The State of Alabama
Agencies and Local Cybersecurity Plan

September 20, 2023

The State and Local Cybersecurity Grant Program (SLCGP) Planning Committee for Alabama is pleased to present the 2022-2026 The State of Alabama Agencies and Local Cybersecurity Plan (the "Plan"). The Plan is a key driver to enable agencies and localities across the state to obtain critical cybersecurity capabilities. This document presents the roadmap to add or enhance capabilities and satisfy the requirement of the current U.S. Department of Homeland Security guidelines for the SLCGP.

The Alabama SLCGP Planning Committee includes representatives from rural, suburban, and urban cities, towns, and counties; public education, public health and public safety. The representatives collaborated to develop the Plan. The Committee developed goals and objectives to ensure Plan completion. These goals and objectives focus on leveraging economies of scale to implement projects and establish resilient program management that reduces and addresses ever-changing cybersecurity risks and work to benefit the represented entities.

Federal funding is projected to be progressively reduced in subsequent SLCGP years. As a result, participants will need to monitor and anticipate increased cost share requirements.

Sincerely,

Daniel Urquhart

Daniel Urquhart,
Chief Information Officer and Chair of Cybersecurity Planning Committee State of Alabama
Office of Information Technology

Table of Contents

Introduction

The content of the Plan follows the Cybersecurity Plan Template provided by, and required by, the FY22 Notice of Funding Opportunity (NOFO) for the State and Local Cybersecurity Grant Program (SLCGP). This template included several sections, which are listed below and referenced throughout the Plan where appropriate.

- Vision and Mission
- Organization, and Roles and Responsibilities
- How feedback and input from local governments and associations was incorporated
- Cybersecurity Plan Elements
- Funding
- Implementation Plan
- Metrics

These required components are included within the Plan below.

Vision and Mission

The State of Alabama Office of Information Technology (OIT) strives to provide consistent, reliable, and secure IT services to executive branch agencies. Recent years have increased the urgency and need for advanced cybersecurity capabilities, which many agencies and localities are unable to provide for themselves. Through the SLCGP, OIT and the Alabama Cybersecurity Planning Committee will support the development of these essential capabilities with local government entities across the state.

Cybersecurity Program Goals and Objectives

The SLCGP Notice of Funding Opportunity (NOFO) sets forward 4 overarching objectives that the state's program goals must meet. These are:

1) Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
2) Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
3) Implement security protections commensurate with risk.
4) Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Alabama seeks to meet these objectives while addressing the most commonly identified cybersecurity maturity challenges. Consideration of these challenges in concert with the SLCGP NOFO objectives led to the selection of the Plan goals.

In addition to addressing the SLCGP objectives, the NOFO specifies 16 required elements to be demonstrated within each state's plan. These elements have been mapped to the Alabama program goals in Appendix B: Project Summary Worksheet and are further referenced within the respective sections of this Plan.

The primary Plan objectives are:

Maturity Assessments and Service Selection

(1a) Cybersecurity maturity assessment surveys, participation, and consent forms

A wide range of cybersecurity capabilities and programs exist within the state of Alabama, from counties with a single employee using Google email addresses, to agencies with dedicated security operations teams and support staff.

A state-wide survey was completed in August 2023 to identify agencies and localities interest in participation and broad sizing of significant cybersecurity gaps. Initial responses are still being collected at the time of this Plan submission.

(1b) Cybersecurity assessments

Many agencies and localities do not know the risks, gaps, or steps to improve their current cybersecurity posture given the limited resources available to them. These cybersecurity assessments will define gaps in current capabilities and serve as the justification for specific projects. Regular assessments, testing, and evaluation to understand risks any planning gaps for additional assessments or evaluation. The SAA and subrecipients will complete the Nationwide Cybersecurity Review (NCSR) during the first award year/subaward period of performance and annually. The cybersecurity assessments for agencies and localities will provide roadmaps for improvement and drive more targeted cybersecurity capability and engagement across the state.

(1c) State-wide cybersecurity services model

The Alabama SLCGP Planning Committee will provide access to foundational cybersecurity services in response to the capability challenges encountered by agencies and localities. The Alabama SLCGP Planning Committee will revise the available services to be offered through Alabama OIT or other options based upon the survey and assessment output from agencies and localities.

(1d) Cybersecurity Coordination

Managing these projects across the state will require coordination. Revising the plan and the projected cybersecurity services model (1c) requires analysis of the surveys, and assessment outputs to identify overarching issues that can and should be addressed with a state-wide service.

(1e) Cybersecurity Training Coordination

In addition to cybersecurity services (1c and project 2), the effort to train and retain competent cybersecurity staff requires specialized coordination and planning. This sub-project tracks the effort to establish and manage the training model.

(1f) Governance and Risk Management Systems

As a stated objective of the NOFO, governance structures to improve cybersecurity capabilities are needed. This project encompasses expanding the Alabama OIT system to provide guidance and frameworks on policies and procedures, as well as support locality requirements and requests for services (1c), which include the selection and scheduling of cybersecurity assessments (1b).

(1g) Management and Administration

This project will track the SLCGP program management of funding to include procurement, schedules, and projects as a separate line item as required by the SLCGP NOFO.

Deploy Foundational Cybersecurity Services

Deploy foundational cybersecurity capabilities to agencies and localities based upon output of Project 1. Many agencies and localities do not have the resources to provide the key cybersecurity capabilities that are needed to properly protect highly targeted government IT systems they use on a day-to-day basis. Therefore, the primary objective of this program will be to expand current capabilities with essential cybersecurity defensive toolsets.

These services are currently planned to include:

(2a) Email hosting of .gov domains

To include mandatory Multi-Factor Authentication (MFA)
Agencies and localities must work with limited available resources. The lack of resources often leads to using cloud-hosted email services like Google instead of a managed solution that can offer added security and reporting.

(2b) Endpoint protection software

Antivirus and Endpoint Agents – monitoring, alerting, and prevention capabilities provide telemetry and active defensive protection across organizations. These tools can prevent potential network compromise events and are increasingly effective at preventing an attacker from gaining an initial foothold at all.

(2c) Routine vulnerability scanning services

Deployment of vulnerability scanning software to perform scheduled internal and external vulnerability scans. Tracking scan results and establishing remediation timelines and standards will eliminate or protect outdated and unsupported operating systems and software.

Offer Cybersecurity Training

(3a) Foundational cybersecurity training

Deploy foundational cybersecurity training. Participants will be allocated a number of "seats" in designated courses, exercises, or other appropriate training methods, once training means are designed by training plan administrators and made available.

Inclusion of Local Government and Association Feedback

The established Alabama SLCGP Planning Committee includes representatives from cities, towns, and counties, rural, suburban, and urban; public education; public health and public safety. As these Alabama programs are extended to the areas across the state, the planning committee will maintain recurring meetings to evaluate and adjust the programs in response to the feedback from the representatives.

Funding

Alabama intends to use 80% of the funds, as required by the SLCGP, to pass through delivery of cybersecurity services and capabilities to agencies and localities. Alabama SLCGP Committee has determined that Alabama will not take nor award individual agency and local entity project requests. These funds provide the ability to meet the Plan objectives. Specific funding requirements for the Plan projects and objectives are detailed within Appendix B: Project Summary Worksheet.

Cost share, if any, will be covered by the State of Alabama through items, services, capabilities, or activities in lieu of funds. The State was granted a cost share waiver for FY22 NOFO funding. Because most of the Alabama SLT entities meet the definition of rural and are geographically widespread, the Alabama SLCGP Committee and the SAA will request Economic Hardship Cost Share Waivers in each NOFO FY. During the first two years, Alabama will use grant funds consistent with a whole-of-state model to pass through cybersecurity items, services, capabilities, or activities. In subsequent years, the SAA may ask agencies and localities to take on, in an increasing share of the cost (e.g., increasing by 25% each year), the purchase of equipment, licenses, or maintenance costs. Alabama anticipates that the implemented benefits of increased cybersecurity capabilities will encourage agencies and localities to allocate their funds to protection and cyber hygiene. Alabama intends to provide initial seeding to entities and then transfer continuation responsibility to entities after the grant period ends, to promote sustainability.

Plan projects are anticipated to be state-run with 20% of the funds, which includes 5% for M&A, used to accomplish whole-of-state projects. Plan projects are expected to continue or expand by year according to priority, needs, and risk mitigation dictates or as NOFO FY funding permits.

Implementation

Organization, Roles, and Responsibilities

Plan implementation is dependent upon several key organizations, and a collaborative effort to deliver effective cybersecurity capabilities across the state. OIT is the State Administrative Agency (SAA) for the SLCGP charged with forming the Alabama SLCGP Planning Committee and administrating the grant program for the state. The Alabama SLCGP Planning Committee developed the Plan and projects with associated funding estimates. Local government entities must opt-in to participate in the SLCGP.

Estimated Implementation Timeline

The table represents anticipated implementation timelines for the Plan objectives.

Alabama SLCGP Implementation Timeline		
Cybersecurity Plan Projects		Target Date
Maturity Assessments and Service Selection	(1a) Cybersecurity maturity assessment surveys	Sept 2023
	(1b) Cybersecurity assessments	June 2024
	(1c) State-wide cybersecurity services model	June 2023
	(1d) Cybersecurity Coordination	April 2024
	(1e) Cybersecurity Training Coordination	April 2024
	(1f) Governance and Risk Management Systems	April 2024
	(1g) Management and Administration	Sept 2023
Deploy Foundational Services	(2a) Email hosting of .gov domains	Dec 2024
	(2b) Endpoint protection software	Dec 2024
	(2c) Routine vulnerability scanning service	June 2023
Offer Cybersecurity Training	(3a) Foundational cybersecurity training	Dec 2024

Metrics

The table below reflects the Plan metrics for tracking as they are implemented. The Plan will adjust as projects are implemented. These metrics provide the needed feedback to identify where these changes are needed.

Alabama Cybersecurity Plan Metrics			
Cybersecurity Plan Projects		Associated Metric(s)	Metric Description
Maturity Assessments and Service Selection	(1a) Cybersecurity maturity assessment surveys and plan	• Number of agencies, cities, counties responded • Plans submitted	Identify interest and submit/revise plan.
	(1b) Cybersecurity assessments	• Number of assessments scheduled/completed	Identify scope and need of services.
	(1c) State-wide cybersecurity services model	• Number of cybersecurity services for deployment	Continuous alignment services and cost allocations.
	(1d) Cybersecurity Coordination	• Number of coordination meetings	While revising the plan is very specific, tracking the coordination efforts will show progress.
	(1e) Cybersecurity Training Coordination	• Number of coordination meetings	While revising the plan is very specific, tracking the coordination efforts will show progress.
	(1f) Governance and Risk Management Systems	• Number of participants using the system	Track usage of the system.
	(1g) Management and Administration	• N/A	
Deploy Foundational Services	(2a) Email hosting of .gov domains	• Number of converted user accounts	Migrate users to .gov
	(2b) Endpoint protection software	• Number of endpoints protected	Track software deployed.
	(2c) Routine vulnerability scanning service	• Number of systems scanned • Report number of vulnerabilities	Report detected vulnerabilities.

Alabama Cybersecurity Plan Metrics			
Cybersecurity Plan Projects		Associated Metric(s)	Metric Description
Offer Cybersecurity Training	(3a) Foundational cybersecurity training	• Number of trainings offered • Number of participants per training	Track training participation metrics

Appendix A: Cybersecurity Plan Capabilities Pre-assessment

To be completed and revised by the Alabama SLCGP Planning Committee based upon survey and assessment output from participating entities.

Plan Required Elements	Description of Current Capabilities	Select capability level from: Foundational, Fundamental, Intermediary, Advanced	Plan Project #(s)	For Assessor (Met/Not Met)
1 – Manage, monitor, and track information systems, applications, and user accounts	Incomplete implementation / Ad-hoc	Foundational	2a, 2b, 2c	
2 – Monitor, audit and track network traffic and activity	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2a, 2b	
3 – Enhance the preparation, response, and resilience of information systems, applications, and user accounts	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2a, 2b, 2c, 3a	
4 - Implement a process of continuous vulnerability assessments and threat mitigation practices prioritized by risk	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2a, 2b, 2c	
5 - Adopt and use best practices including: MFA, enhanced logging, data encryption, ending use of unsupported systems, prohibit use of known/default/fixed credentials, ensure backup/restore capability, and migration to .gov domains	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2a, 2b, 2c	
6 - Promote delivery of safe, recognizable, and trustworthy online services	Incomplete implementation / Ad-hoc	Foundational	1f, 2a, 2c	
7 - Ensure continuity of operations in the event of an incident	Incomplete implementation / Ad-hoc	Foundational	1f, 2b	
8 - Use the NICE Workforce Framework for Cybersecurity to identify workforce gaps and enhance recruitment and retention efforts	Incomplete implementation / Ad-hoc	Foundational	1e, 3a	
9 - Ensure continuity of communications in the event of an incident	Incomplete implementation / Ad-hoc	Foundational	1f, 2a, 2b	

Plan Required Elements	Description of Current Capabilities	Select capability level from: Foundational, Fundamental, Intermediary, Advanced	Plan Project #(s)	For Assessor (Met/Not Met)
10 - Assess and mitigate risks and threats to critical infrastructure and key resources	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2a, 2b, 2c	
11 - Enhance capabilities to share cyber threat indicators	Incomplete implementation / Ad-hoc	Foundational	2a, 2b	
12 - Leverage cybersecurity services offered by CISA – Recipients and sub-recipients will be required to sign up for CISA's Cyber Hygiene Services and complete NCSR	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2c, 3a	
13 - Implement IT and OT modernization review process	Incomplete implementation / Ad-hoc	Foundational	1b, 1f, 2b, 2c	
14 - Develop strategies to address risk and threats	Incomplete implementation / Ad-hoc	Foundational	1b, 1f	
15 - Ensure adequate access and participation in the services by rural areas within the state.	Incomplete implementation / Ad-hoc	Foundational	1a, 1b, 1d, 1e, 1g	
16 - Distribute funds, items, services, capabilities, or activities to local governments	Incomplete implementation / Ad-hoc	Foundational	1a, 1b, 1d, 1e, 1g, 2a, 2b, 2c, 3a	

Appendix B: Project Summary Worksheet

The Project Summary Worksheet is a list of cybersecurity projects that Alabama intends to complete. Cost of projects are represented either by actual (a), TBD (indicating that the uncertainty is high due to related dependencies on predecessor projects, a function of priority alignment, or other mechanisms, controls, or unknowns as of the Plan submission or subsequent revision. These projects address the cybersecurity elements identified in Appendix A: Cybersecurity Plan Capabilities Pre-assessment.

Cybersecurity Plan Projects		Associated SLCGP Elements	Project Description	Cost	Status	Priority	Project Type
Maturity Assessments and Service Selection	(1a) Cybersecurity Plan and maturity assessment surveys	15, 16	Develop initial Plan. Gauge initial interest, needs, and capabilities of agencies and localities.	TBD	In Process	High	Planning Organization M&A
	(1b) Cybersecurity assessments	2, 3, 4, 5, 10, 12, 13, 14, 15, 16	Plan, coordinate, and conduct assessments and maturity reviews for and to identify SLT critical issues, gaps, threats, processes, continuity of operations, and remediations.	TBD	Not Started	High	Planning Organization Equipment Training Exercise
	(1c) State-wide cybersecurity services model	10, 14, 15, 16	Refine planned SLT foundational service offerings.	TBD	Not Started	High	Planning Organization Training Exercise

Cybersecurity Plan Projects		Associated SLCGP Elements	Project Description	Cost	Status	Priority	Project Type
	(1d) Cybersecurity Coordination	15, 16	Establish risk-based plans, define and manage SLT roles, responsibilities, and processes.	TBD	Not Started	High	Planning Organization Equipment Training Exercise M&A
	(1e) Cybersecurity Training Coordination	8, 15, 16		TBD	Not Started	High	Planning Organization Training M&A
	(1f) Governance and Risk Management Systems	2, 3, 4, 5, 6, 7, 9, 10, 13, 14	Whole of State Governance structures to include workflows, methodologies, and systems, licenses to set and measure maturity of asset protections, risk controls/mitigations, compliance standards and evaluations, recovery, and IT processes and security protections.	TBD	Not Started	High	Planning Organization Equipment Training Exercise M&A
	(1g) Management and Administration	15, 16		$192,376.05	Not Started	High	Planning Organization M&A

Cybersecurity Plan Projects		Associated SLCGP Elements	Project Description	Cost	Status	Priority	Project Type
Deploy Foundational Cybersecurity Capability Services	(2a) Email hosting of .gov domains	1, 2, 3, 4, 5, 6, 9, 10, 11, 16	Transition agencies and localities to a hosted email domain; support MFA and user management.	TBD	TBD	High	Equipment, software licensing, PM, implementation professional services
	(2b) Endpoint protection software	1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 16	Address imminent cybersecurity threats, test and deploy continuous endpoint protection software to enable pro-active and automated detection and prevention of malware and attacks against IT systems.	TBD	TBD	High	Planning Equipment Exercises Organization M&A
	(2c) Routine vulnerability scanning service	1, 3, 4, 5, 6, 10, 12, 13, 16	Deploy internal/external vulnerability scanning services to support elimination of outdated systems and software.	TBD	TBD	High	Planning Equipment M&A
Offer Cybersecurity Training	(3a) Foundational cybersecurity training	3, 8, 12, 16	Provide learning platforms and tailored cybersecurity training access.	TBD	TBD	High	Planning Equipment Organization Training Exercise M&A
TOTAL				**TBD**			