stakeholders:
    - National Governors' Association
    - Western Governors' Association
    - Idaho Association of Counties (IAC)
    - Association of Idaho Cities
    - Coalition of City CISOs
    - Idaho Education Technology Association (IETA)
- Idaho State Executive Agencies, such as:
    - Idaho Information Technology Services
    - Idaho Criminal Intelligence Center

The following capabilities, controls, and methodologies are not yet practiced consistently in Idaho. Using the rating scale shown below, these capabilities are generally practiced at a fundamental or intermediate level by state-level agencies and departments in the executive branch that are served by the state's Chief Information Security Officer (CISO), while the capabilities in rural and frontier localities are mostly practiced at a foundational level, if at all. This dichotomy is why Idaho's cybersecurity strategy is particularly focused on our county, municipality, and frontier jurisdictions where good cyber practices are lacking, and the need is the greatest.

Cybersecurity Capability Ratings	
Foundational	Minimal awareness, policies, assessments, unpredictable management that is poorly controlled.
Fundamental	Some awareness, basic policies, some connection to COOP, but reactive and only process specific.
Intermediate	Cyber is well known, practiced & managed proactively at the organization level.
Advanced	Cyber is formally practiced, integrated into operations, measured, and controlled.

Manage, Monitor & Track

Some state agencies have inventoried their assets, but many jurisdictions have not done so and continue to use unsupported hardware and software. Asset tracking, treatment during employee on/offboarding, and patching is practiced - if at all - at a basic level across the state. Our goal is to help move local and state agencies from foundational to fundamental or from fundamental to intermediate through the SLCGP period of performance with an in-person outreach program, policy recommendations and templates, and "how to" guidance. To do so we will use the support of Idaho chapters of organizations like the National Association of Counties (NACo), and the Idaho Association of Cities (IAOC). Idaho will encourage local and rural jurisdictions to use their limited budget and state support to retire their unsupported technology. The State also intends to encourage and help localities take advantage of relevant services from CISA and MS-ISAC.

Monitor, Audit & Track

Most Idaho jurisdictions do not have the tools or means to attain and maintain situational awareness of cyber vulnerabilities and threats. Idaho's goal is to develop a best-of-breed Cybersecurity Fusion Center that will provide jurisdictions with a statewide capability for log analysis and enhanced local information sharing from multiple information feeds like MS-ISAC, sector-specific ISACs, CISA, and others. Then using data analytics to curate information, the Center will provide Idaho's jurisdictions with only relevant, actionable, and current alerts and communications. The Center will be the primary source of threat analysis and dissemination to our stakeholder jurisdictions. This centralized capability will employ cost and operational economies of scale to dramatically improve cybersecurity situational awareness across the state.

Enhance Preparedness

In general, the State of Idaho and most counties have a higher level of employee and system preparedness than local jurisdictions. The State of Idaho and the majority of counties conduct regular phishing training. The state government level system hardening, patching and configuration management is in place at an intermediate level. Some key systems have resiliency and are being backed up. However, local governments are largely at the foundational stage for these practices and cybersecurity awareness training and exercise are not broadly practiced. There is considerable technical debt in the systems of Idaho local and rural stakeholders and patching practice is hard to manage by the limited staff. To move to the next level, Idaho will develop and implement a basic asset inventory program at an early stage of our program so we get a whole-of-state view of the percentage of our infrastructure that must be upgraded. The State will be able to provide continuous system scanning and encourage our participating jurisdictions to develop an acceptable patching cadence. The state will stand up and provide a single source of information on an Internet site so localities can take advantage of training and exercise programs. Information will also be provided about programs already offered by CISA, MS-ISAC, and other non-government organizations (NGO).

Assessment & Mitigation

State policies require an assessment and mitigation capability, but vulnerability scans are in place only at some agencies. Penetration testing is being performed on most websites, but the state government level capability is modest and limited, typically executed only once every three years. Local governments scan and test at a foundational level, although the less populated counties typically do not have a defined program. Currently the Idaho National Guard provides some penetration testing, cyber resilience reviews and demonstrated exploit reviews for participating localities. Once established, the Idaho Cybersecurity Fusion Center will significantly expand these threat mitigations services to local and rural jurisdictions through promotion of services from CISA, MS-ISAC and other low cost or no cost providers, as well as a direct service program operated from the Center.

Best Practices & Methodologies

While Idaho State agencies execute the following practices and controls typically at a fundamental or advanced level, many local and rural entities do so at a foundational level. Over 1,000 of them are insured through ICRMP (Idaho Counties Risk Management Program), which will consider using incentives like lower premiums or reduced deductibles as incentives for insured localities to improve their practice in these control areas as Idaho's cybersecurity program rolls out:

- *Implement Multi-factor Authentication (MFA)*
  MFA is implemented in the state agency environment but not in all local jurisdictions. This capability will be promoted and supported in Idaho's in-person local outreach program over the 2024-27 period of performance, and beyond.

- *Implement Enhanced Logging*
  There is no SIEM at the state government level in Idaho, and enhanced logging is at a widespread foundational level statewide. Standing up the Idaho Cybersecurity Fusion Center will enable the State to offer enhanced logging and the dissemination of actionable information to the smallest local/rural/frontier jurisdictions beginning in 2024.

- *Data Encryption at Rest and in Transit*
  Encryption is mostly in place for data in transit and at rest for Idaho State agencies. At the local level encryption may be implemented in larger jurisdictions but is rarely implemented in smaller rural and frontier environments. This capability will be promoted

and supported as part of the in-person local outreach program over the 2024-27 period of performance, and beyond.

- *End Use of Unsupported/End-of-Life Software & Hardware Accessible from the Internet*
  End of life (EOL) systems exist both at the state and variously at the local level. Idaho's plan is to develop an asset inventory process for all Idaho jurisdictions to gain a perspective of the technical debt that will need to be retired, so the scanning and patching program can take hold. The State will start this inventory process in late 2023 through early 2024, as part of the outreach survey.
- *Prohibit Use of Known/Fixed/Default Passwords & Credentials*
  Strong password management is implemented at the state government level and in larger local jurisdictions, but it is not broadly practiced in small, rural and frontier communities. This will also be a capability that the State will promote and support in the in-person local outreach program over the 2024-27 period of performance, and beyond.
- *Ensure the Ability to Reconstitute System (Back-Ups)*
  Use of backups to reconstitute systems is implemented at most Idaho State government agencies and many larger local jurisdictions. Smaller jurisdictions have considerable gaps. The Idaho State agencies need to do failover testing; that element of this capability is practiced at a fundamental level. Workstations are not backed up, so Idaho State agencies often re-image affected machines. One of the core missions of the Idaho Cybersecurity Fusion Center will be to provide secure storage for participating Idaho jurisdictions' immutable back-ups, so the State can help them address ransomware risk effectively. This will begin to be available in late 2024.
- *Migration to the .gov Internet Domain*
  This migration is implemented at over 85% of the Idaho State agencies and many larger local jurisdictions. Idaho's smaller jurisdictions may use .org or personal Gmail accounts. Idaho will use both SLCGP and state funding as part of the State's plan to help encourage local communities to make this transition, with policy support and our in-person outreach program starting in 2024. Idaho will take advantage of CISA and MS-ISAC free and fee services to support this transition.

NIST Principles

While Idaho is standardizing on NIST 800-53, the administrative load of this standard may be too cumbersome for local and rural jurisdictions, some of which may be using the NIST cyber security framework (CSF), if they are using any framework at all. Idaho will consider NIST 800-171 as a more prescriptive and protection-focused framework that will be less challenging to accommodate for smaller jurisdictions. Idaho will make this decision, develop our plan implementation accordingly, and provide relevant guidance to our stakeholders beginning in late 2023.

Supply Chain Risk Management

A systematic supply chain risk management (SCRM) program is not in place at state government or local levels. Idaho will work with its legal and procurements departments to use NACo's "Recommended Contract Language for Technology and Privacy". This will allow us to develop approved, simple, standardized non-disclosure agreements (NDA) and Terms and Conditions language to guide state agencies and local entities in how they write cybersecurity responsibility into their vendor solicitations or contracts. In addition to promoting the use of free/fee CISA and MS-ISAC SCRM services, Idaho will also develop a simplified risk management process recommendation based on the Federal Information Processing Standards (FIPS) 199 for use by state entities to rate third party risk as low, moderate, or high impact across the confidentiality, integrity, and availability (CIA) construct and help them identify the highest risk vendors for risk mitigation. The State plans to roll this out in 2024.

Knowledge Bases of Adversary Tools & Tactics

Idaho participates in MS-ISAC at the state government level and has a contract with CISA for its associated threat awareness services. Awareness of and participation by local governments varies widely. As the State stands up the Idaho Cybersecurity Fusion Center beginning in late 2024, one mission will be to become the primary source for all threat data feeds from CISA, MS-ISAC, sector-specific ISACs, and other federal sources, supported by data analytics to ensure that the threat information the State provides to our participating jurisdictions is current, relevant, and actionable.

Safe Online Services

Idaho maintains a blacklist, but not a whitelist at the state government level. Practice varies at the local governments, but this capability is not broadly implemented. Transition to the .gov domain at Idaho State agencies is at the advanced threshold. Idaho's in-person local outreach program and participation in CISA and MS-ISAC services will also address this deficiency on a locality-by-locality basis, beginning in 2024.

Continuity of Operations Planning (COOP)

COOP practices in Idaho are at a foundational level. The state's agencies are immature in this practice and have not widely taken advantage of resources available through the Idaho Office of Emergency Management. Modest continuity support for K-12 school districts is provided by the Department of Education and State Board of Education. Seventeen (17) of Idaho's 44 counties have some elementary level of operational continuity plan. Small Idaho towns have a strong self-reliance ethos, feel they can take care of themselves and, if operationally disrupted, they typically seek help from neighboring towns. Engaging these towns to complete threat and hazard identification and risk assessments (THIRA) has been challenging. While there is a brief COOP section in the November 2021 State of Idaho Emergency Operations Plan that also speaks to a Continuity of Government (COG) and senior leader succession plan, these are more policies than plans. While most counties have an emergency management plan at some level, these do not typically include COOPs, and counties generally do not provide COOP support for their towns and communities.

To move from an uneven foundational posture to a functional all-of-state level will require Idaho to make education part of the in-person outreach team, use early adopter jurisdictions to demonstrate success, provide simple COOP tools, and offer deconfliction and plan reviews as part of the State's cybersecurity outreach program.

Workforce

Idaho enjoys a solid equilibrium between the number and quality of cybersecurity-capable job candidates and the demand for these resources across the State. The State has a strong cybersecurity talent market that is well balanced, even if we still have more openings than candidates. Idaho has some high school level programs, two-year technical schools and community colleges and four-year programs. The State tracks the number and type of technically capable graduates but not in a central, organized process. Yet there are challenges in recruiting both at state and especially the local level, where hiring is less of a budgeting issue and more of a local funding issue. The pipeline of new recruits favors Idaho's growing high tech private sector with competitive salaries in the Treasure Valley region. While there is somewhat of a talent drain to high wage areas like Seattle and Silicon Valley, the State is beginning to attract technical talent back to Idaho for cost of living and lifestyle reasons, as well as the strong cyber ecosystem that has developed in the state. The challenge for many local governments is their inability for local and county budgets to keep up with inflation, making hiring more difficult.

Rural areas remain specially challenged for cyber and IT skills. Idaho's in-person outreach plan will help address the dearth of technical skills in rural areas. The State will also support a "twilight career" program to attract civilian, military and government retirees who can agree to government pay levels, provide maturity, stability, and have an attraction for rural living.

The Division of Human Resources (DHR) is pursuing goals to develop workforce recruitment and retention strategies and support Information Technology Services' (ITS) cyber staffing efforts. The State works with our education sector to enhance their capacity to graduate, not only those with "technical" and "engineering" skills, but also with "people and process" attributes of cybersecurity. Idaho is considering government job descriptions with more realistic certification requirements, using on-the-job training, internships, apprenticeships, exploring tribal upskilling, and testing youth incentives (GenCyber camps and grant program, the Air Force's CyberPatriot program, the Department of Defense's Skill Bridge program, and Idaho National Lab's (INL) Summer Camps, for example).

Longer term, Idaho will map technical job classifications with the Workforce Framework for Cybersecurity (NICE) categorization framework and compare this to our graduate production rates, to coordinate the supply and demand of cyber skills in the state using a singular vocabulary. The Idaho Department of Labor's Occupational Wage Survey will be cross walked with Idaho's graduate skill levels and the NICE framework to produce a long-term strategy to ensure we develop and retain enough of the right kinds of cyber talent to support, not only our resource-rich entities, but find a way to attract the necessary skills into Idaho's rural/frontier environments. The State is implementing a new enterprise resource management (ERM) system that will upgrade career, job opening and application processes, making it easier to keep this market in balance and reduce the complexity of the Idaho government hiring process. With a strong benefit and pension program in Idaho government, it will still be easier to attract candidates to state government jobs than to local/rural positions. This emphasizes the importance of designing and rolling out our regional cybersecurity field team and supporting them to deliver the trusted in-region support our small towns will require.

Continuity of Communications & Data Networks

Idaho shares contiguous borders with six states (Montana, Wyoming, Utah, Nevada, Oregon, and Washington) and the Canadian territory of British Columbia. When regional/nation cyber events like Solar Winds occur, the State does a good, but reactive and reflexive "on the fly" job of sharing information widely among state, county and local authorities and its regional neighbors. To improve this communication, Idaho will develop formal memoranda of understanding (MOU) with neighboring states' cyber organizations, explore a cooperative agreement with British Columbia, and standardize a set of procedures for communicating with them and coordinating with CISA, MS-ISAC and other stakeholder organizations, via the Idaho Cybersecurity Fusion Center. The State will expand the use of Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) from DHS' Office of Emergency Communications that prioritizes calls over wireline networks and enables priority access over cellular communications networks. Finally, Idaho will consider the development with our regional partners of an interoperable communications plan.

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

Critical infrastructure is identified by the State of Idaho and Idaho National Labs to include agriculture, electric energy, emergency services, financial services, healthcare, critical manufacturing, water, transportation and information and communication technology. However, ownership and knowledge of threats to critical infrastructure is not well developed or coordinated, especially in the operational technology (OT) space. Much of this technology is in the hands of private operators, and there is a lack of a standard or framework used by the state, counties, localities and school districts for system inventorying, data classification, and risk assessment and remediation. There is over-reliance on security provided by OT equipment manufacturers, and unclear responsibility among IT staff and process engineers as to the “ownership” of cybersecurity in the OT environment. The State’s partnership with INL will continue to focus our OT cybersecurity efforts on the concept of consequence-driven, cyber-informed engineering (CCE) to ensure that engineers increasingly install and manage the components of their OT environments from a proactive cyber-readiness perspective.

Idaho works increasingly well with CISA and MS-ISAC on threats to both the IT and OT environments of those key resources. There is room for improvement in the information sharing process the State has in place with INL. Idaho is a member of InfraGard but needs to develop a concept of operations to better address, monitor and improve preparedness for attacks on our key resources and critical infrastructure locations, operations, and facilities, starting with a way to systematically inventory OT systems and their potential vulnerabilities. Local governments have limited visibility into their critical infrastructure. OT cyber risk identification is not mature in most cases. Idaho needs to address OT cybersecurity responsibility and how the State deals with governance among the numerous organizations that share a stake in securing Idaho’s key resources and critical infrastructure.

Cyber Threat Indicator Information Sharing

Idaho jurisdictions actively subscribe to information sharing services provided by MS-ISAC, CISA, etc. Idaho State agencies operate in this capability area at an intermediate posture, but at a foundational level at our local, rural and frontier jurisdictions. The State intends to materially ramp up that level of cooperation as one of the missions of the Idaho Cybersecurity Fusion Center. This capability will be built to bring in numerous threat intelligence data feeds, including those from CISA and the ISACs, use data analytics to identify the current, relevant, and actionable threat data that state, local, rural and frontier stakeholders can use to protect and respond to threat vectors that we collectively face. There will be a SOC/SIEM and log monitoring capability, since most small Idaho jurisdictions could not afford to implement this locally. CISA's Cyber information Sharing and Collaboration Program and its Automated information Sharing service, as well as MS-ISAC's Real-Time Indicator Feeds will be imported into the State operations center, as appropriate. Idaho will also formalize the process of developing and updating agreements, MOUs, and other types of cooperative arrangements among state, federal and industry data providers to ensure that our view is wide and appropriately inclusive. The strategy is to manage and interpret advanced threat data sharing as a core competence of the state, providing usable and productive output to State localities.

Leverage CISA Services

Some Idaho State agencies and local entities are aware and taking advantage of the broad range of free CISA services. These services are used across Idaho variably, opportunistically, and inefficiently. As described above, the Idaho Cybersecurity Fusion Center will include a comprehensive threat intelligence analysis capability, making use of many of these data sources, using Idaho State resources to procure the combination of free and fee threat indicator data sources, and generally relieving the participating localities from this competence. Idaho's local outreach program will encourage use of the most helpful no-fee services from CISA for those jurisdictions with the capacity to implement them, in addition to how the State handles this data at the Cybersecurity Fusion Center level. Among the bundle of CISA services, participating Idaho entities will be required to enroll in CISA's Cyber Hygiene Services and complete the Nationwide Cybersecurity Review (NCSR) self-assessment survey to help evaluate their cybersecurity posture. Both efforts will be supported by Idaho's outreach program to local, rural, and frontier jurisdictions.

Information Technology & Operational Technology Modernization Review

Idaho's current process for IT/OT modernization is haphazard and practiced at wide levels of planning and effect. At the Idaho State agencies level, IT asset inventory enables them to manage their technology lifecycle, keep technical debt to a minimum, and keep infrastructure at a protectable level. Most Idaho State agencies and departments only address OT modernization in their camera and building operations areas (e.g., Department of Transportation and Corrections). Counties and larger municipalities which operate water utilities, public works departments, and transportation authorities must also protect the operational technology environments of their critical infrastructure sectors like agriculture, critical manufacturing, and electric energy. IT modernization efforts are far better planned and implemented than OT modernization. Awareness and responsibility for OT security falls between IT departments and process/operations engineers, often with no clear ownership, and only some of this environment is government owned and managed. The State of Idaho intends to closely coordinate with identified stakeholders to improve awareness and training around technology modernization as a foundation to better security, and awareness of IT/OT risks to government agencies, departments, and operations. The State will center on NIST IT/OT controls guidance in this process through the CCE approach that couples process engineering and cybersecurity for installed OT infrastructure.

Cybersecurity Risk & Threat Strategies

Idaho government entities currently utilize the Idaho Association of Counties, Association of Idaho Cities, as well as formal and informal relationships with CISA, MS-ISAC, and the Emergency Management Assistance Compact (EMAC) - a national interstate mutual aid agreement that enables states to share resources during times of disaster. The State wants to formalize these and other relationships, not only with the 44 Idaho county governments and capable municipalities, but also with those of our six contiguous states – Montana, Wyoming, Washington, Oregon, Utah, and Nevada - and British Columbia to our north. Idaho shares energy grids and pipeline infrastructures in this international and interstate region, in which the State needs to approach information sharing in a more formal and better documented way.

Rural Communities

Because many of Idaho's 44 counties and 201 municipalities are rural or frontier, the centerpiece of the State's multi-year SLCGP plan is super-serving these autonomous stakeholders with centrally provided, but locally delivered cybersecurity services and technology solutions. The State will explore a model to hire six (6) IOEM personnel to work and live in each of the six state geographic regions. This model is critical to developing the local trust of local jurisdictions who may be reluctant to use state-provided and state-encouraged programs. Idaho's cybersecurity program will be a multi-year local and rural-targeted effort to elevate the cyber posture of its 35 rural counties (of 44 total) and its 193 rural and frontier municipalities (of a total of 199). This can be accomplished by enlisting the support of Idaho State agencies, INL, better prepared local governments, and Idaho's remarkable ecosystem of NGOs, higher education, and private sector entities to help boost adoption of the State's services program.

Idaho's rural community initiatives will be built around a realistic assessment of local needs and cooperation. Initiatives will also be built around on-site in-person outreach by trusted in-state parties, possibly through each county's emergency management point of contact. Idaho currently has key IT personnel who have gained the trust of local governments in helping them with their cybersecurity and technology challenges. The State plans to formalize this program, naming these resources to each of our six regions in the state, and implement the program carefully, by demonstrating success, making it easy to opt in and consider incentives for participation.

FUNDING & SERVICES

Idaho aspires to build a best-in-class long term cybersecurity ecosystem. To do so, the State must first address the insufficient cybersecurity posture that characterizes many rural and frontier stakeholders – as the foundation upon which we will build our ambitious end-state goal.

Idaho has a cybersecurity divide between comparatively well-prepared state agencies and departments and some larger localities, and other less equipped rural and frontier government jurisdictions and school districts. The State's program will be responsive to the clear feedback we received in preliminary outreach to those "have-not" stakeholders for state-provided cybersecurity services instead of cash sub-awards, as the optimal way to bring Idaho's disparate environment into better equilibrium.

Having been awarded $2.4 million in the 2022 SLCGP Notice of Funding in 2022 and $5.2 million in the 2023 NOFO, Idaho expects to also receive additional funding through 2024 and

2025 SLCGP NOFOs. The State also expects to receive funding from Idaho's State Homeland Security Grant monies, and to be awarded a portion of Idaho's Infrastructure Investment and Jobs Act (IIJA) funding.

Idaho has high expectations for the improvements it can make for the whole-of-state cyber posture. To meet these expectations, the State will additionally deploy funds from these federal sources, as well as in-state budget funding from the Idaho Legislature to build the right mix of services, delivery infrastructure, support system, and measurement capability that CISA, the Federal Emergency Management Agency (FEMA), Idaho's Legislature, and our own program office require for success. The State will address all gaps, vulnerabilities and needs identified in this plan through projects approved by the Cybersecurity Planning Committee that are sustainable and benefit the largest number of Idaho stakeholders.

Distribution to Local Governments

Idaho's approach to address the challenge of bringing local, rural and frontier stakeholders from the non-existent or foundational cybersecurity posture to at least a fundamental level is to focus almost exclusively on developing and providing the essential cybersecurity support and technical services that these government entities can never implement without state-guided programs. The State does not envision a grant sub-funding cash distribution, because preliminary outreach has clearly indicated that short term cash awards will not address systemic posture and capability gaps for our under-resourced jurisdictions.

The State expects to provide the opportunity for our local and regional governments and school districts to participate in human support services and technology services - provided by skilled internal, contract, federal, multi-state and NGO personnel utilizing in-place resources as much as possible.

The successful uptake and adoption of those technology services requested by Idaho localities will depend on a carefully planned, staffed, and executed outreach and support system provided by trusted Idaho in-person resources. IT representatives who live and operate in IOEM's six regional field offices will help us provide this "last mile" technical assistance and implementation that will be the driving factor for successful participation rates by our local, rural, and frontier communities.

Eighty percent (80%) of Idaho's 44 counties are rural and 96% of our 201 municipalities are classified as rural. Our 124 towns with populations less than 1,000 are a mix of rural and frontier communities with a median population of 371 residents often quite sparsely settled across their regions. Idaho will thus easily exceed the 25% threshold for grant funding to benefit rural areas, as required by the State and Local Cybersecurity Improvement Act.

See Appendix B: Project Summary Worksheet for Idaho's preliminary list of services, capabilities and support we plan to provide our local, rural, and frontier government grant beneficiaries.

ASSESS CAPABILITIES

As documented in **Appendix A: Cybersecurity Plan Capabilities Assessment**, Idaho's whole-of-state strategy is built around the distinct dichotomy between the resource and cyber capability-rich "Treasure Valley" and the central and panhandle regions that are home to largely rural and sometimes often frontier communities with comparatively no or poor cybersecurity awareness, engagement level, resources, or capabilities. This dearth of cybersecurity capacity is coupled with a level of local independence and self-reliance that will require Idaho's program to meet the needs and capacities of the State's local/rural/frontier communities.

We planned and facilitated a preliminary series of group assessment meetings in Boise, attended both in person and via video conference, with representative county leaders, local and large and small town technical and management leaders, and relevant state agency personnel. These were open, participatory assessment workshops and interviews to gauge the cybersecurity issues, problems, needs, and risk factors across Idaho stakeholders. They indicated how acute the cybersecurity problems are across especially smaller, rural and frontier governments and identified why cash sub-grants are not valued at the local level as affecting their long-term needs is a materially sustainable way.

Idaho complemented these fact-finding workshops with in-depth interviews with the State CISO and Deputy CISO, to ensure we included their state level assessment of the cybersecurity posture of both executive branch state agencies and departments and local communities. We spoke with numerous state agency experts to get a fulsome understanding from which to develop our program.

The State will design a simple, easy to complete cybersecurity capabilities and needs assessment survey to take workshop findings to the whole of state so we can validate and document our preliminary capabilities and needs assessment findings. It will be built around a basic framework like the CIS Controls, as an example. The survey will be self-completed by those more sophisticated jurisdictions. The State will provide personnel to assist less capable entities understand and complete the process, by telephone and some rural outreach, using field-placed local trusted personnel. An intended outcome of this process is not only to obtain the documentation we need for optimal program design, but also to seed the outreach process, begin developing our statewide contact network, and begin to establish the local trust necessary for long term program success.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

The Idaho Office of Emergency Management was granted the statutory authority by the Governor for implementing and managing programs and grants that will further the goals and objectives described in the 2022 Governors' Cybersecurity Task Force report. The Governor also named the IOEM to serve as both the State Administrative Agency (SAA) and the lead implementation organization for our efforts under the SLCGP. While the IOEM's Planning, Grants and other Section Chiefs have strategic and directional responsibility for the work Idaho puts into this grant program during its multi-year period of performance, IOEM will coordinate operational roles and responsibility with the following stakeholders based on their expertise, capacity, and availability:

- Idaho Office of Emergency Management
- Office of the Governor
- Information Technology Services
- Office of the Secretary of State (SOS)
- Idaho National Guard
- Idaho State Board of Education
- Division of Human Resources
- Representative County, Municipal, Rural and Frontier jurisdictions
- Expert Non-Government Organizations
- Idaho National Labs
- CISA Region 10 Idaho Liaison
- Idaho County Risk Management Program
- Idaho Technology Authority
- County, City, CIO and CISO Associations

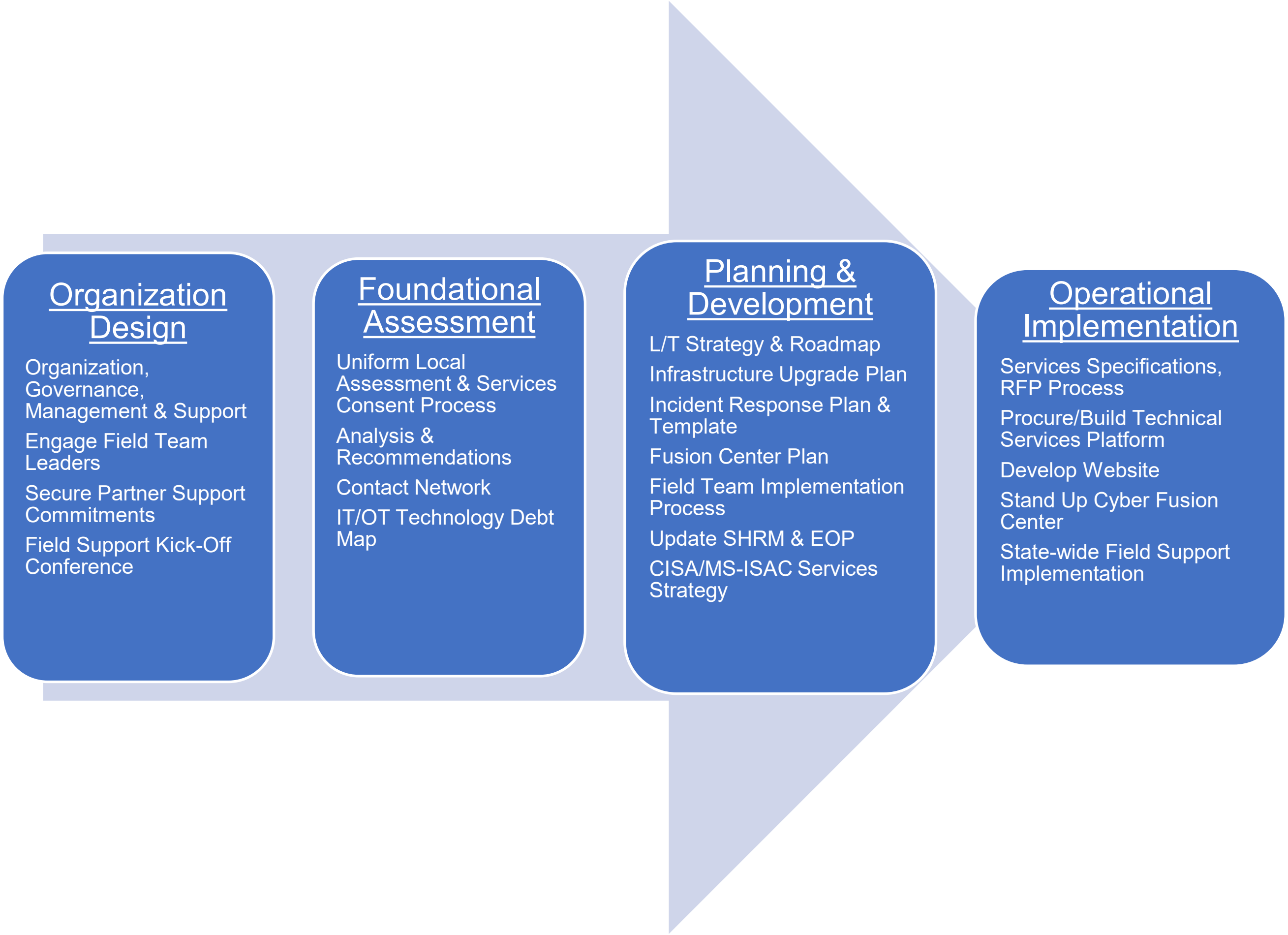
In addition to the metrics that we will use to report progress and effectiveness of our program under the SLCGP, Idaho will develop other internal metrics to support our statewide program roll-out.

To counter the hesitancy to leverage centrally provided programs, in a state where autonomy and self-reliance is highly valued, we will develop a set of Adoption Demonstration Metrics to use as part of our strategy for creating optimal awareness and adoption of cybersecurity services by our local government jurisdictions. When using trusted agencies, organizations, and partners to demonstrate trial, adoption, use, and satisfaction with our centrally provided services, a good way to incent other jurisdictions to participate and consent to one or more of these services is to show them these "success metrics".

Idaho is aware that achieving our cybersecurity goals and executing our strategy will require more than four years of SLCGP funding. We intend to ask our Legislature to further invest in the foundational pillars of our long-term cybersecurity roadmap, recognizing that we will need to show measurable success as the basis for additional Idaho state funding. We will create Success Metrics for In-State Funding, to demonstrate how in-state funding is paying measurable dividends.

Resource Overview and Timeline Summary

The State of Idaho will fund most of the activities encompassed in the organizational design, foundational assessment, and planning and development stages of our plan from our 2022 and 2023 SLCGP grant allotments. Operational implementation of the centerpiece of our plan to focus on improving the cybersecurity posture of local, rural and frontier jurisdiction in Idaho through state-provided cybersecurity technology services will be funded by 2023 and 2024 SLCGP grant allotments supplemented, as necessary, with state-provided capital expenditure (CapEx) funds.



Organization Design

- Organization, Governance, Management & Support
- Engage Field Team Leaders
- Secure Partner Support Commitments
- Field Support Kick-Off Conference

Foundational Assessment

- Uniform Local Assessment & Services Consent Process
- Analysis & Recommendations
- Contact Network
- IT/OT Technology Debt Map

Planning & Development

- L/T Strategy & Roadmap
- Infrastructure Upgrade Plan
- Incident Response Plan & Template
- Fusion Center Plan
- Field Team Implementation Process
- Update SHRM & EOP
- CISA/MS-ISAC Services Strategy

Operational Implementation

- Services Specifications, RFP Process
- Procure/Build Technical Services Platform
- Develop Website
- Stand Up Cyber Fusion Center
- State-wide Field Support Implementation

IOEM has engaged a cybersecurity planning contractor that helped develop this plan and will guide the development of Idaho's 5-year cybersecurity strategic plan and roadmap, develop our incident response (IR) plans, and provide local outreach, develop the strategy and operating policies for the Idaho Cybersecurity Center, and update the cybersecurity chapter of our State Hazard Mitigation Plan so it aligns with our new plans. SLCGP funds will support this engagement. The State may further engage this and other contractors to supplement the resource constraints at the IOEM, ITS, and other coordinating divisions, departments, and agencies for resource-intensive efforts such as outreach program development and management, coordinating our multitude of government, NGO, and educational partnerships, project and program management and oversight, and field support -our operational expenses (OpEx).

The State’s human resources expenditures for the field support team staff and contract “last mile” implementation work, as well as Fusion Center staffing, will be a large long term expense category funded by the IOEM through state funding to the extent personnel expenditure are non-covered SLCGP expenditures. Idaho expects the CapEx costs of leasing and equipping the physical site to stand up the Idaho Cybersecurity Fusion Center and secure compartmented information facility (SCIF) will be largely funded by the state.

Metrics

Our primary metrics are designed to demonstrate internally and to CISA and FEMA that our program objectives and sub-objectives are clear and their implementations measurable, using measures that are relevant and evaluative.

Cybersecurity Plan Metrics - SLCGP			
Program Objectives	Program Sub-Objectives	Metrics	Metric Description (details, source, frequency)[2]
1.1 Establish cybersecurity as a whole-of-state long-term strategic initiative.	Create a 5-year state cybersecurity strategy and roadmap.	Strategy Developed	Strategy and roadmap developed by IOEM and accepted by the Director, once, 1H24.
	Encourage Executive Branch proclamation of the Cybersecurity 5-Year Plan as an operational imperative.	Governor's Proclamation	Official proclamation published by Governor, once, 1H24.
1.2 Communicate cohesively and repetitively about cybersecurity risk awareness, literacy, and management so everyone in the state understands their responsibility for security.	Develop a cybersecurity awareness program to apprise stage agencies, localities, NGOs, military, education and critical infrastructure entities and the Idaho public about the cyber initiative and communicate its successes.	1. Set of adoption and success metrics. 2. Publicity program launched.	1. Local participation success metrics adopted by IOEM, once, 2H23-1H24. 2. Published by IOEM/PIO, quarterly, starting 1H24.
	Create/update a cybersecurity website as the nexus for all cyber resources, information, and services.	Website launched and updated.	Website goes live by 1H24 and updated monthly by IOEM.
1.3 Provide the information, tools, and support to local governments – especially rural and frontier jurisdictions – necessary to protect their systems and information from most cybersecurity threats.	Create and implement a statewide cybersecurity support and implementation organization to provide "last mile" technology integration for all participating local, rural, frontier and tribal entities.	1. Number of regional team staff named. 2. Support program developed.	1. Team organization and charter formalized by IOEM once in 1H24. 2. Regional leads hired, six each, 1H24. 3. Uniform survey launched, once in 2H23.
	Partner with trusted stakeholder organizations to communicate the value of the cyber initiative to their constituents.	Partnerships formalized.	No. of partnerships formed (with Amer. Association of Retired Persons (AARP), ITC, Higher Ed consortium & pilot jurisdictions), 2H23-1H24.
1.4 Increase adoption of basic cybersecurity practices across the state.	Partner with CISA and MS-ISAC on an Idaho bundle of free/fee services for subscription by local jurisdictions.	Idaho-centric services bundle published.	IOEM, CISA, and MS-ISAC jointly publish a service list, annually, starting 2H24.

[2] The timing of our metrics is expressed in calendar year quarters.

Cybersecurity Plan Metrics - SLCGP			
Program Objectives	Program Sub-Objectives	Metrics	Metric Description (details, source, frequency)[2]
	Create a cybersecurity awareness & training program in the field support team to be implemented in their six regions.	Awareness & training program formally approved.	Program formalized and approved by IOEM once, 1H24.
	Support the posture improvement of local jurisdictions via hands-on physical and virtual outreach by the field team.	Percent of regions participating.	For each of six regions, the percentage of local entities accepting outreach services, annually starting 1H24.
2.1 Ensure that all state agencies and local jurisdictions understand their current cybersecurity posture.	Distribute and evaluate a uniform cybersecurity assessment to all local, rural, and frontier jurisdictions.	Percent of surveys completed.	1. Percent of uniform cyber surveys completed and submitted annually, starting 2H23-1H24. 2. Percent improving by one rating level annually.
	Conduct tabletop exercises (TTX) to demonstrate to local officials the criticality of cyber budgeting and funding.	Number of TTXs facilitated.	Number of TTXs facilitated either virtually or on-site by field teams annually, starting 1H24.
	Offer CISA and MS-ISAC testing and assessment services.	Number of entities participating in CISA's NCSR.	Percent of local entities that subscribe to the required NCSR, annually, starting 1H24.
		Number of entities participating in CISA's CyHy services.	Percent of local entities that subscribe to the required CyHy, annually, starting 1H24.
2.2 Develop an IT and security workforce and talent pipeline that meets the demands of our state and local government departments, agencies, and jurisdictions.	Develop a whole of state technical workforce annex to the 5 - year strategy.	Annex developed.	Accepted by the DHR, Board of Ed, IOEM, Higher Ed Consortium, ITC, that agree, once by 1H24.
	Collaborate with the Idaho private sector on a workforce loan program.	Program developed.	Program formalized/accepted by the ITC, DHR, Board of Ed, and IOEM, once by 2H24.
2.3 Bring everyone into the room and foster a shared community of cyber information sharing and support.	Design a cybersecurity fusion center strategy and operating policies.	Strategy and policy document.	Accepted by IOEM once, 2H23-1H24.
	Secure state funding for the fixed costs of the center.	Fixed cost funding.	Source identified once in 1H24.
	Stand up and operate the fusion center.	Formal dedication.	Dedication ceremony, once by the Governor and Director of IOEM, once in 2024.

Cybersecurity Plan Metrics - SLCGP

Program Objectives	Program Sub-Objectives	Metrics	Metric Description (details, source, frequency)[2]
2.4 Develop, maintain, and enhance an inventory of Idaho's critical infrastructure and key resources.	Inventory critical infrastructure (CI) and key resource (KR) sites statewide.	Percent complete.	Percent of CI and KR installations inventory completed by IOEM, INL and ITA, once, 1H24.
	Assess the currency/debt of IT and OT infrastructure.	Assessment completion date.	Date assessment completed, once by IOEM, INL, ITA in 2H-3H24.
	Create a modernization plan.	Plan completed.	Date modernization plan accepted by Gov. Task Force, once 2H24.
3.1 Sustain our deeply collaborative and inclusive public/private partnerships.	Formalize and deconflict the cyber roles of each public/private collaborative organization.	Cyber deconfliction.	Percent of Idaho organizations adopting report, once by all, 1H24.
	Develop partner relationships with organizations that have credibility with Idahoans.	Partnership defined.	Number of partnerships formalized, once by IOEM in 1H24.
3.2 Encourage cross-sector participation and dialog in planning, decisioning, and execution.	Hold a statewide "visioning" session to bring all stakeholders into the cybersecurity strategy planning conversation.	Participation.	Number of Idaho stakeholder organizations that attend the session, once 2H23, by IOEM.
	Plan operational, observer and research seats for the fusion center, encompassing the entire ecosystem.	Fusion Center seats.	Percent of visioning attendees seated in fusion center, once by IOEM, 2024.
3.3 Develop a cyber workforce optimization strategy.	Create a "twilight" career program for technically capable retirees.	Twilight program.	Date program formalized by DHR, IOEM, once in 2024.
	Study a rural technical staffing program for new graduates.	Rural staffing.	Study initiation by IOEM, ITC, and Higher Ed Consortium, once, 2024.
4.1 Develop and establish an organizational and governance model that efficiently connects the cybersecurity program elements.	As part of the 5-Year strategy, clarify and deconflict missions, roles and responsibilities, and decision matrices among relevant state agencies.	Signatories.	Percent of cyber-relevant organizations and entities that are signatories, managed by IOEM once in 2024.
4.2 Encourage local government jurisdictions to fund reasonable hardware replacement budgets.	Develop an IT/OT modernization plan from 2.4 outcomes.	Modernization plan.	Date signed by IOEM, INL, and ITA once in 2H24.
	Secure Idaho and federal funding to retire out of support infrastructure at municipalities and critical infrastructure.	Funding.	Sufficient funding committed from grants and legislation by IOEM once in 2H24.

Cybersecurity Plan Metrics - SLCGP			
Program Objectives	Program Sub-Objectives	Metrics	Metric Description (details, source, frequency)[2]
4.3 Ensure that we solicit expert policy perspectives, recommendations, and hands-on participation from our rich array of partner organizations throughout Idaho.	Create cybersecurity policy objectives to be researched by partners, higher education, and federal labs.	Policy.	Formal policy recommendations submitted to IOEM by stakeholder researchers, annually, starting 2024.
	Expand the Cybersecurity Planning Committee to include additional voices.	Membership.	Number of member stakeholders added to the Committee by IOEM, once in 2024.

Appendix A: Cybersecurity Plan Capabilities Assessment

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts.	Some Idaho State agencies have inventoried their assets, but many jurisdictions may not have done so and continue to use unsupported hardware. Assets tracking, treatment during employee on/offboarding, and patching is practiced - if at all - at a basic level across the state. Our goal is to help move local and state agencies from foundational to fundamental and or from fundamental to intermediate through the SLCGP period of performance with in-person outreach program, policy recommendations, and "how to" guidance. To do so we will use an asset inventory tool, with the help of organizations like the Idaho Association of Counties, the Idaho League of Cities, etc.	Fundamental To Intermediate	Foundational To Intermediate		
2. Monitor, audit, and track network traffic and activity	Most Idaho jurisdictions do not have the tools or means to attain and maintain situational awareness of cyber vulnerabilities and threats. Idaho's goal is to develop a best-of-breed Cybersecurity Fusion Center that will provide jurisdictions with a statewide capability for log analysis and enhanced local information sharing from multiple information feeds like MS-ISAC, sector-specific ISACs, CISA, and others.	Foundational To Intermediate	Foundational To Intermediate		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	In general, the State of Idaho and most counties have a higher level of employee and system preparedness than local jurisdictions. The State of Idaho and the majority of counties conduct regular phishing training. The state government level system hardening, patching and configuration management is in place at an intermediate level. Some key systems have resiliency and are being backed up. However, local governments are largely at the foundational stage for these practices and cybersecurity awareness training and exercise are not broadly practiced. There is considerable technical debt in the systems of Idaho local and rural stakeholders and patching practice is hard to manage by the limited staff. To move to the next level, Idaho will develop and implement a basic asset inventory program at an early stage of our program so we get a whole-of-state view of the percentage of our infrastructure that must be upgraded. The State will be able to provide continuous system scanning and encourage our participating jurisdictions to develop an acceptable patching cadence.	Intermediate	Foundational		
4. Implement a process of continuous cybersecurity risk factors and threat	Vulnerability scanning is performed only at some state agencies. Pen testing is being performed on most websites, but the state level capability is modest and limited, typically only once every	Fundamental /Intermediate	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	State Govt. Select capability level from: Foundational Fundamental Intermediate Advanced	County, City, Tribal Gov. Select capability level from: Foundational Fundamental Intermediate Advanced	Project # (s) *(If applicable – as provided in Appendix B)*	Met
mitigation. practices prioritized by degree of risk	three years. Local governments scan and test at a foundational level, although the less populated counties typically do not have a defined program. Idaho will greatly expand threat mitigation services especially at the local and rural levels through promotion of services from CISA and MS-ISAC, and other partners.				
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)					
a. Implement multi-factor authentication	MFA is implemented in the state agency environment but not in all local jurisdictions. This capability will be promoted and supported in Idaho's in-person local outreach program over the 2024-27 period of performance, and beyond.	Intermediate	Foundational		
b. Implement enhanced logging	Enhanced logging is at a widespread foundational level statewide. We will stand up the Idaho Cybersecurity Fusion Center in the 2024/25 timeframe, which will enable us to offer enhanced logging and the dissemination of actionable information to the smallest local/rural/frontier jurisdictions.	Foundational	Foundational		
c. Data encryption for data at rest and in transit	Encryption is mostly in place for data in transit and at rest at our state agencies. Local area encryption is implemented in the larger jurisdictions, but rarely in smaller rural and frontier	Intermediate	Foundational / Fundamental		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
	environments. This capability will be promoted and supported in our in-person local outreach program over the 2024-26 period of performance, and beyond.				
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	EOL systems exists both at the state and variously at the local level. Our plan is to develop an asset inventory process for all Idaho jurisdictions to gain a perspective of the technical debt that will need to be retired, so our scanning and patching program can take hold, starting the process in late 2023 through early 2024, as part of our outreach survey.	Intermediate	Foundational / Fundamental		
e. Prohibit use of known/fixed/default passwords and credentials	Strong password management is implemented at the state level and at some local jurisdictions. It is poorly practiced in many small, rural and frontier communities. This will also be a capability that we will promote and support in our in-person local outreach program over the 2024-26 period of performance, and beyond.	Intermediate	Foundational / Fundamental		
f. Ensure the ability to reconstitute systems (backups)	Use of backups to reconstitute systems is implemented at most state agencies and larger local jurisdictions. Smaller jurisdictions have considerable gaps. Failover testing is needed. Re-imaging for new hires is practiced instead of need-to-know provisioning. The Idaho Cybersecurity Fusion Center will provide secure storage for all Idaho jurisdictions' immutable back-ups, so we can help them address ransomware risk effectively. This will begin in late 2024-2025.	Fundamental/ Intermediate	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
g. Migration to the .gov internet domain	Migration to .gov is implemented at over 85% of the state level and larger local jurisdictions. Idaho's smaller jurisdictions may use .org, may not even have a domain, and may use personal Gmail accounts for government business. Idaho will use both SLCGP and state funding as part of our plan to help local communities make this transition, with policy support and our in-person outreach program starting late 2023-2024.	Advanced	Foundational to Fundamental		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	Idaho maintains a blacklist at the state level, but not a whitelist. Practice varies at the local government level, but is poorly implemented, if at all. Transition to the .gov domain at the state level is at the advanced threshold. Our in-person local outreach program will also address this deficiency on a locality-by-locality basis, beginning in early 2024.	Intermediate	Foundational		
7. Ensure continuity of operations planning and conducting exercises	Many states and some local agencies maintain and test COOPs. Idaho's local resilience ethos needs to be supplemented with far broader continuity practices. We will explore adopting a well-tested cloud-based system like Bold Planning Solutions with a license that enables all counties and localities to develop basic COOPs. Once this is implemented, with hands-on help for localities on how to do a simple BIA, we will move to the process of helping communities develop simple IT disaster recovery (DR) plans to support their operational resilience. We will provide tabletop	Fundamental/ Intermediate	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
	exercise scenarios and "train the trainer" services for larger jurisdictions and will offer these services virtually or on-site with trusted local Idahoans staffing our in-person outreach program.				
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)	Idaho has a strong cybersecurity talent market and has fair equilibrium between the demand for cyber talent and the production of talent from high school programs, two-year technical schools and community colleges and four-year programs. Yet there are challenges in recruiting both at state and especially the local level, where cyber awareness is low, cyber hiring poorly practiced, and funding to hire qualified staff is inadequate. The pipeline of new recruits favors Idaho's considerable high tech private sector with competitive salaries in the Treasure Valley region. While there is somewhat of a brain drain to high wage areas like Seattle and Silicon Valley employers, Idaho's favorable cost of living and lifestyle and the strong cyber ecosystem that has developed in the state, is starting to attract cyber talent here. Rural areas require support to identify funding for qualified hiring. Our in-person outreach plan includes regionally deployed, trusted cyber support staff to address the dearth of technical skills in rural areas, supported by longer term programs to ensure we create, attract, and maintain a sufficient cyber workforce.	Intermediate	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	Idaho shares contiguous borders with six states and Canada. When regional/nation cyber events like Solar Winds occur, the state does a good, but reactive "on the fly" job of sharing information widely among state, county and local authorities and its regional neighbors. To improve this communication, we will develop formal MOUs with our neighboring states' cyber organizations, explore a cooperative agreement with British Columbia, and standardize a set of procedures for communicating with them and coordinating with CISA, MS-ISAC and other stakeholder organization, via the Idaho Cybersecurity Fusion Center.	Fundamental	Foundational		
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	Critical infrastructure is identified at the state level, where we work increasingly well with CISA and MS-ISAC on threats to both the IT and OT environments of those key resources. While we work with Idaho National Labs for its exceptional OT expertise in critical infrastructure, there is room for improvement in that information sharing process. Idaho needs to develop a concept of operations to better address, monitor and improve our preparedness for attacks on our key resources and critical infrastructure locations, operations, and facilities - starting with a way to systematically inventory OT systems and their potential vulnerabilities. Local governments have	IT: Intermediate OT: Fundamental	IT: Fundamental OT: Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
	limited visibility into their critical infrastructure, and OT risk identification is not mature in most cases.				
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	While Idaho subscribes to some services provided by CISA, our practice is not as strategically managed as it should be. We intend to materially ramp up that level of cooperation as one of the missions of the Idaho Cybersecurity Fusion Center. This capability will be built to bring in numerous threat intelligence data feeds, use data analytics to identify the current, relevant and actionable threat data that our state, local, rural and frontier stakeholders can use to protect and respond to threat vectors that we collectively face. There will be a SOC/SIEM and log monitoring capability, since most small Idaho jurisdictions can never afford to implement this locally. CISA's Cyber information Sharing and Collaboration Program and its Automated information Sharing service, and MS-ISAC's Real-Time Indicator Feeds will be imported into our center.	Intermediate	Foundational		
12. Leverage cybersecurity services offered by the Department	MS-ISAC's free and fee services are used across Idaho variably. As we described above, our Idaho Cybersecurity Fusion Center will include a comprehensive threat intelligence analysis capability, making use of many of these data sources. Our local outreach will further encourage use of at least the no-fee services from CISA.	Intermediate	Foundational /Fundamental		
13. Implement an information technology	Idaho's current process for IT/OT modernization is uneven and practiced at wide levels of planning	Fundamental	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	State Govt. Select capability level from: Foundational Fundamental Intermediate Advanced	County, City, Tribal Gov. Select capability level from: Foundational Fundamental Intermediate Advanced	Project # (s) *(If applicable – as provided in Appendix B)*	Met
and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	and effect. At the state level, our IT asset inventory enables us to manage our technology lifecycle, keep technical debt to a minimum, and keep infrastructure at a protectable level of recency. Most state agencies and departments only address OT modernization in their camera and building operations areas (e.g., Department of Transportation [DoT] and Corrections). At counties and larger municipalities that operate water utilities, public works departments, and transportation authorities, IT modernization efforts far exceed OT modernization, as awareness and responsibility for OT security falls between the responsibility realms of IT departments and process/operations engineers. We plan to work more closely with Idaho National Labs, CISA and MS-ISAC to improve awareness and training around technology modernization as a foundation to better security, and the nature of IT/OT risks to our government agencies, departments, and operations.				
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	Idaho government entities currently utilize the Idaho Association of Cities, Idaho Association of Counties, as well as formal and informal relationships with CISA, MS-ISAC, and the EMAC - a national interstate mutual aid agreement that enables states to share resources during times of disaster. We want to formalize these and other relationships, including not only our 44 county	Fundamental	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
	governments and capable municipalities, but also those with our six contiguous states and British Columbia to our north with a review of MOUs, agreements, and a strategy around this, as a cohesive set of coordination processes.				
15. Ensure rural communities have adequate access to, and participation in plan activities	Because our 44 counties and 201 municipalities skew heavily to rural and frontier, the centerpiece of our multi-year SLCGP plan is to super-serve these autonomous stakeholders with centrally provided, but locally delivered cybersecurity services, both personnel-based and technology-based. We will explore a model to name staff for our six state regions, with administrative and funding connection to IOEM, but operational connection to their regions. This model is critical to developing the local trust of our stakeholders who otherwise resist state-provided and state-encouraged programs.	Fundamental	Foundational		
16. Distribute funds, items, services, capabilities, or activities to local governments	Idaho's strategy will be to exceed the 80% rural grant beneficiary requirement by standing up, staffing and funding a local/regional trusted outreach program to provide human and technology services to all receptive Idaho local, rural and frontier jurisdictions in the state. We heard from them in our initial outreach that sustained security and support services from the state represents far more value than a short-term cash sub-grant infusion. Services like local network development, assessment, and training	Fundamental	Foundational		

COMPLETED BY THE STATE OF IDAHO					FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**State Govt. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**County, City, Tribal Gov. Select capability level from:** **Foundational** **Fundamental** **Intermediate** **Advanced**	**Project # (s)** ***(If applicable – as provided in Appendix B)***	**Met**
	as well as back-up storage, a secure network and a centralized SOC/SIEM with threat data analysis and integration will be rolled out. Success will be demonstrated by in-state success stories, and technical implementation support will be provided by trusted staff experts assigned to each of our six regions so the program will be "by Idahoans, for Idahoans" in an approach that breaks the mold of rural hesitancy to government programs. **See Appendix B for more details.**				

Appendix B: Project Summary Worksheet

Project Number	Project Name	Project Description	Related Required Element Number addressed by the project	Estimated Cost	Status (future, ongoing, complete)	Priority (high, medium, low)	Project Type (plan, organize, equip, train, exercise)
1	Establish Field Team	Design implementation team strategy, organization, management, & support strategy & identify & begin the engagement process for six (6) regional liaisons.	3, 4, 5 a-g, 8, 10, 11, 13, 14, 15, 16	TBD	Future	High	Organize
2	Secure Partnerships	Identify NGO, military, not-for-profit, education sector and associations as trusted partners to support local services awareness and adoption.	4, 8, 9, 10, 11, 12, 13, 14, 15, 16	TBD	Ongoing	High	Organize
3	Field Support Conference	Kick off the field implementation and support and operations planning with Boise conference.	14, 15, 16	TBD	Future	Medium	Plan
4	Foundational Assessment & Consent - Design	Design a uniform assessment for local, rural, and frontier jurisdictions including capabilities & needs, gaps to CIS, asset aging inventory, use of/readiness for CISA & MS-ISAC service, multiple points of contact (political & technical), formal consent mechanism, and future services consent process.	1, 2, 3, 4, 5 a-g, 6, 7, 8, 10, 11, 12, 13	TBD	Future	Medium	Plan
5	Foundational Assessment & Consent - Implementation	Distribute the assessment, reach out to all jurisdictions to offer completion support, analyze results, and make further program recommendations; supplements the preliminary outreach already completed.	1, 2, 3, 4, 5 a-g, 6, 7, 8, 10, 11, 12, 13	TBD	Future	Medium	Plan
6	Whole-of-State Contact Network	Create a definitive pan-Idaho local government network and contact list, as a living document to be used and updated forever.	9, 11, 12, 14, 15, 16	TBD	Future	High	Organize

Project Number	Project Name	Project Description	Related Required Element Number addressed by the project	Estimated Cost	Status (future, ongoing, complete)	Priority (high, medium, low)	Project Type (plan, organize, equip, train, exercise)
7	IT/OT Debt Map	Create a technical debt map and index to size the challenge of upgrading IT and OT infrastructure to a state of currently supported and patchable. Expanding existing ITA program to localities will use SLCGP monies.	10, 13	TBD	Future	Medium	Plan
8	L/T Strategy & Roadmap	Create a whole-of-state 5-year cybersecurity strategic plan and roadmap that describes our aspirational end state and the elements we will put into place to achieve it. The roadmap, starting off where the Governor's Task Force Report left off will be SLCGP funded.	14, 15, 16	TBD	Future	High	Plan
9	Infrastructure Upgrade Plan	With Idaho Technology Authority and ITS develop a plan to state-fund an infrastructure retirement and replacement process, so the equipment of Idaho jurisdictions can be patched and protected.	1, 3, 4, 5 d&e, 7, 10, 13, 14, 15	TBD	Future	Medium	Plan
10	Incident Response Plan	Review the in-place state IR plan and process, the process encouraged by ICRMP for county IT, and a sample of municipal IR plan; then redesign the Idaho state plan, create a customizable local government template, and provide how-to training outreach to all local, rural and frontier jurisdictions on completing their IT plan.	3, 5f, 7, 9, 14, 15	TBD	Ongoing	Medium	Plan
11	Cyber Fusion Center Plan	Develop the strategy, operating model, and policies for an Idaho	2, 3, 4, 5 b&f, 9, 10, 11, 12, 14, 15, 16	TBD	Future	High	Plan

Project Number	Project Name	Project Description	Related Required Element Number addressed by the project	Estimated Cost	Status (future, ongoing, complete)	Priority (high, medium, low)	Project Type (plan, organize, equip, train, exercise)
		Cybersecurity Fusion Center for Boise.					
12	Field Team Implementation Process & Metrics	Develop a field implementation process and procedures for supporting the participation by local, rural, and frontier Idaho government entities in the cybersecurity services to be operated and offered by IOEM.	15, 16	TBD	Future	High	Plan
13	Update SHMP & EOP	Review the cybersecurity chapters of Idaho's State Hazard Mitigation Plan and Emergency Operations Plan and update them to comport to Idaho's SLCGP Cybersecurity Plan, Long Term Strategy and Roadmap, and other new cyber-related plans and program elements.	4, 7, 9, 10, 11, 12, 14	TBD	Future	Low	Plan
14	CISA/MS-ISAC Services Bundle & Consent	Coordinate with CISA and MS-ISAC to develop an Idaho-appropriate bundle of services and support plan for the field implementation team to promote locally, using our SLCGP consent process; explore TTX facilitation services.	2, 3, 4, 5b&e, 6, 7, 9, 10, 11, 12, 14, 15, 16	TBD	Ongoing	High	Plan
15	Specifications, RFPs	Develop the specification, use cases, features and functionality, and any solicitations required for a mix of cybersecurity technology services to be developed for the benefit of all local entities.	2, 3, 4, 5b&f, 9, 10, 11, 12, 13, 14, 15, 16	TBD	Future	High	Equip
16	Procure Technology Services	Purchase cloud, on-premises or hybrid technology services that may include immutable back-up storage, secure networks services, SOC/SIEM capability, data analytics	14, 15	TBD	Future	High	Equip

Project Number	Project Name	Project Description	Related Required Element Number addressed by the project	Estimated Cost	Status (future, ongoing, complete)	Priority (high, medium, low)	Project Type (plan, organize, equip, train, exercise)
		and curated threat analysis dissemination, a SCIF, fusion center space, equipment, communications, and staffing.					
17	Develop Website	Continually upgrade and update the current cybersecurity-related Idaho websites, creating main nexus/portal for our state agencies, divisions, and departments and all local government personnel to access official cyber related information and resources. Improvements to the website will be SLCGP funded.	5 a-g, 6, 8, 9, 11, 12, 13, 15, 16	TBD	Ongoing	Medium	Equip
18	Stand Up Cyber Fusion Center	Physically lease the space in Boise, equip and cable the fusion center, provision it with all cybersecurity services capabilities, engage fusion center staff and fellows, and test its operations.	14, 15, 16	TBD	Future	High	Equip
19	Launch & Dedicate the Fusion Center	Hold the official public announcement, launch and dedication of the fusion center with the Governor and participating state, NGO, defense, education, and federal stakeholders.	14, 15, 16	TBD	Future	High	Organize
20	Local Stakeholder Implementation	Launch and sustain the whole-of-state process of awareness, outreach support, and "last mile" technical implementation to connect Idaho's state, local, rural, frontier, infrastructure, school, and special districts to fusion center services.	4, 5b&f, 7, 9, 11, 12, 14, 15, 16	TBD	Future	High	Train

Appendix C: Entity Metrics

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**[3]
1. Develop a sustained internal capacity across Idaho to prevent cybersecurity events, reduce the impact of successful attacks, respond effectively, and recover with minimal long-term degradation of operational integrity, services delivery, and the confidentiality, integrity, and availability of our most important assets – data and information and control systems.	1.1 Establish cybersecurity as a whole-of-state long-term strategic initiative supported by a statewide cybersecurity strategy and roadmap.	1. 5-year cybersecurity strategic plan and roadmap 2. Governor's declaration	1. Plan and roadmap completed and adopted by IOEM once in 1H24 2. Formal declaration by the Governor published once in 1H24.
	1.2 Communicate cohesively and repetitively about cybersecurity risk awareness, literacy, and management so everyone in the state understands their responsibility for security.	1. Cybersecurity awareness program 2. Local jurisdiction adoption metrics	1. Program publicly launched, once by IOEM and the Idaho PIO in 1H24. 2. Set of demonstration metrics developed and approved, once by IOEM in 2024.
	1.3 Provide the information, tools, and support to local governments – especially rural and frontier jurisdictions – necessary to protect their systems and information from most cybersecurity threats.	1. Statewide local support and implementation program 2. Recruit locally trusted partners.	1. Regional team leads named and hired, once by IOEM in 1H24. 2. Agreements signed with participating partners, once in 1H24 by IOEM. 3. Local support program operating model developed and approved by IOEM, once in 1H24.
	1.4 Increase adoption of basic cybersecurity practices across the state.	1. CISA & MS-ISAC services bundle 2. Awareness and training program	1. Services list jointly published to local entities, annually by IOEM, CISA, MS-ISAC. 2. Awareness and training program formally approved, once by IOEM in 1H24.

[3] The timing of our metrics is expressed in calendar year quarters.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**[3]
		3. Demonstrated local cyber posture improvement	3. Annual maturity assessments by IOEM field team measuring percent improving on CIS controls period over period.
2. Encourage and enhance extraordinary cooperation and collaboration among state agencies and departments, local government jurisdictions, critical infrastructure, educational institutions, and private industry.	2.1 Ensure that all state agencies and local jurisdictions understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and ed assessments.	1. Statewide uniform cyber assessment 2. Tabletop exercises 3. CISA, MS-ISAC testing 4. Required CISA CyHy services and NCSR assessment	1. Percent of localities participating, annually, by IOEM. 2. Percent improving by 1 rating level, annually, by IOEM. 3. Number of TTXs facilitated by IOEM, annually. 4. Number of localities participating in CyHy services and the NCSR. 5. Percent improvement in participation rate, year over year by IOEM.
	2.2 Develop an IT and security workforce and talent pipeline that has the requisite knowledge, skills, and capabilities to meet the demands of our state and local government departments, agencies, and jurisdictions.	1. Workforce annex to 5-year plan 2. Workforce loan program	1. Annex development and acceptance once in 2H24 by IOEM, DHR, Bd. Of Ed, ITC, and Higher Ed consortium. 2. Program formalized and accepted once in 2024 by these organizations.
	2.3 Bring everyone into the room and foster a shared community of cyber information sharing and support through consideration of a best-of-breed Cybersecurity Fusion Center, meeting Recommendation 1.2 of the March 2022 Governor's Cybersecurity Task Force Report and improving outreach and	1. Cyber Fusion Center strategy and policies 2. Fixed cost funding 3. Stand up the Cyber Fusion Center	1. Acceptance once by IOEM, 2H23-1H24. 2. Funding sources identified and approved for purpose, annually by IOEM starting in 1H24.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)[3]**
	information sharing with rural counties, meeting Recommendations 4.1 and 4.4 of the March 2022 Governor's Cybersecurity Task Force Report.		3. Operation center operational and dedicated by the Governor and IOEM Director once in 2H24-1H25.
	2.4 Develop, maintain, and enhance an inventory of Idaho's critical infrastructure and key resources, meeting Recommendation 1.4 of the March 2022 Governor's Cybersecurity Task Force Report.	1. Critical infrastructure inventory 2. IT/OT debt 3. Modernization plan	1. Percent of installations inventoried once by IOEM, INL, ITA in 1H24. 2. Assessment completed once by IOEM, ITS, INL and ITA in 1H23-2H23. 3. Plan accepted by the Governor's Task Force, once in 2024.
3. Support, maintain, and protect Idaho's unique mix of world-leading cybersecurity and engineering capacity and applying its extraordinary knowledge for broader statewide benefit as a key ingredient of our readiness for the cybersecurity challenges facing our state and nation.	3.1 Sustain our deeply collaborative and inclusive public/private partnerships.	1. Cyber deconfliction 2. Locally trusted support	1. Percent of entities adopting deconfliction report, once by all in 1H24. 2. Number of partnerships formalized by all parties once in 1H24.
	3.2 Encourage cross-sector participation and dialog in planning, decisioning, and execution.	1. Visioning session 2. Cyber Fusion Center seats	1. Number of stakeholder organizations attending, once in 2H23-1H24. 2. Percent of Idaho cyber ecosystem seated, once in 2H24 by IOEM.
	3.3 Develop a cyber workforce optimization strategy, considering programs to encourage cyber up-skilling of rural government employees and tribal members, incenting early career security employment and twilight career programs	1. Twilight program 2. Rural staffing	1. Program formalized once by Div. of HR and IOEM in 2H24. 2. Study initiated once in 2H24 by IOEM, ITC, higher ed. consortium.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**[3]
	for older technically skilled workers to work in rural areas, and actively recruiting veterans.		
4. Sustain the strong, decisive direction and tone from the top of state government.	4.1 Develop and establish an organizational and governance model that efficiently connects the cybersecurity program elements necessary for success and establishes clear missions, roles and responsibilities, and decision matrices among relevant state agencies, so we de-conflict any duplication of effort and authority.	1. Signatories to 5-year plan.	1. Percent of cyber-active entities signing onto plan, once in 2024.
	4.2 Encourage local government jurisdictions to fund reasonable budget requests from their IT or security departments or persons, supporting the replacement of out of support hardware, software, and services with more securable infrastructure.	1. Modernization plan 2. Funding	1. Signed once in 2024 by IOEM, INL and ITA. 2. Sufficient funding committed from grants and legislation by IOEM, annually starting 2024.
	4.3 Ensure that we solicit expert policy perspectives, recommendations, and hands-on participation from our rich array of partner organizations throughout Idaho.	1. Policy 2. Membership	1. Formal policy recommendations to IOEM by stakeholder researchers, annually, starting 2024. 2. Number of stakeholders added to Committee by IOEM, once in 2024.

Appendix D – List of Idaho Committee Members

Name	Title	Agency	Representation	Cyber-Capable
Brad Richy	Homeland Security Advisor	Office of Emergency Management	Eligible Entity (SAA)	Yes
John Brown	CISO	Technology Services	Office of the State CISO	Yes
Scott Knights	CISO – Health & Welfare	Health & Welfare	Public Health	Yes
Chris Campbell	CIO	Board of Education	Public Education	Yes
Blake Brandon	Cyber Navigator	Secretary of State	Elections Security	Yes
Jennifer Dvorak	CISO – Judicial	Idaho Supreme Court	Judicial Services	Yes
Josh Haver	Policy Advisor	Public Utilities Commission	Public Utilities	Yes
Greg Adams	IT Director	Teton County	County Representative	Yes
Alexandra Winkler	IT Director	City of Boise	City Representative	Yes
Laurel Caldwell	IT Director	Latah County	Urban Representative	Yes
Robert Peterson	IT Director	Washington County	Rural Representative	Yes
Jarred Edgar	IMD Cybersecurity Task Force	Idaho National Guard	Military Liaison	Yes
Josh Stemp	Cybersecurity State Coordinator	CISA Region 10 (advisory only)	Federal Advisor	Yes

Appendix E – Acronyms

Acronym	Definition
BIA	Business Impact Assessment
CapEx	Capital Expenditure
CCE	Consequence-driven, Cyber-informed Engineering
CI	Critical Infrastructure
CIA	Confidentiality, Integrity & Availability
CIO	Chief Information Officer
CIS	Center for Information Security
CISO	Chief Information Security Officer
COG	Continuity of Government
COOP	Continuity of Operations Planning
CSF	Cyber Security Framework
DHR	Division of Human Resources
DHS	US Department of Homeland Security
DoT	Department of Transportation
DR	Disaster Recovery
EMAC	Emergency Management Assistance Compact
EOL	End of Life
EOP	Emergency Operations Plan
ERM	Enterprise Resource Management
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FTE	Full Time Equivalents
GETS	Government Emergency Telecommunications Service
IAC	Idaho Association of Counties
IACIT	Idaho Association of County IT
ICRMP	Idaho County Risk Management Program
IETA	Idaho Education Technology Association
IIJA	Infrastructure Investment and Jobs Act
INL	Idaho National Lab
IOEM	Idaho Office of Emergency Management
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
ITA	Idaho Technology Authority
ITS	Information Technology Services
KR	Key Resources
MFA	Multi-factor Authentication
MOU	Memoranda of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NACo	National Association of Counties
NASCIO	National Association of CIOs
NCSR	Nationwide Cybersecurity Review

NDA	Non-disclosure Agreement
NGO	Non-Government Organizations
NICE	Workforce Framework for Cybersecurity
NIST	National Institute of Standards and Technology
NOFO	Notices of Funding
OpEx	Operational Expenses
OT	Operational Technology
PIO	Public Information Officer
SAA	State Administrative Agency
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SOC/SIEM	Security Operations Center/Security Information and Event Management
SLCGP	State and Local Cybersecurity Grant Program
SOS	Secretary of State
STEM	Science, Technology, Education & Math
THIRA	Threat and Hazard Identification and Risk Assessment
TTX	Tabletop Exercise
US-CERT	U.S. Computer Emergency Readiness Team
WPS	Wireless Priority Service