Texas Department of Information Resources

Transforming How Texas Government Serves Texans

State of Texas SLCGP Cybersecurity Plan

Version 1.0

September 14, 2023

Approved by the State of Texas Cybersecurity Planning Committee
on September 14, 2023

Table of Contents

Letter From Cybersecurity Planning Committee

Greetings,

The State and Local Cybersecurity Grant Program (SLCGP) Planning Committee for Texas is pleased to present the Fiscal Year 2022-2023 State of Texas SLCGP Cybersecurity Plan (or Cybersecurity Plan). This Cybersecurity Plan represents the State of Texas' continued commitment to supporting and improving the cybersecurity posture of local government entities across the state. This Cybersecurity Plan satisfies the requirements of the current U.S. Department of Homeland Security guidelines for the SLCGP.

The Texas SLCGP Planning Committee comprises representatives from cities, towns, and counties; rural, suburban, and urban areas; higher education and K-12 public education; and public health and safety sectors. This diverse group of representatives collaborated to develop the Cybersecurity Plan with actionable and measurable goals and objectives that target the current known cybersecurity gaps across the state. These goals and objectives for Texas incorporate all required SLCGP elements and focus on building a culture of cyber awareness, preparing and planning for cyber incidents, maturing cyber capabilities, and collaborating and sharing information.

As Texas entities continue to enhance the statewide cybersecurity posture, we must remain dedicated to improving our resilience across disciplines and jurisdictional boundaries. With help from local government entities, we will work to achieve the goals set forth in the Cybersecurity Plan and maintain our position as a model for cyber resilience.

Sincerely,

DocuSigned by:
Amanda Crawford
53180BD9DEA349F...

Amanda Crawford
Executive Director and State Chief Information Officer
Texas Department of Information Resources

DocuSigned by:
Tony Sauerhoff
FD9250ED2F864A9...

Tony Sauerhoff
State Cybersecurity Coordinator and Chair of Cybersecurity Planning Committee
Texas Department of Information Resources

Introduction

The content of the plan follows the Cybersecurity Plan Template provided and required by the Notice of Funding Opportunity for the SLCGP.

The Cybersecurity Plan is a two-year strategic planning document that contains the following components:

- **Vision and Mission:** Articulates the vision and mission of the SLCGP Planning Committee for improving cybersecurity resilience over the next one to three years.
- **Organization, Roles, and Responsibilities:** Describes the current roles and responsibilities—and any governance mechanisms—for cybersecurity as well as successes, challenges, and priorities for improvement. This section includes a strategy for the cybersecurity program and the organizational structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of the State of Texas' cybersecurity program. The Cybersecurity Plan is a guiding document required by the SLCGP and does not create any authority or direction over any of the State of Texas' local systems or agencies, or any branch of the Texas State Government.
- **Local Governments and Associations Feedback Incorporated:** Describes how input from local governments was used to reduce overall cybersecurity risk across the eligible entity, which is especially important in developing a holistic cybersecurity program.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding and Services:** Describes funding sources and allocations to build cybersecurity capabilities within the state of Texas along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the State of Texas' plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of—and progress toward—the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how the State of Texas will measure the outputs and outcomes of the program across the entity.

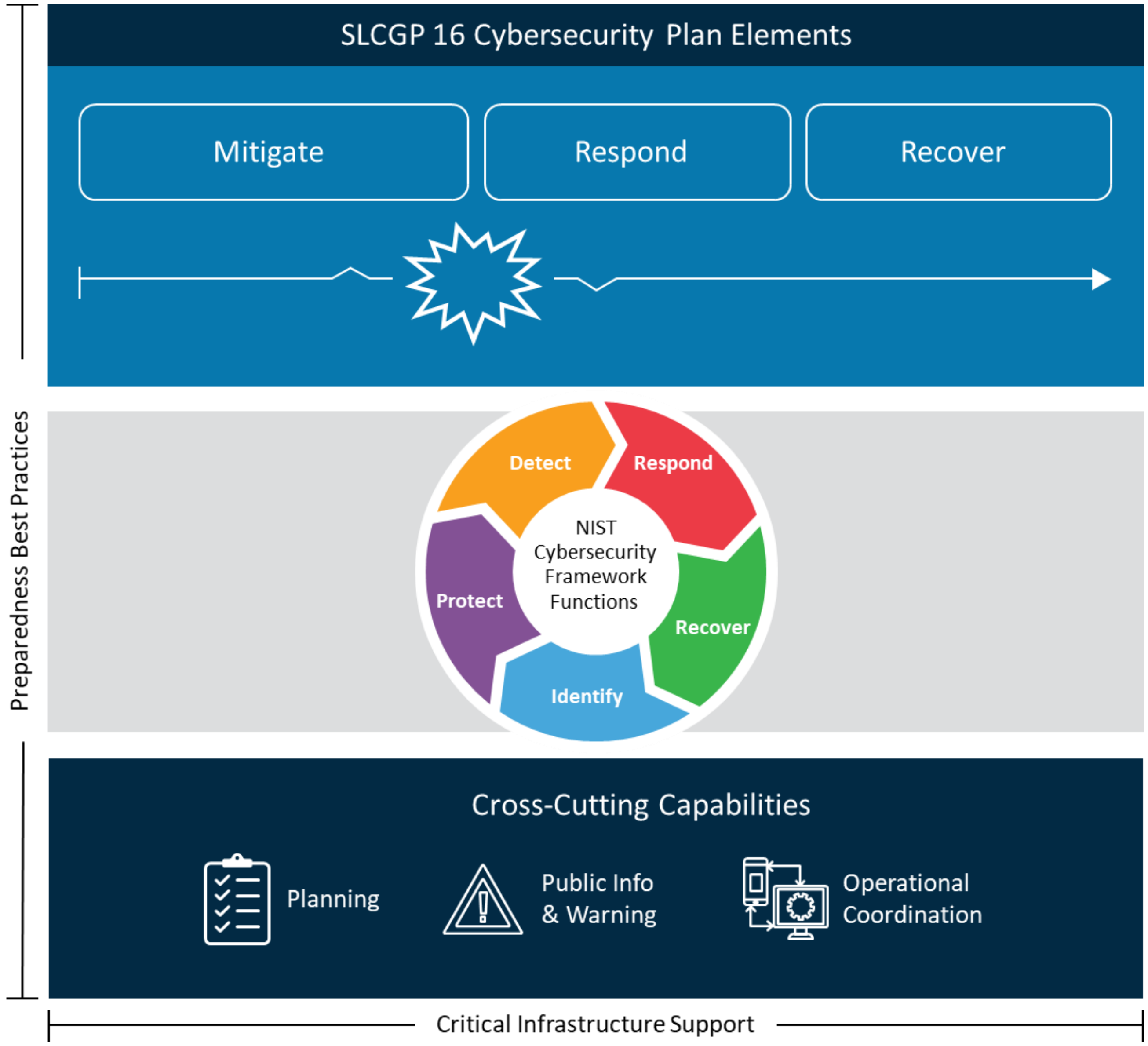

SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

Figure 1 Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

Vision and Mission

This section describes the vision and mission for improving cybersecurity across Texas.

Vision:

Texas will use its resources efficiently, collaboratively, and effectively to form a protected and resilient cybersecurity environment and create a risk-aware culture that prioritizes protecting information.

Mission:

To assist public sector security personnel in improving their organization's cybersecurity effectiveness through alignment with statewide goals.

Cybersecurity Program Goals and Objectives

Cybersecurity goals and objectives for this program are based on the Texas Cybersecurity Strategic Plan for fiscal years 2018-2023 and the requirements of the Department of Homeland Security Notice of Funding Opportunity for the fiscal year (FY) 2022 SLCGP. As statewide progress is made, the Cybersecurity Plan will be updated and resubmitted to add more mature objectives in future years.

Program Goal	Program Objectives
1 Improve and refine SLCGP Cybersecurity Plan.	Work with committee to ensure Plan aligns with statewide needs.
2 Build a culture of cyber awareness.	Provide outreach to share free and low-cost resources with local entities.
3 Implement multi-factor authentication.	Encourage the implementation of multi-factor authentication at all local entities.

4 Implement enhanced logging.	Encourage the implementation of enhanced logging at all local entities.
5 Implement data encryption for data at rest and data in transit.	Encourage the implementation of encryption for data at rest and data in transit.
6 End use of unsupported/end-of-life software and hardware that are accessible from the internet.	Encourage the replacement of all unsupported/end-of life-software and hardware that are accessible from the internet.
7 Prohibit use of known/fixed/default passwords and credentials.	Encourage all local entities to prohibit the use of known/fixed/default passwords and credentials.
8 Ensure the ability to reconstitute systems (backups).	Encourage the adoption of capabilities to reconstitute systems.
9 Migrate local entities to .gov domain.	Encourage all local entities to migrate to the .gov internet domain.
10 Improve incident response capabilities.	Encourage all local entities to establish and test an incident response plan.
11 Collaborate and share information.	Grow the Texas Information Sharing and Analysis Organization (TX-ISAO) and encourage members to share information on threats and vulnerabilities impacting the state.

Cybersecurity Plan Elements

The Cybersecurity Plan contains the following elements.

Manage, Monitor, and Track

At the state and local levels, entities should establish procedures that effectively control and restrict access to agency information assets. State and local entities should authorize users based on defined business and legal requirements (essentially, access should be limited to a "need-to-use" and/or "need-to-know" basis). Entities should implement mechanisms that provide for the control, administration, and tracking of access to—and the use of—information assets, including the protection of such assets from unauthorized or unapproved activity and destruction.

Entities should remove any systems and technology that are no longer supported by the manufacturer from the network as soon as practicable or implement additional protections if the systems or technology are required.

Monitor, Audit, and Track

Asset owners, asset custodians, and information security and privacy officers at the state and local levels should:

- Ensure that the information assets under their purview are assessed for security and privacy risks. The assets should be configured such that event logging is enabled to ensure an adequate level of situational awareness regarding potential threats to the confidentiality, integrity, availability, and privacy of agency information and information systems, and that threats are identified and managed; and
- Review and retain event logs in compliance with all applicable local, state and federal laws, regulations, executive orders, circulars, directives, internal agency and State of Texas policies, and contractual requirements.

The Texas Department of Information Resources (DIR) is implementing a Regional Security Operations Center (RSOC) program that will provide system and network traffic monitoring for local government entities. The first RSOC was established in San Angelo, in partnership with Angelo State University. The Texas Legislature funded two additional RSOCs in 2023 that will be located in Edinburg, and Austin, in partnership with the University of Texas Rio Grande Valley and the University of Texas at Austin, respectively.

Enhance Preparedness

State and local government entities should implement continuous risk management processes that account for the identification, assessment, treatment, and monitoring of risks that can adversely impact their operations, information systems, and information. These processes will inform the exercise and execution of incident response plans and continuity of operations plans. Lessons learned from these exercises will be incorporated into future planning, inform organizational decisions, and aid in identifying additional equipment and training needs.

Texas local government entities have access to the DIR statewide Cybersecurity Incident Response Team (CIRT) and Volunteer Incident Response Team (VIRT) for cyber incident response support.

DIR's Office of the Chief Information Security Officer (OCISO) provides an incident response team Redbook template that can be used as a framework for local government entities to use while creating their own incident response plan documents. Through the TX-ISAO, DIR also provides a monthly tabletop exercise scenario with supporting resources (such as PowerPoint presentations, facilitator guides, and situation manuals). The CIRT is also available to facilitate incident response tabletop exercises.

The State of Texas requires local government entities to administer annual cybersecurity awareness training. Employees, elected officials, and appointed officials who have access to a local government computer system or database and use a computer to perform at least 25 percent of their duties are required to take annual training. School districts are the exception to this requirement as state law only requires the district's cybersecurity coordinator to complete annual cybersecurity training. The state provides a free training offered in both English and Spanish and certifies over 100 training programs that state and local entities may choose to use.

Assessment and Mitigation

All information technology (IT) systems and applications operated by—or on behalf of—state and local government entities should undergo vulnerability assessments to ensure adequate security controls are implemented and risks are identified and managed to acceptable levels throughout their lifecycles. Risk management processes include identifying, assessing, and addressing security risks at the inception of the project until its decommissioning. These actions enable state and local government entities to maintain the security of a system throughout its lifecycle. To aid in satisfying the ongoing assessment requirements, assessment results from the following sources can be used: continuous monitoring, audits and authorizations, and other system development life cycle activities.

Recipients and sub-recipients of SLCGP funds are required to sign-up for Cybersecurity and Infrastructure Security Agency (CISA) cyber hygiene services: vulnerability scanning and web application scanning. Other entities are not required to use these services but are encouraged to do so.

Best Practices and Methodologies

The Cybersecurity Planning Committee will prioritize individual projects that assist entities with adopting the following best practices and methodologies that enhance cybersecurity:

- Implementing multi-factor authentication.
- Implementing enhanced logging.

- Implementing data encryption for data at rest and data in transit.
- Ending use of unsupported/end of life software and hardware that are accessible from the internet.
- Prohibiting use of known/fixed/default passwords and credentials.
- Ensuring the ability to reconstitute systems (backups).
- Migrating to the .gov internet domain.

Safe Online Services

Utilizing the .gov domain is a priority for government entities to promote the delivery of safe, recognizable, and trustworthy online services. For those entities with websites that are not already on the .gov domain, individual projects must include this migration in order to be considered for funding.

Continuity of Operations

State and local government entities will be required to develop, update, implement, test with exercises, and maintain Continuity of Operations (COOP) plans for all information systems that deliver or support essential or critical functions. This will enhance the availability of critical and essential systems to ensure those functions can be continued throughout, or resumed rapidly after, a disruption of normal operations.

Workforce

Enhanced workforce recruitment and retention policies will be developed based upon the National Initiative for Cybersecurity Education (NICE) framework to identify and mitigate any gaps in cybersecurity workforces of the state or local governments. In addition, these policies enhance recruitment and retention efforts for those workforces. Efforts will be made to 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.

Continuity of Communications and Data Networks

As part of COOP plans, options such as a crisis communications service for notification of employees and Web Emergency Operations Center (WebEOC) for crisis management will be considered. Analysis of interconnection issues between systems that may lead to a secondary impact when one or the other is affected by an incident will be performed. Using a risk-based approach, state and local governments will deploy backup solutions for the critical services that they provide to their constituents. IT, Internet of things (IOT), operational technology (OT), cyber resilience, and threat mitigation programs will be explored and considered. Entities should establish guidelines and standards for these critical services.

Disaster recovery and business continuity tabletop exercises will be performed as backup solutions and services are developed.

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

The approach to assess and mitigate cybersecurity risks and threats to critical infrastructure and key resources (CIKR) includes working with the Texas Critical Infrastructure Protection Coordinator to ensure CIKR across the state are first identified. Next, layers of mitigation such as participation in the TX-ISAO and participation in the Texas Infrastructure Protection Taskforce are encouraged. Any available training through the training investment as well as open-source training will be promoted and made available.

Cyber Threat Indicator Information Sharing

DIR manages the TX-ISAO for the sharing of cyber threat indicators and related information between the State and state and local governments, CISA, the Multi-State Sharing and Analysis Center (MS-ISAC), and other public and private partners. TX-ISAO members have access to a secure portal to share information with other members. Prior to September 1, 2023, local governments in Texas voluntarily reported cyber incidents; as of September 1, 2023, state law requires local governments to report cyber incidents to the state. Incident information shared with the state is anonymized and non-sensitive information is shared with other TX-ISAO members.

Leverage CISA Services

Local government entities are encouraged to use cybersecurity services provided by CISA. Recipients of SLCGP funds are required to sign-up for CISA's vulnerability scanning and web application scanning services. To register for these services, entities should email vulnerability_info@cisa.dhs.gov with the subject line “Requesting Cyber Hygiene Services – SLCGP.” The body of the email should indicate that the request is part of the SLGCP.

The Nationwide Cybersecurity Review (NCSR) is a free and anonymous annual self-assessment designed to measure gaps and capabilities of a state, local, and territorial cybersecurity program. The NCSR is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is sponsored by the Department of Homeland Security and the MS-ISAC. SLCGP grant recipients must complete the NCSR, administered by the MS-ISAC, during the first year of the award/subaward period of performance and annually thereafter.

SLCGP grant recipients are strongly encouraged to become a member of the MS-ISAC and/or Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), as applicable. Membership is free.

The MS-ISAC receives support from—and has been designated by—the Department of Homeland Security as the cybersecurity information sharing and analysis center for state, local, and territorial governments. The MS-ISAC provides services and information sharing that significantly enhances state, local, and territorial governments' ability to prevent, protect against, respond to, and recover from cyberattacks and compromises. The Department of Homeland Security maintains operational-level coordination with the MS-ISAC through the presence of MS-ISAC analysts in CISA Central to coordinate directly with its own 24/7 operations center that connects with state, local, and territorial government stakeholders on cybersecurity threats and incidents. To register, visit https://learn.cisecurity.org/ms-isac-registration.

The EI-ISAC is a collaborative partnership between the Center for Internet Security (CIS), CISA, and the Election Infrastructure Subsector Government Coordinating Council. The EI-ISAC is funded through Department of Homeland Security grants and offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and training products. To register, please visit https://learn.cisecurity.org/ei-isac-registration.

Information Technology and Operational Technology Modernization Review

The approach to modernizing IT and OT should employ a strategy in which OT, Internet of Things (IoT), Industrial Internet of Things (IIoT), and IT security are managed as part of a coordinated effort—a comprehensive approach to safeguarding data, systems, and people from cyber threats. Cybersecurity goals and strategies for IT and OT should align with the business objectives and culture and promote security-conscious practices among all stakeholders. Alignment of these technologies requires continuous evaluation and improvement of the security posture, and proactive incident response and recovery. Following this approach combines IT and OT functions rather than seeing them as distinct functions. The State will seek opportunities to train local entities in this approach and its methodologies.

Cybersecurity Risk and Threat Strategies

The Cybersecurity Planning Committee will consult with various stakeholder groups with the state including Texas' 24 regional Councils of Government (COGs) to develop and coordinate strategies to address cybersecurity risks and cybersecurity threats at the local level.

Rural Communities

Rural communities are assured access to funding under the SLCGP through outreach activities supported by the Cybersecurity Planning Committee. Additionally, the funding distribution plan in Texas is to divide available funds by region, by population. This approach will ensure that rural communities receive adequate participation in the program based on their populations.

Funding and Services

The federal allocation for Texas for FY22 is $8,465,324. Matching funds will be $846,532.40, making a total of $9,311,856.40 available to be spent on cybersecurity projects for FY22 via the SLCGP.

The federal allocation for Texas for FY23 will be approximately $17,418,110. Matching funds will be approximately $3,483,622, making a total of approximately $20,901,732 available to be spent on cybersecurity projects for FY23 via the SLCGP.

Matching funds will be paid by grant recipients/sub-recipients. All local government entities will be required to fund their own matching funds for all approved projects.

The matching funds percentage will increase annually according to the list below:

- FY22 – 10%
- FY23 – 20%
- FY24 – 30%
- FY25 – 40%

The State of Texas SLCGP Planning Committee intends to focus on five key efforts to strengthen cybersecurity across the State. These efforts are to:

- Update and refine this Cybersecurity Plan.
- Fund cybersecurity protections for local government entities commensurate with risk.
- Fund cybersecurity training for local government entities commensurate with responsibility.
- Ensure projects align with the required elements and best practices listed in this plan.
- Ensure projects only fund one-time cybersecurity services to ensure that this program does not become an unfunded mandate on local government entities.

Distribution to Local Governments

The maximum amount of SLCGP funds will be made available to local government entities. Texas will divide funds by geographic region by population according to the state's 24 regions.

The State of Texas will pass through a minimum of 80% of the funding received through SLCGP to local government entities. As part of the local pass-through requirement, at least 25% of the federal funds provided under the grant will be passed through to rural areas. Texas is expected to pass through more than the required 25% to rural areas, as many of the state's municipalities currently meet the designation of rural area.

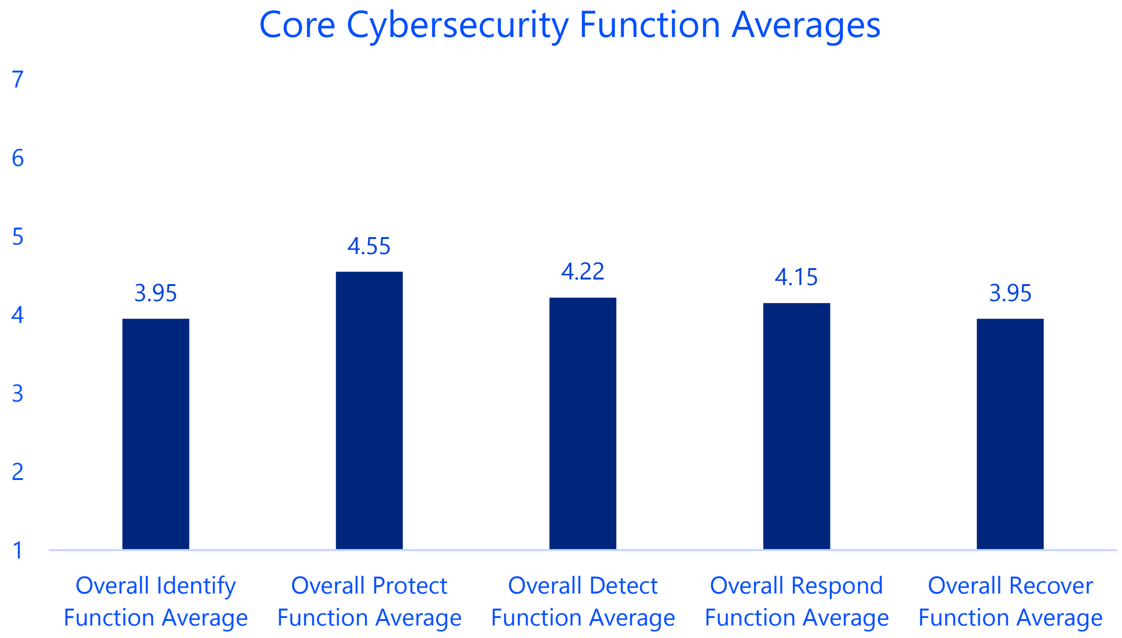
Assess Capabilities

One of the biggest challenges facing states is how to assess cybersecurity maturity and capabilities at the local entity level. There are numerous complications in gaining a true local picture including: lack of trust to share information, lack of understanding on the part of the local entity, lack of human resources to address the topic, and the sample size of those who are willing to participate is not always representative of the whole. Those local entities that are willing to participate and share their capabilities are usually more mature and feel more confident in sharing their gaps in capabilities.

The State of Texas commits a great deal of resources to improving communications and establishing trust with local entities through its outreach efforts. Information learned through outreach efforts combined with data from the 2021 NCSR assessment was used to complete Appendix A: Cybersecurity Plan Capability Assessment. With over 7,200 local government entities across Texas, these data sets are not comprehensive, but are representative of the needs found by the state. This information informed discussions by the Planning Committee.

In 2021, 230 local government entities in Texas, the majority of which were cities, participated in the NCSR. The NCSR is a cybersecurity self-assessment that measures maturity in five functional areas (Identify, Protect, Detect, Respond and Recover) and is based on the NIST Cybersecurity Framework (CSF).

The NCSR ranks agency responses on a seven-point maturity scale. Local government entities scoring between three and five are either in the process of developing their policies and standards or implementing the controls required by those documents.



Source: 2021 NCSR

The following chart shows a breakdown of NCSR overall averages by responding entity category:

Entity Category	Number of Responses	NIST CSF Function (average by entity category)				
		Identify	Protect	Detect	Respond	Recover
Texas State (214 agencies aggregated to one report)	1	5.43	5.46	5.74	6.09	6.00
Counties	58	3.98	4.67	4.43	4.29	4.09
Cities	93	3.98	4.71	4.33	4.23	3.94
K-12	18	3.42	3.75	3.57	3.71	3.54
Public Safety	16	4.73	4.88	4.64	4.66	4.54
Fire EMS 911	8	2.67	3.09	3.06	3.41	3.07
Other*	37	4.01	4.51	3.99	3.87	3.91

**Other includes categories with < 5 respondents: Town/Village, Associations, Commissions, Local Public Utilities, Local Health Services, Local Elections, Local Community College, Local Mass Transit.*

Source: 2021 NCSR

These results indicate that assistance is needed in all functional areas of the NIST CSF in local government entities across Texas.

More detail is listed in Appendix A: Cybersecurity Plan Capabilities Assessment.

Implementation Plan

The implementation plan contains the following elements.

Organization, Roles, and Responsibilities

The State of Texas SLCGP Planning Committee includes voting members from state, county, city, and town governments as well as champions from public education and public health institutions to ensure the Cybersecurity Plan goals are achieved. To ensure statewide perspectives, members of the Committee are also representatives of urban, suburban, and rural areas of the state. The Committee shall develop, approve, implement, monitor, review, and revise (as appropriate) the Cybersecurity Plan that establishes funding priorities. The Committee makes funding recommendations for projects to the Office of the Governor, who is the State Administrative Agency (SAA), which are intended to identify, assess, and address cyber risks within and across state and local government organizations in the state of Texas in accordance with the requirements of the Infrastructure Investment and Jobs Act (IIJA) and SLCGP.

The State Cybersecurity Coordinator will act as Chair of the Committee. The State Cybersecurity Coordinator will be responsible for ensuring the execution and reporting of the Cybersecurity Plan priorities and maintaining a diverse committee membership wherein all government entities are represented. The Chair of the Committee and/or Co-Chair, with the consent of the Committee members, may invite representatives from public and private sector organizations within the state to act as advisors to the Committee, providing varied perspectives and guidance. Such relevant groups may include the Texas Association of Counties (TAC), Texas Municipal League (TML), Texas Education Agency (TEA), Texas Commission on Environmental Quality (TCEQ), and leading vendors in key strategic risk mitigation areas.

The Committee shall provide ongoing communication of required documentation and project reporting to all stakeholders throughout the SLCGP period of performance. The Committee shall meet as deemed appropriate by the Chair or Co-Chair of the Committee. Both will ensure that meetings are documented. The Chair and/or Co-Chair will consult with the SAA as appropriate. The Office of the Governor as SAA will be responsible for administrating the grant program. All grant activities shall comply with the requirements set forth in the applicable SLCGP Notice of Funding Opportunities.

Below is a table showing all Planning Committee members and supporting staff:

Representation	Role	Name	Title	Organization
Eligible entity	Chair	Tony Sauerhoff	State Cybersecurity Coordinator	DIR

State Chief Information Security Officer (CISO)	Co-Chair	Nancy Rainosek	State CISO	DIR
State Administrative Agency (SAA)	Voting Member	Robert Cottle	Director of Planning and Grant Programs	Office of the Governor
County	Voting member	Ted Daniels	IT Director	Duval County
City	Voting member	Tony Gonzalez	IT Director	City of New Braunfels (Texas Association of Governmental Information Technology Managers Past President)
Town	Voting member	William Pham	Chief Technology and Innovation Officer (CTIO)	The Woodlands
Institution of Public Education	Voting member	Todd Pauley	Deputy CISO / CISO	TEA
Institution of Public Education	Voting member	Luis Hernandez	Vice President, Information Resources	University of Texas at El Paso
Institution of Public Education	Voting member	Keith Bryant	Superintendent	Lubbock-Cooper ISD
Institution of Public Health	Voting member	Roberto Beaty	Associate Commissioner for Program Operations	Department of State Health Services
DIR Legal Counsel	Ex-officio	Josh Godbey	General Counsel	DIR
DIR Executive Director and State CIO	Ex-officio	Amanda Crawford	Executive Director and State CIO	DIR
DIR Public Affairs	Ex-officio	Brady Vaughn	Director of Public and Strategic Affairs	DIR

Resource Overview and Timeline Summary

The Office of the Governor and DIR will provide the necessary resources to oversee grant administration and performance oversight.

The anticipated timeline for the 2022 funding cycle is as follows:

Activity	Date
Submit SLCGP Cybersecurity Plan to CISA	September 15, 2023
CISA approval of SLCGP Cybersecurity Plan	November 30, 2023
Notify local entities of application process and make sub-grant applications available	December 15, 2023
Grant application submissions due	February 15, 2024
Applications evaluated by SAA and SLCGP Planning Committee	April 15, 2024
Submission of projects and revised Investment Justifications to FEMA	May 15, 2024
FEMA releases funds	Pending CISA project approval
Grant agreements executed/projects funded – 45 days after release of funds	Within 45 days of notification of project approval

Applicant Requirements

To receive grant funding from the State of Texas through the SLCGP program, each sub-recipient must meet the following requirements:

- Must be able to provide matching funds.
- Rural communities must meet the 49 U.S.C. § 5302 definition of a rural area stated in the NOFO.
- Must be a member of the TX-ISAO (membership is free).
- Sign up for free CISA cyber hygiene services, specifically vulnerability scanning and web application scanning.
- Local units of governments must comply with the Cybersecurity Training requirements described in Texas Government Code Section 772.012 and Section 2054.5191e.
- All FY22 SLCGP sub-recipients must complete the NCSR by December 1, 2023. To receive SLCGP funds in subsequent years, entities must annually complete the NCSR.

Sub-recipients are strongly encouraged to:

- Join MS-ISAC (membership is free).

Metrics

This table reflects the goals and objectives of the Texas SLCGP program:

Cybersecurity Plan Metrics

Program Goal	Program Objectives	Metric Description
Improve and refine SLCGP cybersecurity plan	Work with committee to ensure plan aligns with statewide needs.	CISA approves statewide plan
Build a Culture of Cyber Awareness	Provide outreach to share free and low-cost resources with local entities.	Number of resources provided by the state and by CISA. Number of members who have joined the TX-ISAO.
Implement multi-factor authentication	Encourage the implementation of multi-factor authentication at all local entities.	Number of sub-recipients who have or are implementing multi-factor authentication.
Implement enhanced logging	Encourage the implementation of enhanced logging at all local entities.	Number of funded projects that include enhanced logging capabilities.
Data encryption for data at rest and in transit	Encourage the implementation of encryption for data at rest and in transit.	Number of funded projects that include data encryption.
End use of unsupported/end of life software (SW) and hardware (HW) that are accessible from the Internet	Encourage the replacement of all unsupported/end of life SW/HW that is accessible from the Internet.	Number of funded projects that include the replacement of unsupported/end of life SW/HW.
Prohibit use of known/fixed/default passwords and credentials	Encourage all local entities to prohibit the use of known/fixed/default passwords and credentials.	Number of entities with policies prohibiting use of known/fixed/default passwords and credentials.

Ensure the ability to reconstitute systems (backups)	Encourage the adoption of capabilities to reconstitute systems.	Number of funded projects that include capabilities to reconstitute systems.
Migration to the .gov internet domain	Encourage all local entities to migrate to the .gov internet domain.	Number of sub-recipients who have already migrated to the .gov domain or funded projects that include services to migrate to the .gov domain.
Improve incident response capabilities	Encourage all local entities to establish and test an incident response plan.	Number of entities reporting the existence of an incident response plan.
Collaborate and Share Information	Grow the TX-ISAO.	Number of TX-ISAO members. Number of members who have joined the TX-ISAO.
	Share information on threats and vulnerabilities impacting the state.	Number of times members share information with the TX-ISAO. Number of alerts the TX-ISAO shares with members.

Appendix A: Cybersecurity Plan Capabilities Assessment

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	Brief Description of Current Capabilities of SLTT within the Eligible Entity	Select capability level from: Foundational Fundamental Intermediary Advanced	Project # (s) (If applicable – as provided in Appendix B)	Met
1. Manage, monitor, and track information systems, applications, and user accounts.	Incomplete implementation across the totality of the state and local government entities.	Foundational	18, 19	
2. Monitor, audit, and track network traffic and activity.	Incomplete implementation across the totality of the state and local government entities.	Foundational	16, 17, 22, 23	
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts.	Incomplete implementation across the totality of the state and local government entities.	Foundational	8, 10, 19, 20	
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk.	Incomplete implementation across the totality of the state and local government entities.	Fundamental	19, 20, Free CISA services in Year 1	

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** **Foundational** **Fundamental** **Intermediary** **Advanced**	**Project # (s)** **(If applicable – as provided in Appendix B)**	**Met**
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST).	Incomplete implementation across the totality of the state and local government entities.	Foundational	1, 2, 3, 4, 5, 6, 7, 19, 20	
a. Implement multi-factor authentication.	Incomplete implementation across the totality of the state and local government entities.	Foundational	1	
b. Implement enhanced logging.	Incomplete implementation across the totality of the state and local government entities.	Foundational	2	
c. Data encryption for data at rest and in transit.	Incomplete implementation across the totality of the state and local government entities.	Intermediary	3, 23	
d. End use of unsupported/end of life software and hardware that are accessible from the Internet.	Incomplete implementation across the totality of the state and local government entities.	Foundational	4	

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** **Foundational** **Fundamental** **Intermediary** **Advanced**	**Project # (s)** **(If applicable – as provided in Appendix B)**	**Met**
e. Prohibit use of known/fixed/default passwords and credentials.	Incomplete implementation across the totality of the state and local government entities.	Foundational	5	
f. Ensure the ability to reconstitute systems (backups).	Incomplete implementation across the totality of the state and local government entities.	Intermediary	6	
g. Migration to the .gov internet domain.	Incomplete implementation across the totality of the state and local government entities.	Intermediary	7	
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain.	Incomplete implementation across the totality of the state and local government entities.	Intermediary	7, 22, 23	
7. Ensure continuity of operations including by conducting exercises.	Incomplete implementation across the totality of the state and local government entities.	Intermediary	8	

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				**FOR ASSESSOR**
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** **Foundational** **Fundamental** **Intermediary** **Advanced**	**Project # (s)** **(If applicable – as provided in Appendix B)**	**Met**
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity).	Incomplete implementation across the totality of the state and local government entities.	Intermediary	N/A Year 1	
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks.	Incomplete implementation across the totality of the state and local government entities.	Intermediary	6, 8	

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** **Foundational** **Fundamental** **Intermediary** **Advanced**	**Project # (s)** **(If applicable – as provided in Appendix B)**	**Met**
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity.	Incomplete implementation across the totality of the state and local government entities.	Fundamental	1, 2, 3, 4, 5, 6, 7, 8, 9, 19, 20, 21, 22, 23	
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department.	Incomplete implementation across the totality of the state and local government entities.	Intermediary	9	
12. Leverage cybersecurity services offered by the Department.	Incomplete implementation across the totality of the state and local government entities.	Foundational	8, 9	

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** **Foundational** **Fundamental** **Intermediary** **Advanced**	**Project # (s)** **(If applicable – as provided in Appendix B)**	**Met**
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.	Incomplete implementation across the totality of the state and local government entities.	Fundamental	N/A Year 1	
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.	Incomplete implementation across the totality of the state and local government entities.	Advanced	Ongoing effort by Cybersecurity Planning Committee and stakeholders	
15. Ensure rural communities have adequate access to, and participation in plan activities.	Incomplete implementation across the totality of the state and local government entities.	Advanced	Cybersecurity Planning Committee Priority	

COMPLETED BY the State of Texas SLCGP Cybersecurity Planning Committee				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of SLTT within the Eligible Entity**	**Select capability level from:** **Foundational** **Fundamental** **Intermediary** **Advanced**	**Project # (s)** **(If applicable – as provided in Appendix B)**	**Met**
16. Distribute funds, items, services, capabilities, or activities to local governments.	Incomplete implementation across the totality of the state and local government entities.	Advanced	Cybersecurity Planning Committee Priority	

Appendix B: Project Summary Worksheet

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment.**

The State of Texas intends to pass through over 90% of SLCGP funds to local government entities across the state. The projects listed below are estimates of a single project for one local government entity. With over 7,200 local government entities in Texas, the projects below will be replicated many times and will vary greatly in scope and cost for each sub-recipient. Actual budgets are not available as no projects have yet been selected for funding.

1. ID	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
1	MFA	Implement multi-factor authentication for all remote access and privileged accounts within a local government entity.	5	$50,000.00	Future	High	Equip
2	Enhanced Logging	Implement enhanced logging for systems within a local government entity.	5	$50,000.00	Future	High	Equip
3	Data Encryption	Implement data encryption for data at rest and data in transit for a local government entity.	5	$50,000.00	Future	High	Equip
4	End-of-support (EoS)/ End-of-life (EoL) HW/SW	End use of unsupported EoS/ EoL software and hardware within a local government entity.	5	$100,000.00	Future	High	Equip

1. ID	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
5	Default Passwords	Prohibit use of known/fixed/default passwords and credentials on all systems within a local government entity.	5	$10,000.00	Future	High	Equip
6	Backups	Ensure the ability to reconstitute critical systems within a local government entity.	5	$50,000.00	Future	High	Equip
7	.gov Domain	Migrate a local government entity to the .gov domain.	6	$50,000.00	Future	High	Equip
8	Incident Response Plan	Establish and test an incident response plan at a local government entity.	3, 7	$25,000.00	Future	High	Train
9	Collaborate and Share Information	Grow the TX-ISAO and share information on threats and vulnerabilities impacting the state.	14	$100,000.00	Future	High	Equip
10	Endpoint Detection and Response (EDR)	Implement Endpoint Detection and Response.	10	$50,000.00	Future	Medium	Equip

1. ID	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
11	Cyber/IT Staff Training	Provide training to cyber/IT staff to enhance the knowledge, skills, and abilities to implement cybersecurity best practices and respond to incidents.	8	$25,000.00	Future	High	Train
12	Security assessments	Conduct security assessments to evaluate an entity's maturity level and provide recommendations for improving the security maturity and posture of the organization.	10	$25,000.00	Future	Medium	Plan
13	Cloud strategy	Develop a cloud migration strategy.	5, 9	$25,000.00	Future	Medium	Plan
14	Cloud migration	Migrate an organization's applications and data to the cloud.	5, 9	$25,000.00	Future	Medium	Equip
15	Uninterruptible Power Supply (UPS) Backup Power	Deploy UPS systems to support critical systems.	7, 9	$15,000.00	Future	Medium	Equip
16	Firewalls	Implement web application firewalls to monitor and filter web traffic.	2	$15,000.00	Future	High	Equip

1. ID	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
17	Intrusion Detection System/Intrusion Prevention System (IDS/IPS)	Implement IDS/IPS to detect and prevent cyber-attacks.	2	$15,000.00	Future	Medium	Equip
18	Automated asset discovery	Install automated asset discovery to identify and catalogue all the systems, services, hardware, and software.	1	$25,000.00	Future	High	Equip
19	Vulnerability Scanning	Implement scanning solution to scan IT assets for vulnerabilities.	1, 3, 4, 5, 10	$25,000.00	Future	High	Equip
20	Vulnerability Patching	Implement patching solution to patch vulnerabilities in IT assets.	3, 4, 5, 10	$25,000.00	Future	High	Equip
21	Penetration Test	Conduct penetration tests to check for exploitable vulnerabilities on a computer network.	10	$50,000.00	Future	Medium	Exercise
22	Web Filtering	Implement web filtering solution to scan web traffic for cyber threats.	2, 6	$25,000.00	Future	High	Equip

1. ID	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
23	Virtual Private Network (VPN)	Implement VPN solution to encrypt all traffic to/from remote users.	2, 5, 6	$25,000.00	Future	High	Equip

Appendix C: Entity Metrics

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
1. The State of Texas has an approved Cybersecurity Plan that meets the SLCGP requirements as defined in the NOFO.	1.1 Draft the Plan.	Draft Plan exists in Document Library.	CISO confirms Draft Plan is in Document Library.
	1.2 Committee Approves Plan.	Signed Letter by State CIO.	Committee Meeting Minutes.
	1.3 Submit the Plan to CISA.	Confirmation of Receipt.	Email from CISA.
	1.4 CISA Approves Plan.	Statement of Approval.	Email from CISA.
2. Solicit for SLCGP projects.	2.1 Notify eligible entities of availability of funding and application process.	Project submission process is published by the SAA.	Funding announcement is posted online by SAA.
3. Receive project submissions from potential sub-recipients.	3.1 Applicants submit applications to the SAA via eGrants.	Receive applications for projects, conduct initial eligibility reviews.	Eligible applications are prepared for Committee review.
4. Select projects and make sub-awards.	4.1 Committee reviews each project submission and makes funding recommendations to SAA.	Committee documents project selection process.	Meetings at regular intervals during project review period.
	4.2 FEMA/CISA approves projects.	Selected projects are submitted by SAA to FEMA/CISA for approval.	FEMA/CISA approves selected projects and releases fund holds.

Cybersecurity Plan Metrics			
Program Goal	**Program Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
	4.3 SAA releases sub-awards to subrecipients.	SAA collects programmatic and financial reports from sub-recipients.	Programmatic and financial reporting submitted to FEMA by SAA.
5. Review, revise, and update plan for next FY.	5.1 Repeat Objectives for Goal 1 for subsequent FY.	See Goal #1.	See Goal #1.