SLCGP PROJECT PROPOSAL

Submission Deadline: Tuesday, July 18, 2023

All applications **MUST BE RECEIVED** by the due date.

INSTRUCTIONS

- **GREEN worksheet tabs** are for reference, in particular the Ref-Guidance tab.
- **BLUE worksheet tabs** are the Project Proposal and must be filled out.
- Cream colored cells indicate where input is needed
- Proposals are due via email to **preparedness.grants@mil.wa.gov.**

Please do NOT send a PDF version of the Excel workbook.

TIMELINE

Date	*Activity*	
June 20, 2023	Project Proposal form available/shared with entities	
6/20-7/18	Application period - technical assistance offered as needed	
Jul 18, 2023	**APPLICATIONS DUE TO EMD (can submit before)**	**PREPAREDNESS.GRANTS@MIL.WA.GOV**
July 24-31, 2023	Projects scored and ranked by the Cybersecurity Planning Committee	
August 1-4, 2023	Notice of projects selected for funding	
October-November	Grant agreements executed (once funding is released)	

QUESTIONS - CONTACT

Primary grant points of contact are below - technical cybersecurity assistance will be forwarded to WaTech subject matter experts as required.

Contact	Position	Phone	Email
Jackie Chang	Program Manager	253-512-7083	jacqueline.chang@mil.wa.gov
Sierra Wardell	Financial Operations Section Manager	253-512-7121	sierra.wardell@mil.wa.gov

SLCGP APPLICANT INFORMATION

If your project is selected for funding, a grant agreement will be executed between you and the Washington Military Department. The information below will be used to draft the grant agreement.

Entity	Snohomish County
Entity Address	3000 Rockefeller Avenue M/S 709
	Everett, WA 98201
Project Contact	Tim Wise
Title	County Information Security Officer
Email	tim.wise@snoco.org
Phone	425.388.3314
Alternate Contact	Fred Hartmann
Title	Division Manager, Infrastructure & Security
Email	fred.hartmann@snoco.org
Phone	425.388.3998
UEI #	LG8NG8JNJD83
UBI #	313-014-461
EIN #	91-6001368
Legislative District(s)	1,10,21,32,38,39,44
Congressional District(s)	1,2,7
SWV #	0002794-07
Grant Agreement Signatory	Ken Klein
Title	Executive Director
Second Signatory (if required)	
Title	
Additional Key Contacts	
Name	Joanie Fadden
Title	Accounting and Grant Management Contact
Email	DIS.Admin@snoco.org
Phone	425-388-7046

SLCGP PROJECT PROPOSAL

INSTRUCTIONS: Fill out all cream colored cells as applicable. Not fully addressing the section/question asked may affect scoring of the project. While you should answer questions as clearly as possible, please be careful when including sensitive information.

APPLICANT	Snohomish County	
APPLICANT TYPE	Local-Non Rural	*INSTRUCTIONS: Rural area is defined as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce*

INSTRUCTIONS: Provide the project title; must reflect the nature of work to be completed under the project.

PROJECT TITLE	***Disaster Recovery Infrastructure - Compute***	
AMOUNT REQUESTED	**$ 160,000**	*Will populate based on budget below.*

PROJECT DESCRIPTION

INSTRUCTIONS: Provide a brief narrative describing the project at a high level. Include the activities that will occur as a part of the project. If the project improves an existing solution or existing components of a solution already in use, describe how the new solution will be implemented.

Snohomish County is in the process of transitioning its production virtual server environment from Microsoft Hyper-V to Microsoft Azure Stack Hyperconverged Infrastructure (HCI). This transition has provided an opportunity to re-envision the county's disaster recovery strategy.
Snohomish County leases space in Yakima County's data center to serve as its disaster recovery (DR) site. The County recently installed a redundant 10 Gigabit Internet circuit in Yakima, WA and have completed configuration and testing of Border Gateway Protocol (BGP). The next step in DR preparedness is an investment in the infrastructure necessary to reconstitute and deliver county systems and applications at the DR site.
This proposal is designed to provide one-time funding to establish the infrastructure for application recovery and compute capabilities.

ALIGNMENT WITH SLCGP OBJECTIVES

INSTRUCTIONS: The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk. Applicants are required to address how the following program objectives will be met in their applications. Select alignment from the drop down menu for all applicable Objectives.

No	OBJECTIVE 1: Develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
Yes	OBJECTIVE 2: State, Local, and Tribal agencies understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
Yes	OBJECTIVE 3: Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)
No	OBJECTIVE 4: Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

ALIGNMENT WITH WA STATE CYBERSECURITY PLAN

INSTRUCTIONS: Describe how the project aligns with state Cybersecurity Plan and the connection to one or more of the 16 required elements. Include each element by number (e.g. [Element 2]).

The project aligns with two elements of the state Cybersecurity Plan:
Element 3: Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
Element 7: Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
The infrastructure equipment requested in this proposal will create the infrastructure needed to provide County IT will the ability to deliver disaster recovery services from the Yakima DR site. The outcome of this project is an enhancement to Snohomish County's position in preparation, response and resilience of essential systems and data against cybersecurity risks and threats. This infrastructure is a key component of ensuring continuity of operations for vital government services, establishing geographicly diverse redundant systems that are available in the event of disaster, emergency or cybersecurity incident.

ALIGNMENT WITH OTHER PLAN(S)

INSTRUCTIONS: How does the project align with the strategic and technical elements of any existing local strategic plan or policy(ies). These may internal or references to existing frameworks (e.g., NIST, CIS, CISA).

Snohomish County Information Technology publishes a Strategic Technology Plan every three years. The associated strategic initiatives and business objectives are intentionally aligned with the County's overall goals and objectives. The Disaster Recovery Infrastructure project is aligned with IT Strategic Initiative 3: Security, Privacy and Data Protection and the Business Objective: Mature the county's approach to IT Disaster Recovery documentation, processes and infrastructure for disaster recovery.
https://www.snohomishcountywa.gov/DocumentCenter/View/50007/Snohomish-County-Strategic-Technology-Plan-2021-2024?bidId=
The proposed infrastructure investments also align with elements of both the NIST (Recovery) and CIS (Control 3-Data Protection and Control 11-Data Recovery) frameworks.
[Mastery: Investment incorporates multiple elements of the state Cybersecurity Plan or existing local plan -- such as technology reuse, data minimization, security, principles, publishing open data, mobile solutions, cloud technology solution --over customization.]

ALIGNMENT WITH CYBERSECURITY PROGRAM

INSTRUCTIONS: How does this project align with the buildout of your cybersecurity program? Describe how end users (internal and external) will be involved in the project to include governance and implementation activities.

The County Information Security Officer (CISO) and Security team have developed a prioritized list of cybersecurity initiatives that align with the IT Strategic Technology Plan. Additional inputs into these initiatives includes findings from a 2020 CMAT audit and penetration tests, feedback from cyber insurers and security sources (CISA/MS-ISAC/NCSR), and learnings from security collaboratives (Seattle UASI/ACCIS/WA State).
Improving the county's data backup architecture and resilience has been a major point of emphasis over the last year. Addressing deficiences in the county's disaster recovery and COOP strategies and capabilities are a signficant focus for the organization. Led by the Department of Emergency Management, County COOP activities are in progress, while IT continues to build out the Yakima disaster recovery site. COOP outputs will serve to inform planned updates to the disaster recovery plan.
[Competent: Mostly aligned with Mastery]

GAP BEING ADDRESSED

INSTRUCTIONS: What is the gap the project addresses? Explain the capability assessment which identified the gap and how the project activities will mitigate it.

Execution of this project will accomplish four objectives for Snohomish County:
1. The infrastructure equipment will provide County IT will the ability to deliver disaster recovery services from the Yakima DR site.
2. The Yakima DR site would also be equipped to serve as the county's Isolated Recovery Site (IRE) in the event of a ransomware attack.
3. Requested infrastructure equipment will provide the ability to reconstitute systems and deliver workloads from the Yakima DR site.
[Competent: Mostly aligned with Mastery]

URGENCY

INSTRUCTIONS: Describe the urgency of implementing the project and the impacts if it does not proceed as planned.

Snohomish County currently lacks the disaster recovery infrastructure to effectively recover business operations in the event of major event impacting the primary data center. Establishing a presence outside of the immediate geological area and provisioning sufficient connectivity have been the priorities to date. Investments in the requested infrastructure will address imminent failures in certain recovery scenarios.
[Level 3: Investment addresses imminent failure of a system or infrastructure.]

SUSTAIN/BUILD? Build

*INSTRUCTIONS: Select "**build**" if this project focuses on starting a new capability or the intent of the project is to close a capability gap. Select "**sustain**" if the purpose of the project strictly maintains an existing capability at its existing current level.*

IMPACT

INSTRUCTIONS: Describe the impact of the project. How will the proposed project continue to add value and/or improvement in the future? As applicable, describe any future improvements and investments that are planned to continue the work in this proposal and what ongoing funding support is needed after the grant funding is applied.

The project will provide Snohomish County with the infrastructure needed to recover in the event of a disaster. Next phases will include configuring the ability to deliver recovered workloads to employees from Yakima, developing runbooks for reconstituting complex business applications and updating the disaster recovery plan to reflect capabilities available in Yakima. Also, IT intends to leverage the Yakima DR site as its Isolated Recovery Site (IRE) in the event of a ransomware attack. Further analysis will be necessary to identify requirements and determine what future investments, configuration and planning are needed for this use case.
Since funds are being requested for capital expenditure only, Snohomish County recognizes and is prepared to cover ongoing maintenance and support costs for the equipment.
[Mastery: Proposed solution supports interoperability and/or interfaces of existing systems. For new capability, the investment allows for reuse of principles in the future. Plan for future ongoing funding in place if needed.]

OUTCOME

INSTRUCTIONS: What is the outcome when the project is complete? Describe and quantify (as applicable) the specific impact(s) to stakeholders, reduction in cybersecurity risk, and increases in resilience through strengthened cybersecurity practices. Include incremental performance metrics if any.

The requested infrastructure equipment will provide County with the ability to recover and deliver disaster recovery services from the Yakima DR site. The Yakima DR site can also serve as a the county's Isolated Recovery Site (IRE) in the event of a ransomware attack. Validation measures to include the ability to isolate the Yakima site from the county network and reconstitute applications in the Yakima DR site, and then move those workloads back to the primary data center.
The County's primary data recovery source is our daily immutable backups, the secondary being the replica backups being streamed to Yakima daily, and the third being offline backups. Validation measures to include the ability to recover applications in the Yakima DR site, the ability for users to access and utilize applications running from the Yakima DR site from on-premises, the ability for users to access and utilize applications running from the Yakima DR site remotely, the ability to reconstitute applications in the Yakima DR site and move select workloads to Azure, and the ability to bring workloads back on-premise from Azure.
[Competent: Mostly aligned with Mastery.]

PRELIMINARY WORK/PROJECT SCOPING

INSTRUCTIONS: What preliminary work has been completed prior to this proposal, such as research, stakeholder outreach, feasibility study, etc.? Articulate how benefits (to include who) were determined and any stakeholder engagement. Some CISA services will be required before reimbursement of costs (see REF-Guidance tab Requirements) - if your entity has already signed up, note that here.

This project has been ongoing for over a year, as foundational components of the Yakima DR site were identified, provisioned, configured and tested. The team leveraged vendors including Microsoft, DataOn, Veeam, Palo Alto, and Gartner to evaluate design concepts and best practices. Recent disaster recovery design work has dovetailed with Azure Stack HCI research, testing, and implementation activities. Additionally, proof-of-concept testing of the disaster recovery approach have been performed to validate the architecture behaves as expected and yields the intended outcomes. Upon receipt of grant funding, the county is ready to initiate the competitive procurement process.
Snohomish County Continunity of Operations Planning (COOP) planning is also in progress and customer feedback from this effort will help to inform IT's recovery priorities in the event of a disaster.
The County completes the NCSR annually, is a member of MS-ISAC, already leverages CISA's Vulnerability Scanning and has signed up for CIS services.
[Competent: Mostly aligned with Mastery.]

PROJECT MANAGEMENT

INSTRUCTIONS: Describe the project management and governance structures and processes that will be in place to support the project. Examples include project management resources, methodologies, executive sponsor, steering committee, vendor/contract management, and change control.

The project team meets weekly to discuss design, identify tasks and dependencies, and prioritization. An IT project manager has been assigned to the effort and the IT Engineering Supervisor and IT Division Manager, Engineering and Security assist with clearing roadblocks including resource assignments. The team leverages the agile methodology for project delivery.
Project status is input weekly into IT's project management tool, Asana, so interested parties have continued visibility. Per normal IT practices, all changes go before the Change Control Board for discussion and review. A cross-section of representatives from throughout the County attend the weekly CCB meeting, which gives them insight into IT's activities and affords them an opportunity to voice an concerns or raise questions before changes are implemented.
IT follows a standard process for procurement and contract negotiations. Requests are submitted via the County's ITSM solution and they are routed to the IT Business Operations team for processing. The Business Ops team works collaboratively with Purchasing and/or the Prosecuting Attorney's Office to ensure all activities meet county guidelines and follow established procedures.
[Mastery: For this request, entity describes governance processes that include appropriately placed executive sponsor, representative steering committee, vendor/contract management approach, proposed budget, and assigned resources.]

PROJECT IMPLEMENTATION

INSTRUCTIONS: Describe the implementation of the project to include resourcing. What have you done to prepare? Will in-house resources be used, or will resources be procured elsewhere? How has organizational change management been factored into the planning and approach?

The project team has already identified the infrastructure needed, including make and model, to achieve the intended outcome. Once funding is available, the IT project manager engage County Purchasing to initiate the competitive procurement process with acquisition via either the county's bid process or by leveraging an approved state contract. Due to internal procurement processes and ongoing industry supply chain issues, we've built up to 90 days into the timeline for delivery .
The Yakima disaster recovery has already been configured with 10Gig Internet Connection and BGP and a 10Gig point-to-point circuit is in place between Yakima and the county's primary data center. Upon delivery of the equipment, the IT Engineering team will begin infrastructure build and configuration. Once completed, the equipment will be transported to Yakima and installed by County IT personnel.
Following final in-place configuration in Yakima, IT will begin the process of configuring communication between production systems located in Everett and the newly installed equipment. The project timeline includes up to 30 days for testing of configured data transport between sites, the recovery of a subset of systems/applications in Yakima as validation.
[Mastery: Entity readiness is well defined and demonstrates planning of resources including project team, SMEs, other technical resources.]

PROJECT SCHEDULE

INSTRUCTIONS: Enter the major milestones for the project.

START DATE	END DATE	MILESTONE
11/1/2024		PROJECT START
11/1/2024	1/31/2025	COMPETITIVE PROCUREMENT & SOURCING
2/1/2025	3/30/2025	CONFIGURATION & BUILD
4/1/2025	5/31/2025	INSTALLATION/IMPLEMENTATION
6/1/2025	6/30/2025	TESTING & VALIDATION
	6/30/2025	PROJECT COMPLETION

PROJECT BUDGET

INSTRUCTIONS: Enter projected amounts for each budget category under the applicable solution area (POETE element). Enter indirect charges as applicable.

	SOLUTION AREA					
	PLANNING	ORGANIZATION	EQUIPMENT	TRAINING	EXERCISE	**TOTAL**
Salaries & Benefits	$0.00	$0.00		$0.00	$0.00	**$0.00**
Supplies	$0.00	$0.00		$0.00	$0.00	**$0.00**
Travel/Per Diem	$0.00	$0.00		$0.00	$0.00	**$0.00**
Contractor/Consultant	$0.00	$0.00		$0.00	$0.00	**$0.00**
Passthrough	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Other	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Equipment			$160,000.00			**$160,000.00**
SUBTOTAL	$0.00	$0.00	$160,000.00	$0.00	$0.00	$160,000.00
Indirect						**$0.00**
TOTAL	**$0.00**	**$0.00**	**$160,000.00**	**$0.00**	**$0.00**	**$160,000.00**

M&A	*Requirement: Up to 5% of the Project total may be used for management and administration of the project.*					
Salaries & Benefits	Supplies	Travel/Per Diem	Consultant	Other	Indirect	Total
$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Indirect included?	***Type of back-up***	N/A				

BUDGET NARRATIVE/ITEMIZED COSTS

INSTRUCTIONS: Provide detail of the projected expenses. The estimated costs should align with the application budget categories (salaries and benefits, supplies, travel/per diem, contractor/consultant, passthrough, other, and equipment) in the Budget above.

DataOn 3-Node S2D-6112-HCI Cluster for Azure Stack - $160,000

Equipment must be refreshed over time and requires maintenance to ensure availability. Snohomish County IT has an established technology replacement (TRP) program that evaluates deployed equipment and assigns annual funding to the future replacement of assets over time. The equipment listed above will be added to the TRP planning at the County to ensure local funding is secured so it is maintained and replaced as needed to ensure future operational availability for this essential disaster recovery equipment.

SLCGP PROJECT GUIDANCE

FEDERAL REFERENCES

Link to FY 2022 State and Local Cybersecurity Grant Program Notice of Funding Opportunity (NOFO)
Link to Home Page | CISA

TOPICS BELOW

SLCGP Purpose

The potential consequences of cyber incidents threaten national security. Strengthening cybersecurity practices and resilience of state, local, and territorial (SLT) governments is an important homeland security mission and the primary focus of the State and Local Cybersecurity Grant Program (SLCGP). Through funding from Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), the SLCGP enables DHS to make targeted cybersecurity investments in SLT government agencies, thus improving the security of critical infrastructure and improving the resilience of the services SLT governments provide their community.

Eligibility

State agencies, local governments, and tribes may apply for funding. At least eighty percent of the funding will be passed through to local/tribal entities. Twenty five percent of the total award will be awarded to rural entities. The following definitions will be used for

"**Local government**" is defined in 6 U.S.C. § 101(13) as
A) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments, regional or interstate government entity, or agency or instrumentality of a local government;
B) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation;
C) A rural community, unincorporated town or village, or other public entity. Per the Homeland Security Act of 2002, a **rural area** is defined in 49 U.S.C. §5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce.

Federal Funding Available

It is anticipated each year over the next four years funding will be available to WA state under SLCGP. Only FY22 is known but the following chart shows projected funding levels for the remaining 3 years.

		WA State Allocation	State 20%	Local 80%
	FY22	$3,667,735	$733,547	$2,934,188
PROJECTION	*FY23*	*$7,077,000*	*$1,415,400*	*$5,661,600*
	FY24	*$5,308,000*	*$1,061,600*	*$4,246,400*
	FY25	*$1,769,000*	*$353,800*	*$1,415,200*
		$17,692,000	$3,564,347	$14,257,388

Match Requirement

Each year of SLCGP will have a cost share requirement. In State Fiscal Year 2022 and 2023, the State legislature granted funding for the required cost share. The Washington Military Department has requested additional funding to meet the requirement for the grant over the next biennium.

All matching costs must be verifiable, reasonable, allocable and necessary, and otherwise allowable under the grant program, and in compliance with all applicable federal requirements and regulations. Unless otherwise authorized by law, the non-federal cost share requirement cannot be matched with other federal funds.

Requirements

All SLCGP recipients and subrecipients will be required to participate in a limited number of free services by CISA before reimbursement of costs can occur.

Cyber Hygiene Services

• **Web Application Scanning** is an "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.
• **Vulnerability Scanning** evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.

To register for these services, email vulnerability_info@cisa.dhs.gov with the subject line "Requesting Cyber Hygiene Services – SLCGP" to get started. Indicate in the body of your email that you are requesting this service as part of the SLCGP.

For more information, visit CISA's Cyber Hygiene Information Page.

Cyber Infrastructure Survey (CIS)

The CIS is a free service provided by CISA that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of an organization's cybersecurity ecosystem. This can be done through a self-assessment or with CISA's assistance. The CIS will provide a baseline that will later be used to show improvement in the information security maturity of the organization based on the proposed project.

For more information, visit CISA's Cyber Resource Hub information page.

Multi-State Information Sharing and Analysis Center (MS-ISAC) membership

Membership is free. The MS-ISAC receives support from and has been designated by DHS as the cybersecurity ISAC for SLT governments. The MS-ISAC provides services and information sharing that significantly enhances SLT governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises.

To register, please visit https://learn.cisecurity.org/ms-isac-registration.
For more information, visit MS-ISAC (cisecurity.org)

Nationwide Cybersecurity Review (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the MS-ISAC. Entities and their subrecipients should complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance **(due date 12/1/2023)** and annually thereafter. The NCSR is open October-February each year.

For more information, visit Nationwide Cybersecurity Review (NCSR) (cisecurity.org).

Allowable Costs

Expenditures made in support of the funding priorities generally fall into one of the following allowable categories:
• Planning
• Organization
• Equipment
• Training
• Exercises
• Management & Administration (M&A).

• **Planning** - SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision

• **Planning** - SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of the holistic, entity-wide cybersecurity plan and other planning activities that support the program goals and objectives and Cybersecurity Planning Committee requirements.
• **Organization** - Organizational activities include: program management, development of whole community partnerships that support the Cybersecurity Planning Committee, structures and mechanisms for information sharing between the public and private sector, and operational support.
• **Equipment** - SLCGP equipment is intended to be used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments. All equipment must meet all applicable statutory, regulatory, and DHS standards to be eligible for purchase. In addition, subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment. Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations. The use of SLCGP grant funds for maintenance contracts, warranties, repair or replacement costs, upgrades, and user fees are allowable, unless otherwise noted.
• **Training** - Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align to the eligible entity's Cybersecurity Plan and address a performance gap identified through assessments and contribute to building a capability that will be evaluated through a formal exercise.
• **Exercises** - Exercises conducted with grant funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP).
• **M&A** - M&A activities are those directly relating to the management and administration of SLCGP funds, such as financial management and monitoring. Subrecipients may retain a maximum of up to five percent of the awarded funding solely for M&A purposes associated with the SLCGP award.

Ineligible Costs

Grant and match funds **cannot** be used for:
• To supplant state or local funds; however, this shall not be construed to prohibit the use of funds from a grant under this NOFO for otherwise permissible uses on the basis that the SLT has previously used SLT funds to support the same or similar uses;
• To meet a cost-sharing contribution;
• To pay a ransom;
• For recreational or social purposes;
• To pay for cybersecurity insurance premiums;
• To acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities; or
• For any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity that receives the grant or a local government within the jurisdiction of the eligible entity.

Subrecipients are subject to the prohibitions described in section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA), Pub. L. No. 115-232 (2018) and 2 C.F.R. §§ 200.216, 200.327, 200.471, and Appendix II to 2 C.F.R. Part 200, and may not use grant funds to:
(1) Procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system;
(2) Enter into, extend, or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology of any system; or
(3) Enter into, extend, or renew contracts with entities that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

IF THE PROJECT IS SELECTED FOR FUNDING

Period of Performance

If the project is selected for funding, each grant agreement will have an end date based on the amount of time needed to complete the project balanced within the FY22 award (end date 11/30/2026). Projects will be not be given the max amount of time unless justified.

Reimbursement of Costs

If the project is selected for funding, each grant agreement will have a schedule for reimbursement submissions based on the award amount and activities planned for the funding cycle. Project expenditures will be reimbursed by submission of a Reimbursement Spreadsheet and an A-19 Invoice Voucher. (A Reimbursement Workbook will be emailed to the subrecipient upon execution of the agreement.) ***Processing can be expedited if funding is limited by notifying your assigned POC.***

Reporting

If the project is selected for funding, each grant agreement will have a schedule for reporting to ensure the project is on-target. Additionally, individual metrics will be assigned for reporting. A report template will be emailed to the subrecipient upon execution of the agreement. Reports will be shared with the Planning Committee and compiled into the FEMA required annual report.

WA STATE CYBERSECURITY PLAN

[Link to Washington Cybersecurity Plan]

Purpose

This strategy aims to establish a clear vision for the State of Washington's cybersecurity with goals and objectives that address current gaps in cybersecurity. Goals provide high-level themes, objectives provide measurable and attainable milestones needed to achieve maturity toward the goal, and key tasks deliver specific proposed action items that fall underneath each broader goal and objective. While this strategy is a two-year plan, it is a living document that will be reevaluated based on the ever-evolving threat landscape, emerging technologies, and current needs.

Scope

This strategy establishes a framework for a whole-of-state approach to cybersecurity. It is structured to provide clear direction over the next two years for mitigating risks and addressing cyber threats across the state. Partnerships with federal, state, local and private sectors will be utilized and leveraged to accomplish the goals and objectives of the strategy. This plan does not attempt to answer all possible questions concerning cyber response in the state, but merely provides a format and structure for a state response for the SLCGP. This plan should work in collaboration, in support of, or in coordination of existing, adopted security plans.

Goal 1 – Improve the cybersecurity posture of all local governments.

Objectives

- Enhance risk assessment and risk management capabilities within local jurisdictions by improving Nationwide Cybersecurity Review (NCSR) responses to level 5 per the NIST CSF. (SLCGP NOFO elements 12, 141).
- Enhance business continuity (BC) and information technology disaster recovery (IT DR) capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process) per the NIST CSF. (SLCGP NOFO elements 1, 5, 9)
- Enhance incident response and recovery capabilities within local jurisdictions by improving NCSR responses to level 5 (Implementation in Process) per the NIST CSF. (SLCGP NOFO elements 2, 3)
- Identify best practices for sharing threat intelligence, indicators of compromise and indicators of attack between victims and partner organizations. (SLCGP NOFO element 11)
- Promote industry standards for information security. (SLCGP NOFO element 6)

Suggested Potential Projects

- Jurisdictions or entities may implement Multi-Factor Authentication (MFA). (SLCGP NOFO element 5)
- Facilitate implementation of the .gov domain for all government jurisdictions. (SLCGP NOFO elements 5 and 6)
- Analyze and address state and local government entity risk management gaps. (SLCGP NOFO elements 12, 14)
- Analyze and address state and local government entity incident response plan gaps. (SLCGP NOFO elements 2, 3)
- Analyze and address state and local government entity gaps in threat information sharing. (SLCGP OFO element 11)

Goal 2 – Increase cybersecurity and privacy capacity at the state and local level.

Objectives

- Implement redundant and resilient data storage and transmission systems. (SLCGP NOFO element 7)
- Develop a competent professional IT workforce using standardized curriculum. (SLCGP NOFO element 8)
- Promote a cyber aware culture within state and local jurisdictions through accessible awareness content. (SLCGP NOFO element 8)

Suggested Potential Projects

- Provide financially accessible awareness programs on cybersecurity, privacy and protection of sensitive information and infrastructure systems for SLT employees. (SLCGP NOFO element 8)
- Increase the number of individuals with professional training and certification in cybersecurity, privacy and infrastructure protection within local jurisdictions and entities. (SLCGP NOFO element 8)
- Support participants in higher education programs (bachelor and masters programs) across the state. (SLCGP NOFO element 8)
- Identify opportunities for IT professionals to demonstrate skills and gain experience in real-world and simulated incident response and recovery operations (tabletop and cyber range exercises). (SLCGP NOFO element 3)
- Identify gaps in secure storage and transmission capabilities within state and local entities (SLCGP NOFO element 7)

Goal 3 – Develop enduring partnerships to support cyber resilience across the State of Washington.

Objectives

- Identify coalitions of local jurisdictions to support implementation of identified SLCGP projects. (SLCGP NOFO element 13)

• Work with SLT stakeholders to ensure compatibility of state and local cyber incident response plans. (SLCGP NOFO element 3, 14)
• Invest in the future cybersecurity workforce by conducting outreach on cybersecurity career pathways for K-12, and college and university students. (SLCGP NOFO elements 8, 13)

Suggested Potential Projects

• Partner with the Association of County and City Information Services (ACCIS) professionals, the Washington Coalition for Infrastructure Protection and Homeland Resilience (WA-CIPHR), and other organizations throughout the state to identify opportunities to improve cybersecurity statewide. (SLCGP NOFO element 14)
• Assist with the development and review of local jurisdictional cybersecurity programs and plans. (SLCGP NOFO element 14)
• Partner with national organizations and federal partners (including the FBI, Cybersecurity and Infrastructure Security Agency [CISA], Secret Service, Multi-State Information Sharing and Analysis Center [MS-ISAC], and the National Initiative for Cybersecurity Education [NICE]) to harness best-practices and information sharing.
• Work with state higher education institutions, and non-governmental organizations to improve workforce development and resources. (SLCGP NOFO element 8)

Goal 4 – Effectively use existing funds and identify sustainable funding options.

Objectives

• Demonstrate progress towards cyber risk reduction at the end of each funding cycle. (SLCGP NOFO element 10)
• Amplify the reach of projects by prioritizing those that can be extrapolated and shared with other jurisdictions. (SLCGP NOFO element 10)
• Leverage state master contracts to support accessible pricing for cyber resilience products, platforms, and solutions to all jurisdictions throughout Washington State. (SLCGP NOFO element 4)
• Apply values of equity when prioritizing proposed projects from local jurisdictions or entities. (Appendix E: Alignment with Equity and Inclusion Directives).

Suggested Potential Projects

• Develop outreach products for elected officials and executive personnel to clearly communicate funding needs for cyber related projects. (SLCGP NOFO element 10)
• Equitably distribute funds to areas of highest need and prioritize underserved jurisdictions. (SLCGP NOFO element 10, 15)

All projects selected for funding must tie to the state's Cybersecurity Plan, address an identified gap or need, and support one of the required plan elements. Completion of the projects will demonstrate the implementation of the Plan over time.

REQUIRED PLAN ELEMENTS

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology. Reimbursement Spreadsheet and an A-19 Invoice Voucher. (A Reimbursement Workbook will be emailed to the subrecipient upon execution of the agreement.)

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

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

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

5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below. The following cybersecurity best practices under required element 5 must be included in each eligible entity's Cybersecurity Plan:
•Implement multi-factor authentication;
•Implement enhanced logging;
•Data encryption for data at rest and in transit;
•End use of unsupported/end of life software and hardware that are accessible from the Internet;
•Prohibit use of known/fixed/default passwords and credentials;

•Ensure the ability to reconstitute systems (backups); and
•Migration to the .gov internet domain

Additional best practices that the Cybersecurity Plan can address include:
•The National Institute of Standards and Technology (NIST) Cybersecurity Framework;
•NIST's cyber chain supply chain risk management best practices; and
•Knowledge bases of adversary tools and tactics.

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

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

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

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

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

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

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

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

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

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

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

PROJECT SELECTION CRITERIA

Each year, WaTech is required by RCW 43.88.092 to evaluate proposed information technology budget requests and establish priority rankings of the proposals. Questions posed are based on industry best practice, statewide technology policy and strategy, and lessons learned from prior state projects. The scoring criteria for SLCGP funding is based on this process used by WaTech to rank the diverse IT projects for funding.

Process : Volunteers from the Planning Committee or their proxies will score and rank the projects, preparing a ranked list. From that list, the Planning Committee will decide which projects to recommend to the State Chief Information Officer who will have the final decision of which projects are funded.

CRITERIA: **JURISDICTION READINESS**

Subcriteria: ***Due Diligence***

Assess the evidence of needs assessment, high-level requirements, or similar due diligence, to understand needs and research and selected technology solution. Articulate who benefits from project. Explain stakeholder engagement.

Scoring Scale

- Mastery: Investment demonstrates complete due diligence with a thorough needs assessment that includes high level requirements, or market research analysis to support the investment.
- Competent: Mostly aligned with Mastery.
- Adequate: Partially aligned with Mastery.
- Insufficient: There is limited or non-existent documentation on needs assessment, high level requirements, or market research to support the investment.

Subcriteria: ***Project Management and Governance***

For this investment, assess the planned proposal's governance, project management approach, and resourcing including sponsorship, and management.

Scoring Scale

- Mastery: For this request, entity describes governance processes that include appropriately placed executive sponsor, representative steering committee, vendor/contract management approach, proposed budget, and assigned resources.
- Competent: Mostly aligned with Mastery.
- Adequate: Partially aligned with Mastery.
- Insufficient: Proposal has no or insufficient evidence of executive sponsor, representative steering committee, and vendor/contract management approach. Entity does not have identified budget and resource processes.

Subcriteria ***: Readiness***

Assess the planned investment approach and implementation staffing/resourcing, including assumptions about staffing, governance, and budgeting.

Scoring Scale

- Mastery: Entity readiness is well defined and demonstrates planning of resources including project team, SMEs, other technical resources.
- Competent: Mostly aligned with Mastery.
- Adequate: Partially aligned with Mastery.
- Insufficient: Investment narrowly targets organizational needs and the proposed solution does not demonstrate planning and organizational readiness in all areas that would be impacted by the investment.

CRITERIA: **CYBER PLAN ALIGNMENT**

Subcriteria ***: Strategic and Technical Alignment***

Scoring Scale

Assess proposal against the state Cybersecurity Plan, or existing local strategic plan (or risk assessment) including alignment with the goals, objectives, and initiatives/tasks.	•Mastery: Investment incorporates multiple elements of the state Cybersecurity Plan or existing local plan -- such as technology reuse, data minimization, security, principles, publishing open data, mobile solutions, cloud technology solution --over customization. •Competent: Mostly aligned with Mastery. •Adequate: Partially aligned with Mastery. •Insufficient: Investment is inconsistent with elements of the state strategic vision and does not incorporate the state's strategic goals, objectives and initiatives.
Subcriteria ***: Sustainability*** Assess degree to which solution will continue to add value in the future or need future improvements. Are current systems or components that are already in place utilized or improved? Is ongoing funding support for project considered and planned past grant funding.	***Scoring Scale*** •Mastery: Proposed solution supports interoperability and/or interfaces of existing systems. For new capability, the investment allows for reuse of principles in the future. Plan for future ongoing funding in place if needed. •Competent: Mostly aligned with Mastery. •Adequate: Partially aligned with Mastery. •Insufficient: Investment does not demonstrate exploration or reuse of existing solutions, contract or components used in the state. The solution is a new proposal and does not allow for reuse by other agencies in the future. There is no future funding identified when funding is required to be successful in the future.
CRITERIA: **CYBER PROGRAM ALIGNMENT**	
Subcriteria ***: Cybersecurity Program Alignment*** Assess if there is a clear cybersecurity need. Does the project address the expressed need or gap? Will the project offer outcomes desired and expressed in existing processes, or proposal? Describe how end users (internal and external) will be involved in governance and implementation activities.	***Scoring Scale*** •Mastery: Investment implementation is being driven by cybersecurity processes and integrated with this technology. Solution supports and/or improves existing cybersecurity processes. End users (internal and external) will be involved in governance and implementation activities. •Competent: Mostly aligned with Mastery. •Adequate: Partially aligned with Mastery. •Insufficient: Investment implementation is nominally considering the cybersecurity processes impacted by this investment. No evidence showing end user involvement in governance or implementation activities.
Subcriteria ***: Measurable Outcomes*** Assess the presence of anticipated cybersecurity outcomes, measures and targets as a result of this investment.	***Scoring Scale*** •Mastery: Investment is focused on providing customer value and security. For public services, the user experience is primary. For entity investments, provides tangible and measurable benefits and outcomes to entity users. Investment plan includes input from customer stakeholders and addresses methods to incorporate user experience/feedback. •Competent: Mostly aligned with Mastery. •Adequate: Partially aligned with Mastery. •Insufficient: Investment is being implemented in isolation from customers and end users. There is no demonstrated plan for incorporating citizen or customer feedback. There are no tangible and measurable performance benefits and outcomes identified.
CRITERIA: **URGENCY**	
Taken into consideration when ranking request	**Scoring Scale**

During the evaluation and ranking process, the Planning Committee will consider the urgency of the project request. Entities need to describe urgency of implementing the IT cybersecurity investment in this cycle and impacts if effort doesn't proceed as planned.	• Level 4: Investment addresses a currently unmet, time-sensitive legal mandate or addresses audit findings requiring urgent action. Identify the mandate or audit finding. Level 3: Investment addresses imminent failure of a system or infrastructure. Level 2: Investment addresses an agency's technical debt of aging systems and provides an opportunity for modernization. Level 1: Investment provides an opportunity to improve services or enhanced functionality however does not address imminent risk.

SLCGP PROJECT GUIDANCE

PROJECT IDEAS

NOTE: the grant is intended to provide "one-time" funding to address current technical gaps. Proposals must consider and address ongoing support costs.

Planning

- Development of an overall cybersecurity program and/or strategic plan
- Planning for response to cyber security events and threats
- Development of incident response plans
- Development of risk management plans
- Continuity of operations (COOP) planning

Assessments, testing, evaluations

- Maturity assessments of existing information security programs
- Tabletop exercises used to improve incident response plans
- Cyber-range exercises to test efficacy of team capabilities and controls

Security Protections - inclusion of the acquisition of licenses, cloud platforms or hardware

- Implementation of technical controls such as multi-factor authentication (MFA)
- Endpoint security controls
- Intrusion detection/prevention
- Migrating to the .gov domain

Training

- Professional training for information security practitioners such as CISSP, HISP, CISM, etc.
- Support for cyber professionals completing advanced degrees (bachelors or masters) in cybersecurity
- Awareness programs and/or platforms for organization employees
- Targeted awareness campaigns for high risk individuals (i.e., executives, political leaders, etc.)
- Phishing simulation platforms

Other

- Multi-jurisdictional projects related to information sharing and/or cybersecurity collaboration activities
- Projects that incorporate multiple types such as an assessment of cybersecurity gaps accompanied with the proposal to acquire security protective controls to address the gap