Application Proposal Worksheet for the 2024 State & Local Cyber Grant Program (SLCGP)

Due 15 May 2026

Write project proposals supporting the following federal objectives:

- *Understand your organization's current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.*
- *Implement security protections commensurate with risk.*
- *Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.*

Please reference the Program Goals/Objectives in the Cybersecurity State Plan (see pages 12 & 13) that support these federal objectives for which you are seeking grant funds. ***Note: The project should be completed within one year.***

Instructions: *Please fill in all the blocks of this proposal worksheet with the requested information and submit this Microsoft Word document to Bob Connell (rconnell@sled.sc.gov) (SAA) not later than 15 May 2026. Please name your submitted proposal worksheet file as follows (Your Jurisdiction, Organization, Objective Addressed): JurisdictionAgencyObjective. For example, if my jurisdiction was Charleston County and my agency was the Sheriff's Office and I was focused on Objectives 3.1 and 4.2 of the State Cybersecurity Plan on pages 12 & 13, the file name would be: CharlestonCoSO3.1,4.2.*

If your proposal is accepted, additional information will be required at a later time.

Project Proposal Identification—All Fields Must Be Completed Accurately!

Project Start Date:	Enter date	**Sub-recipient Org. Name:** **Address:**	
Project End Date:	Enter date	**Zip Code+4:** **Type:**	State, Local, or *Rural

*Less than 50,000 people in jurisdiction

Project Director:		**E-Mail:**	
		Phone:	
Funding Request ($):		**UEI Number:**	

Project Name (100 Character Max):	
Sustain or Build a capability?	

Deployable: **Yes or No (mobile, used in any state)**

Shareable: **Yes or No (not physically deployable, but shareable at local, state, or federal levels)**

Primary Cyber Goal(s) (1, 2, 3 and/or 4) You Will Focus on for This Cyber Security Project:	
Applicable Project Management Step for This Project (Initiate, Plan, Execute, Control, Close Out -- See Appendix 2):	

I.B. Provide a narrative describing the project (3000 character maximum). Provide each of the cyber security objectives this project supports and how.

Additional Instructions (**remove these instructions with your inputs**).
The first line must identify the **Cybersecurity Planning Objective(s)** --by number--that will be addressed/resolved by this project. Provide a detailed description of how you will address and accomplish each objective identified, by number and in order.

II.A. Funding Plan by POETE elements

Provide the total estimated cost for the period of performance for this project by completing the following table:

- ***Provide funding requests by POETE (Planning, Organization, Equipment, Training, Exercise) areas***
- ***For each POETE element that has associated funds requested, provide a brief summary description of the planned expenditures***

POETE	Homeland Security Grant Program Funding Request
Planning	
Organization	
Equipment	
Training	
Exercises	
Total	

Planning

Organization

Equipment

Training

Exercise

II.B. Programmatic Milestones

Provide specific descriptive milestones for the project over the period of performance (1-yr, July 26 – June 27), including start and end dates for each milestone; up to 10 milestones may be provided.

Milestone 1: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 2: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 3: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 4: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 5: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 6: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 7: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 8: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone 9: Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

Milestone10:Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

III.A. Project Impact / Used for Project Evaluation

What outcomes will indicate that this project is successful at the end of the period of performance? Discuss anticipated outcomes of success by Cybersecurity Planning Objectives:

Provide any other information to clarify how this project will significantly impact cyber security in South Carolina:

APPENDIX 1.

Cybersecurity Plan

INTRODUCTION

The South Carolina Comprehensive Cybersecurity Plan (CCP) plays a pivotal role in guiding the state's efforts to establish and enhance cyber resilience. It encapsulates all five essential aspects of the National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1: identification, protection, detection, response, and recovery. South Carolina has integrated existing plans, structures, and other relevant initiatives to form our inclusive cybersecurity strategy. Leveraging pre-existing structures and capabilities empowers South Carolina to establish governance and a framework to efficiently address significant cybersecurity demands while optimally utilizing available resources. By incorporating feedback from local jurisdictions, the State of South Carolina fulfills requirement e.2.A.ii of the State and Local Cybersecurity Grant Program (SLCGP).

The CCP is a three-year strategic planning document that contains the following components:

- Vision and Mission: Articulates the vision and mission for improving cybersecurity resilience interoperability over the next three years.
- Cybersecurity Plan Elements: Maps the technology and operations to the Cybersecurity Capabilities Assessment, an analysis of South Carolina's cybersecurity maturity against the 16 required cybersecurity elements. The Plan was built using the results of the Assessment and goals prioritized with the goal of rapidly maturing South Carolina's cybersecurity capabilities.
- Funding: Describes the strategy for allocating funds received from the SLCGP and matching funds provided by the state of South Carolina from existing projects along with in-kind hours donated by the organizations supporting the effort.
- Assessment of Capabilities and Needs: Describes how inputs from local governments were used to reduce overall cybersecurity risk across the eligible entity and ensure that the developed plan takes a holistic view.
- Implementation Plan: Describes the State of South Carolina's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan will include the resources and timeline where practicable.
- Organization, Roles, and Responsibilities: Describes the leaders and organizations responsible for executing the tasks and activities to achieve the goals and support the mission and vision. The leaders and organizations collaborate with local entities; however, the Plan is a guiding document and does not create any authority or direction over local entities.
- Metrics & Milestones: Describes how South Carolina will measure the outputs and outcomes of the program across the entity.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decisions made about risk management activities through various levels of organizations from senior executives to business and process level personnel, including implementation and operations.

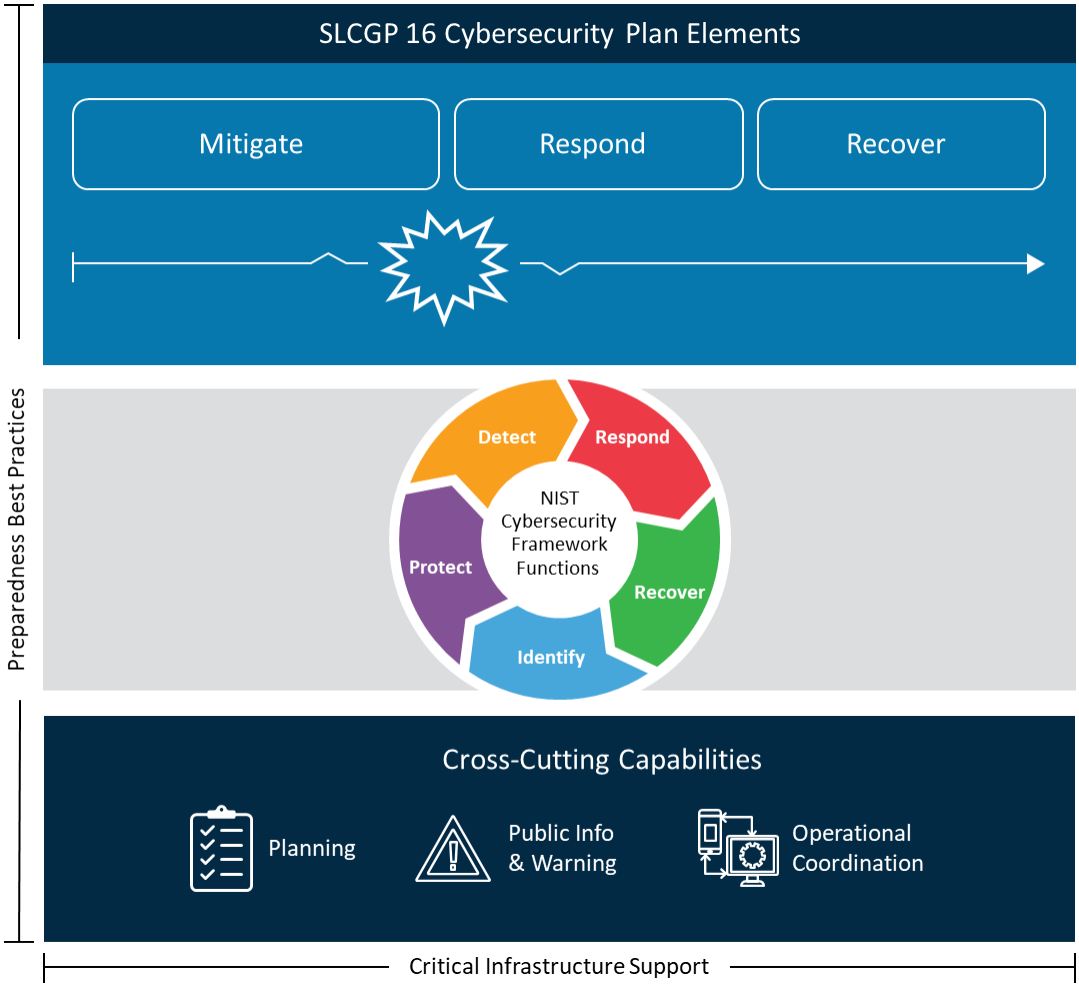

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

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

Vision and Mission

This section describes South Carolina's vision and mission for improving cybersecurity:

Vision:

A state where all South Carolinians are protected from cyber threats, through a collaborative effort between state, local, and critical infrastructure entities that continuously expand and advance cybersecurity training, practices, and adoption of cybersecurity technology.

Mission:

To increase cyber resiliency in South Carolina by leveraging committees, partnerships, and working groups to mature cybersecurity practices and incident response across the state.

Cybersecurity Plan Overview

The Plan's principal purpose is to increase the cyber resiliency of South Carolina's state and local government entities. After reviewing incident response data, cyber posture reviews, and conducting interviews, the SLCGP committee identified goals that would have the biggest impact on improving the cybersecurity practices of these entities. From these goals, objectives were identified that support achieving each goal to aid in meeting and accomplishing the Plan's principal purpose.

As the Plan unfolds under the guidance of the SLCGP committee, the focus will be on specified milestones and strategies, driving the necessary tasks that will ensure the Plan's realization. Nested within these strategies and tasks are the goals and 16 required elements prescribed by the Cybersecurity and Infrastructure Security Agency (CISA), for a clearer correlation between the mandated goals and required elements with this Plan's goals, strategies, and tasks.

At least annually, the Committee will engage in a progress assessment and fine-tuning of the Plan. This proactive approach ensures continuous alignment with the Plan's ambitions, strategies, and tasks, especially when navigating an ever-evolving landscape of cyber challenges.

Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	Program Objectives
1. Enhancing Cyber Resilience	1.1 Facilitate Endpoint Detection and Response (EDR) adoption to raise visibility across network infrastructure and protect state and local government assets in real-time.
	1.2 Conduct and participate in interactive cyber tabletop exercises to assess and improve organization readiness.
	1.3 Support new and existing vulnerability scanning capabilities.
	1.4 Promote and adopt the use of .gov top-level domains to increase confidence in the legitimacy of state and local government websites and communications.
	1.5 Develop and participate in a statewide comprehensive Managed Detection and Response (MDR) function capable of monitoring, alerting, and responding to cybersecurity incidents.
	1.6 Promote the adoption of Domain Name Service (DNS) filtering.
	1.7 Promote the adoption of multi-factor authentication.
	1.8 Deploy a Security Information and Event Management (SIEM) service to ingest security logs, improving threat visibility and reducing the time to detect and respond to incidents.
	1.9 Leverage cloud-based security solutions to support continuous monitoring, flexibility, scalability, and more direct access to provider expertise as well as robust security features such as identity and access management, data classification, or data loss prevention.
	1.10 Deploy immutable storage solutions that protect against unauthorized tampering or deletion of backup data.
2. Cyber Training and Workforce Development (Aligned with NICE Workforce Framework for Cybersecurity)	2.1 Deliver and participate in live fire cyber training through a shared platform to increase incident response readiness statewide.
	2.2 Support and participate in cyber training to ensure on-demand incident response capabilities and essential skills are current.
	2.3 Support new and existing Phishing and Security Awareness capabilities across state and local government entities.
	2.4 Participate in initiatives aimed at fostering cybersecurity training and educational programs to enhance the professional growth and retraining of existing personnel.
	2.5 Grow and support cybersecurity internship, apprenticeship, and scholarship for service programs necessary to develop a proficient cyber workforce.
3. Risk Management	3.1 Support, promote, and utilize CISA's Cross-sector Performance Goals (CPGs).
	3.2 Support, promote, and utilize CISA's Known Exploited Vulnerabilities Catalog in prioritizing patching decisions.
	3.3 Develop and produce cybersecurity progress reports to key stakeholders that identify trends, risks, and emerging threats.

Program Goal	Program Objectives
	3.4 Compile and provide basic cybersecurity policy templates for organizations to customize and implement.
4. Strengthening Information Sharing	4.1 Enhance collaboration and communication with stakeholders.
	4.2 Conduct thorough post-incident reviews after each cybersecurity incident to communicate areas for improvement and implement changes based on lessons learned.
	4.3 Develop and distribute relevant security awareness materials, alerts, and advisories.
	4.4 Foster improved collaboration between statewide cybersecurity initiatives and operators of critical infrastructure and vital resources in South Carolina.

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require support and cooperation from the individuals, groups, or agencies listed above, and may be added as formal agenda items for review during regular governance body meetings.

FUNDING & SERVICES

The Plan was formulated with the acknowledgment that the SLCGP will provide supplemental backing to enhance the resources of state and local government entities. This aims to foster sustainability beyond the designated performance periods. The state has assessed the necessary funding for the future and taken steps to ensure that the projects will continue to be supported through their completion.

Resource Allocation & Prioritization

Efficiently prioritizing and promptly allocating resources is crucial in optimizing the impact of the funds granted by the SLCGP to the State. When deliberating on the most effective distribution of funds, services, equipment, and software to state and local government entities, the Committee will weigh various factors, which encompass, but are not confined to these considerations:

- Endeavors that mitigate cybersecurity vulnerabilities affecting public health, citizen welfare, safety, the economy, or state or national security.
- Undertakings that directly help safeguard the cybersecurity of essential infrastructure systems for state or local government entities.
- Initiatives that align with the program goals and the 16 key elements outlined in the Statewide Cyber Plan.

In addition, the Committee will ensure at least 80% of the funds, services, equipment, and software are allotted to local government entities with 25% of that 80% allotted to rural areas.

ASSESSING CAPABILITIES AND NEEDS

The state and local government capabilities that exist in the state of South Carolina have been assessed using data collected through the SC CIC program to include incident response engagements, cyber posture reviews, and interviews with these entities.

- Incident response – While responding to cybersecurity incidents that affect critical infrastructure in the State, SC CIC performs lessons learned at the end of each engagement to identify security weaknesses in the affected entities. From that data, trends can be identified that indicate where efforts should be focused to improve cybersecurity for the State.
- Cyber Posture Reviews (CPRs) – The Cyber Posture Review is a self-assessment that SC CIC delivers to participants which aligns with CISA's Cybersecurity Performance Goals (CPGs). The CPR data provides unique insights from a strategic perspective across multiple entities. As state and local government falls under the 16 critical infrastructure sectors, this compiled data can be used to identify gaps that can be addressed to strengthen the cybersecurity of those entities.
- Interviews – SC CIC maintains two-way communication with hundreds of entities in the State, which includes state and local governments. These existing relationships allow for direct interactions with local government IT and security staff, which were leveraged to get feedback on issues that can be addressed by the projects in the SLCGP.

The SLCGP committee leveraged these data-driven insights to identify goals that would have the biggest impact on improving the State's overall cybersecurity posture while aligning with the 16 critical objectives identified by CISA.

IMPLEMENTATION PLAN

Organization, Roles, and Responsibilities

The SLCGP Planning Committee Charter outlines the roles, responsibilities, and duties of the SLCGP

Planning Committee (the "Committee") in creating, overseeing, evaluating, and modifying this Plan, as needed. Concurrently, it prioritizes funding efforts and greenlights projects aimed at diminishing cyber risks throughout South Carolina's state and local government entities, in alignment with the Infrastructure Investment and Jobs Act (IIJA) and the SLCGP Notice of Funding Opportunity (NOFO). The SLCGP Committee is currently composed of representation from multiple entities that include:

- South Carolina Governor's Office
- South Carolina Law Enforcement Division (SLED)
    - *South Carolina Critical Infrastructure Cybersecurity (SC CIC)*
- South Carolina Department of Administration
    - *Office of Technology and Information Security (OTIS)*
- South Carolina Office of the Adjutant General
    - *National Guard and Emergency Management*
- South Carolina Election Commission
- Various local government entities

This Plan promotes a comprehensive state defense approach but simultaneously acknowledges the authority, roles, and duties of individual state and local government entities in South Carolina. Each body holds primary responsibility and accountability for upholding its distinct cybersecurity program and performing the daily security and IT management functions of its designated systems and networks. Every state and local government agency is tasked with defining its risk tolerance while instituting administrative, physical, and technical protocols and safeguards based on those limits. Resources like funds, services, hardware, and software, potentially sourced from the SLCGP, are not intended to override, or replace their existing powers or duties. Rather, they aim to boost the agencies' resources, elevating their security stances and bolstering their resilience against evolving threats.

METRICS

Throughout the course of the SLCGP grant process, the Planning Committee will consistently assess advancements made in accordance with the established goals, objectives, and action items outlined in this plan. The Planning Committee and the SAA will collaboratively formulate and support collection of administrative, financial, and other pertinent grant management metrics throughout the duration of the grant. It remains the duty of the Planning Committee to monitor progress through meaningful metrics and comprehensive reporting. A brief description of the metrics that will be used for tracking progress can be found in Appendix C.

APPENDIX 2.

PROJECT MANAGEMENT LIFECYCLE

Steps Description Process

Initiate The authorization to begin work or resume work on any particular activity. Involves preparing for, assembling resources and getting work started. May apply to any level, e.g. program, project, phase, activity, task.
Plan The purposes of establishing, at an early date, the parameters of the project that is going to be worked on as well as to try to delineate any specifics and/or any peculiarities to the project as a whole and/or any specific phases of the project. Involves working out and extending the theoretical, practical, and/or useful application of an idea, concept, or preliminary design. This also involves a plan for moving a project concept to a viable project.
Execute The period within the project lifecycle during which the actual work of creating the project's deliverables is carried out. Involves directing, accomplishing, managing, and completing all phases and aspects of work for a given project.
Control A mechanism which reacts to the current project status in order to ensure accomplishment of project objectives. This involves planning, measuring, monitoring, and taking corrective action based on the results of the monitoring. Involves exercising corrective action as necessary to yield a required outcome consequent upon monitoring performance. Or, the process of comparing actual performance with planned performance, analyzing variances, evaluating possible alternatives, and taking appropriate correct action as needed.
Close Out The completion of all work on a project. Can also refer to completion of a phase of the project. Involves formally terminating and concluding all tasks, activities, and component parts of a particular project, or phase of a project.