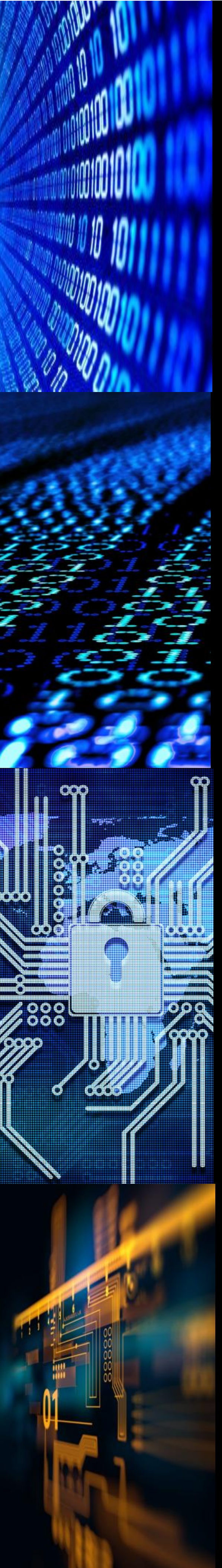


[ENTITY] CYBERSECURITY PLAN

NOTE: This template is provided as an optional tool for eligible entities to use (as needed) to develop their cybersecurity plan. This template includes key requirements of the State and Local Cybersecurity Grant Program. Ultimately, eligible entities are encouraged to develop a plan that reflects their unique situation while meeting program requirements. This includes using existing plans and documents as appropriate.

Replace all grey text, as appropriate, to reflect the eligible entity.

Text highlighted in yellow provides instruction for plan authors and should be deleted before the final draft of the document is complete. *Delete text box before final draft.*

INSERT ENTITY SEAL OR LOGO

MONTH YEAR

Approved by INSERT GOVERNING BODY on INSERT DATE
Version X

[Including this statement regarding the entity's cybersecurity governing body demonstrates that the plan has been approved by an appropriate planning committee]

DRAFT – INTERNAL WORKING DOCUMENT

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM [CYBERSECURITY PLANNING COMMITTEE]

[Including a letter from the eligible entity's Cybersecurity Planning committee chair and the CIO/CISO/CSO or equivalent demonstrates that the plan has been approved by the appropriate officials]

Greetings,

The Cybersecurity Planning committee for [Entity] am pleased to present to you the 202X [Entity] Cybersecurity Plan. The Cybersecurity Plan represents the [Entity's] continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, this update meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the [Entity governing body/represented bodies with the Cybersecurity Planning Committee] collaborated to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on [[Insert plan priorities]. They are designed to support our entity in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

As we continue to enhance cybersecurity, we must remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Sincerely,

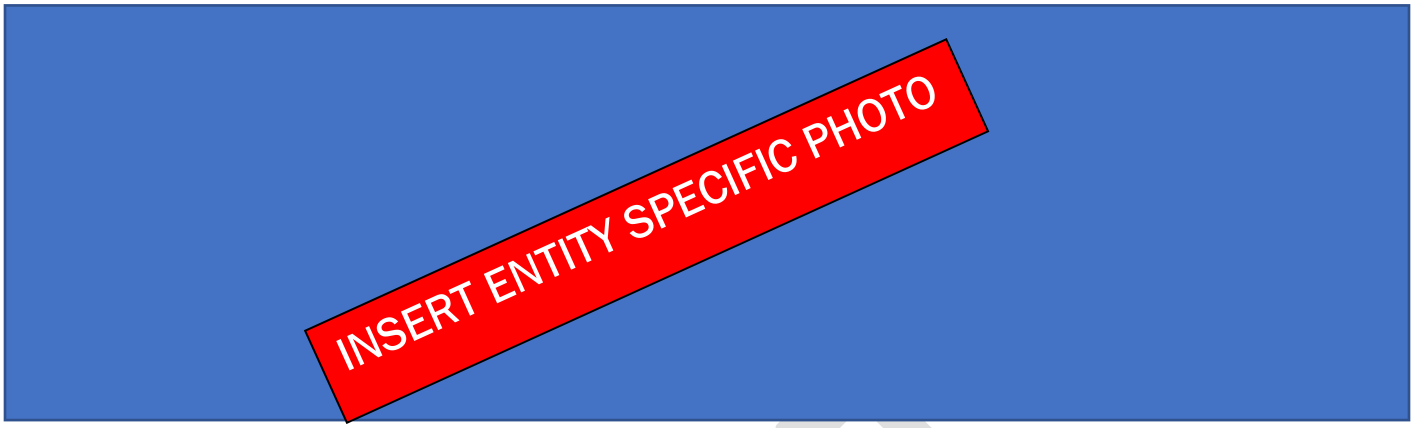
____

[CIO, CISO, CSO NAME]
[ENTITY TITLE]
[DEPARTMENT]

____

[Chair of Cybersecurity Planning Committee]
[ENTITY TITLE]
[DEPARTMENT]

INTRODUCTION



[A Cybersecurity Plan is a key component to helping you build cyber resilience. As applicable, eligible entities should use existing plans, structures, and other relevant efforts to build your comprehensive cybersecurity plan. Building upon existing structures and capabilities allows you to provide governance and a framework to meet your critical cybersecurity needs while making the best use of available resources. For example, consider referencing your emergency management plan to address potential downstream impacts affecting health and safety when responding to or recovering from a cybersecurity incident. For Entities, describe how you will consult, solicit, and incorporate feedback from local governments and association of local governments into your cybersecurity plan.

The Cybersecurity Plan is a [one-to-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 one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any governance mechanisms for cybersecurity within [the entity] as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of [the entities] cybersecurity program. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of [the entity's] or local systems or agencies.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from local governments as used in order to reduce overall cybersecurity risk across the eligible entity. This is especially important in order to develop a holistic cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within [the entity] along with methods and strategies for funding sustainment and enhancement to meet long-term goals.

- **Implementation Plan:** Describes [the entity's] 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 entity] will measure the outputs and outcomes of the program across the entity.

[The following provides an example of how the The National Institute of Standards and Technology (NIST) Cybersecurity Framework can be used. It is not required to adopt the NIST Cybersecurity Framework or any other specific framework, but such frameworks do provide a consistent model to gauge progress over time.] The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

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

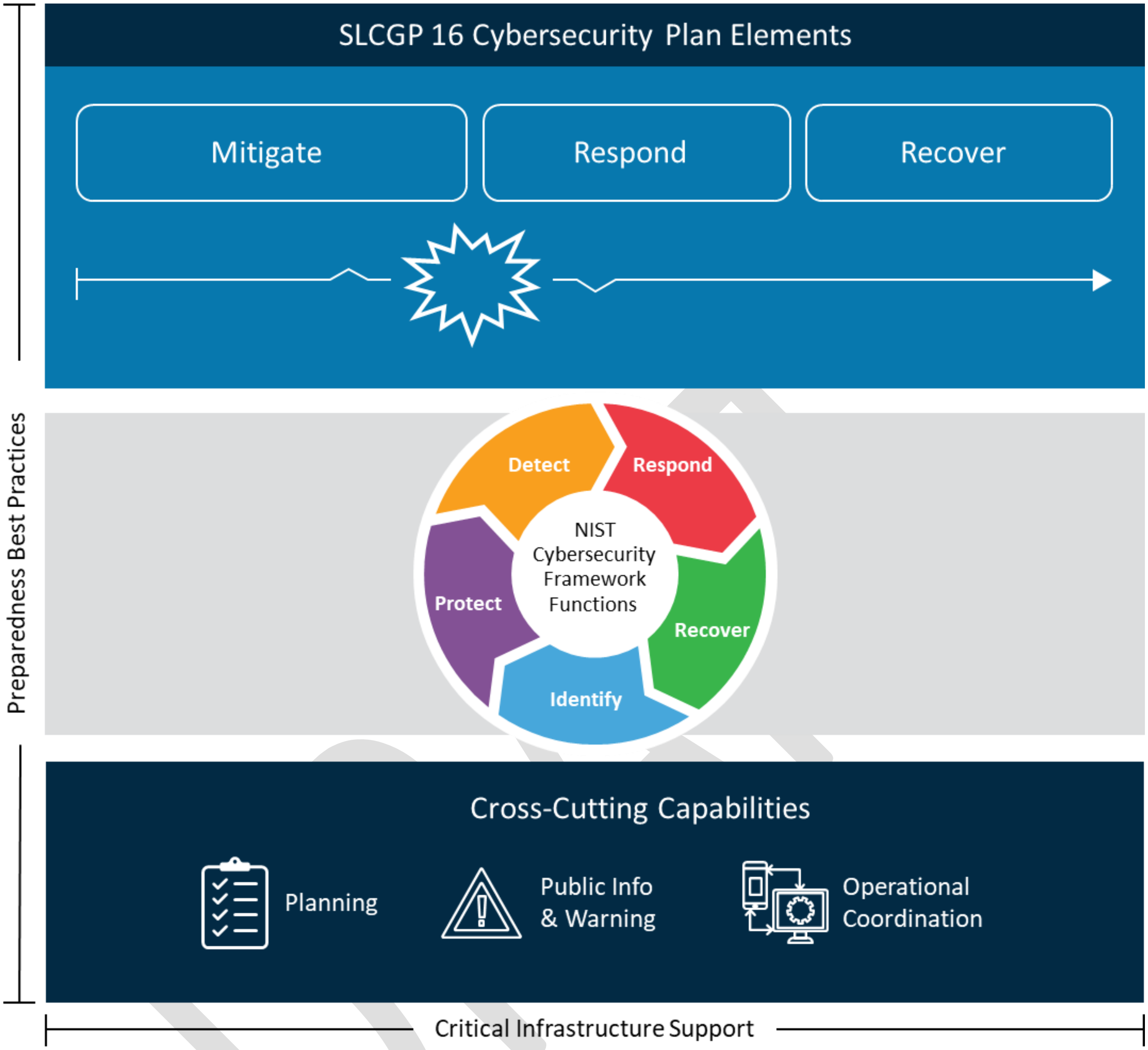

SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

Vision and Mission

This section describes [ENTITY'S] vision and mission for improving cybersecurity:

Vision:

INSERT VISION

Mission:

INSERT MISSION

Cybersecurity Program Goals and Objectives

[The following goals and objectives are different than the SLCGP's goals and objectives. The entity's goals set's the desired and achievable outcome that is typically broad and long-term. Objectives are specific, measurable actions that will be taken to achieve each goal.]

[Entity] Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	Program Objectives
1.	1.1
	1.2
	1.3
2.	2.1
3.	3.1
	3.2
4.	4.1
	4.2
	4.3
5.	5.1

CYBERSECURITY PLAN ELEMENTS

Note: If you have an existing plan that can meet any of the sections below, incorporate by reference. For example: Document Name in Section XXX.XX and describe the way in which the eligible entity meets each of the plan elements.

Delete before final draft.

This plan incorporates the following plans:

- [Insert plan citation and summary of intent]

- [Insert plan citation and summary of intent]
- [Insert plan citation and summary of intent]

Note: The Cybersecurity Plan is intended to be a strategic plan for the entire entity. Descriptions for each of the following required elements should not focus of a single entity. Instead, the focus should be on setting the desire end state and approach for improving SLTT capabilities within each element across the eligible entity. The plan should address the next 2 to 3 years, recognizing that it can be updated s frequently are necessary.

Delete before final draft.

Manage, Monitor, and Track

[Describe the strategic approach to improve the management, monitoring, and tracking of information systems, applications, and user accounts. Activities can include managing, monitoring, and tracking hardware, software, and services (such as software as a service, cloud services, etc.) that you use for day-to-day business.

NOTE: Systems and technology that are no longer supported by the manufacturer are particularly vulnerable to cybersecurity threats. These legacy systems may require additional effort managing, monitoring, and tracking to effectively protect, detect, respond to, and recover from cybersecurity incidents.

Monitor, Audit, and Track

[Describe the strategic approach to improve the monitoring, auditing, and tracking of network traffic and activity. This could include your security / information technology operation centers, partnerships such as CISA services, MS-ISAC and/or vendor network monitoring, auditing, and tracking services or other specific solutions you use.

Enhance Preparedness

[Describe the strategic approach to enhancing the preparation, response, and resiliency of your information systems, applications, and user accounts against cybersecurity risks and threats. This element addresses the need for comprehensive planning – beyond response to include planning, organization, equipment, training, and exercises.

Assessment and Mitigation

[Describe the strategic approach to implementing a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk. These efforts are to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts you own or are operated on your behalf.

Best Practices and Methodologies

[Describe the strategic approach for adopting and using best practices and methodologies to enhance cybersecurity. The following cybersecurity best practices must be included:

- 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).
- Migration to the .gov internet domain.

These are not required to be implemented immediately, but all Cybersecurity Plans must clearly articulate efforts to implement these best practices across the eligible entity within a reasonable timeline. Individual projects that assist SLTT entities adopt these best practices should also be prioritized.

Additional best practices that the Cybersecurity Plan can address include:]

NIST Principles

[… the cybersecurity framework (CSF) developed by the National Institute of Standards and Technology (NIST) (while adopting the NIST CSF is not required - adoption of a recognized framework will significantly improve your ability to meet this requirement)]

Supply Chain Risk Management

[… cyber supply chain risk management (C-SCRM) best practices identified by NIST. This involves identifying, prioritizing, and assessing information technology suppliers, vendors, and service providers to understand the related and/or cascading risks to your (and, as applicable, all your jurisdictions) supply chain]

Tools and Tactics

[… knowledge bases of adversary tools and tactics. This may involve engaging the MS-ISAC, CISA, and other partners and systems to gain access to knowledge bases of adversary tools and tactics to improve your cybersecurity efforts.

Safe Online Services

[Describe the strategic approach that will promote the delivery of safe, recognizable, and trustworthy online services (including using the .gov internet domain).

Continuity of Operations

[Describe the strategic approach to ensure continuity of operations (COOP) in the event of a cyber incident. Include conducting exercises to practice COOP response actions. This may involve referencing, linking to, or incorporating your continuity of operations plans, systems, and personnel in your cybersecurity plan.

Workforce

[Describe the strategic approach to using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in your cybersecurity workforce. This includes enhancing recruitment and retention efforts, as well as bolstering your personnel's knowledge, skills, and abilities to address cybersecurity risks and threats (for example, providing cyber hygiene training for personnel entity wide).

Continuity of Communications and Data Networks

[For Entities, describe how you will ensure continuity of communications and data networks – across jurisdictions in your purview – in the event of an incident involving those communications or data networks.

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

[Describe the strategic approach to the assessment and mitigation, to the greatest degree possible, of cybersecurity risks and threats relating to critical infrastructure and key resources (such as power and telecommunications) that may impact the performance of information systems within your purview.

Cyber Threat Indicator Information Sharing

[Describe the strategic approach to enhancing capabilities to share cyber threat indicators and related information. This may involve leveraging CISA's Cyber Information Sharing and Collaboration Program (CISCP), CISA's Automated Indicator Sharing capability and systems and subscribing to and participating in the MS-ISAC Real-Time Indicator Feeds or other applicable systems and processes to share cyber threat indicators and related information.]

Department Agreements

[Describe how you will share cyber threat indicators and related information with local governments – including by expanding information sharing agreements with CISA.

Leverage CISA Services

[Describe the strategic approach to leveraging cybersecurity services offered by CISA.

Information Technology and Operational Technology Modernization Review

[Describe the strategic approach to your implementation of a modernization review process that ensures alignment between information technology and operational technology cybersecurity objectives.

- Information technology – systems that use, store, retrieve, send, process information, and
- Operational technology – or industrial controls systems, including hardware and software that manages, monitors, and causes physical changes to systems such as water, power, fuels, wastewater, mechanical, industrial, safety, and other systems and process.

Cybersecurity Risk and Threat Strategies

[Describe how the Planning Committee will develop and coordinate strategies to address cybersecurity risks and cybersecurity threats with other organizations, including consultation with local governments and associations of local governments within their jurisdiction, neighboring entities, Territories, and Tribal governments (as applicable), or members of an ISAC; and neighboring countries (this may involve existing international cooperation frameworks, mutual aid, and other agreements with neighboring countries consistent with your authorities and law).]

Rural Communities

[Describe the strategic approach to ensuring rural communities (as described by section 5302 of title 49 of the USC) have adequate access to and are able to participate in cybersecurity services and activities.

FUNDING & SERVICES

[Provide a narrative overview for the program, highlighting key initiatives to strengthen cybersecurity for the eligible entity.]

Distribution to Local Governments

[Describe the strategic approach to the distribution of funds, items, services, capabilities, or activities to local governments, including plans to distribute 25% of cybersecurity grant funding received to rural areas.

Use the table in **Appendix B: Project Summary Worksheet** to list items, services, capabilities, or activities you plan to provide to local governments to implement your cybersecurity plan.

By documenting your entity's approach distribute funds, items, services, capabilities, or activities to local governments (including distribution of 25% of cybersecurity grant funding received to rural areas) demonstrates that the plan meets requirement **in the State and Local Cybersecurity Improvement Act: e.2.B.xvi.**]

ASSESS CAPABILITIES

[In accordance with the State and Local Cybersecurity Improvement Act; Describe the strategic approach implemented to assess capabilities for the preceding requirements (cybersecurity plan elements) outlined above. Information can be captured in **Appendix A: Cybersecurity Plan Capabilities Assessment**.]

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

[Provide an overview of the relationship between the cybersecurity organizations in the entity. Define roles and responsibilities; and if entity is a state, the organizational structure, and identified roles and responsibilities assumed.

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 numerous individuals, groups, or agencies, and may be added as formal agenda items for review during regular governance body meetings.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

[As able, provide an overview of resources needed to implement the plan, as well as the projected timeline to implement the entity's cybersecurity plan.

By documenting, as able, the necessary resources and a projected timeline you demonstrate you're your comprehensive cybersecurity plan meets requirement **in the State and Local Cybersecurity Improvement Act: e.2.E.**]

METRICS

[describe the metrics the eligible entity will use to measure progress towards

- Implementing the Cybersecurity Plan
- Reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.]
- You may use the following table for reporting metrics. Please note: This table requests **PROGRAM OBJECTIVES NOT THE CYBERSECURITY PLAN OBJECTIVES**

Sample Table - Cybersecurity Plan Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1.	1.1		
	1.2		
	1.3		
2.	2.1		
3.	3.1		
	3.2		
4.	4.1		
	4.2		
	4.3		

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

[By taking the following actions, an entity will demonstrate that their cybersecurity plan incorporates the required assessment relating to the **Cybersecurity Plan Required Elements.** Ensure that the assessment incorporates an **entity-wide** perspective**.** It also links any line items from the **project summary worksheet** that will help to establish, strengthen, or further develop your cybersecurity capabilities**.**

Eligible entities can use the "EVAL" column as a self-assessment tool. Entities with newly initiated programs could use this spreadsheet to track the status of their cybersecurity planning efforts. Similarly, entities with advanced programs could use this worksheet to evaluate their current cybersecurity plan using "Yes, No, Partial, or N/A."]

COMPLETED BY [ENTITY]				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				
2. Monitor, audit, and track network traffic and activity				
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts				
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk				
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)				

a. Implement multi-factor authentication				🟥
b. Implement enhanced logging				🟥
c. Data encryption for data at rest and in transit				🟥
d. End use of unsupported/end of life software and hardware that are accessible from the Internet				🟥
e. Prohibit use of known/fixed/default passwords and credentials				🟥
f. Ensure the ability to reconstitute systems (backups)				🟥
g. Migration to the .gov internet domain				🟥
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain				🟥
7. Ensure continuity of operations including by conducting exercises				🟥
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)				🟥
9. Ensure continuity of communications and data networks in the event of an incident involving 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 eligible entity				🟥
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department				🟥
12. Leverage cybersecurity services offered by the Department				🟥
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				🟥
15. Ensure rural communities have adequate access to, and participation in plan activities				🟥
16. Distribute funds, items, services, capabilities, or activities to local governments				🟥

APPENDIX B: PROJECT SUMMARY WORKSHEET

[The project worksheet should mirror all projects applied for in the Individual Justification (IJ) form.]

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.**

[Instructions: Completing the table below, including the following information in each column to expedite review and approval:

- **Column 1.** Project number assigned by the entity
- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Element the project addresses
- Column 5. Estimated project cost
- **Column 6.** Status of project (future, ongoing, complete)
- **Column 7.** Project priority listing (high, medium, low)
- **Column 8.** Project Type (Plan, Organize, Equip, Train, Exercise)]

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type

APPENDIX C: ENTITY METRICS

[Describe the metrics you will use to measure implementation and cybersecurity threat reduction (to be provided in your annual report to CISA), including:

1) progress toward implementing the cybersecurity plan; and
2) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to your information systems.

Consider the following when developing metrics:

- Metrics must be aligned to the Cybersecurity Plan and the established goals and objectives
- Review existing metrics that are already be used across the eligible entity
- The data for each metric must be available and reportable and should not create unnecessary bourdons to collect.

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.	1.1		
	1.2		
	1.3		
2.	2.1		
3.	3.1		
	3.2		
4.	4.1		
	4.2		
	4.3		
5.	5.1		

APPENDIX D: ACRONYMS

Acronym	Definition

UPDATE ALL ACRONYMS IN TABLE