SLCGP Cybersecurity Plan: 16 Required Elements Reference Sheet

From Fiscal Year 2022 State and Local Cybersecurity Grant Program Notice of Funding Opportunity:

- https://www.grants.gov/web/grants/view-opportunity.html?oppId=343579
- **You can find the Notice of Funding Opportunity (NOFO) and CISA's suggested Cybersecurity Plan Template here (go to the "Related Documents" tab)**
- **The 16 required elements are described on pages 68-70 of the NOFO and listed below**

There are 16 required elements that are central to the Cybersecurity Plan and represent a broad range of cybersecurity capabilities and activities. They also include specific cybersecurity best practices that, when implemented over time, will substantially reduce cybersecurity risk and cybersecurity threats. While each of the 16 required elements must be addressed in the plan, this may include a brief explanation as to why certain elements are not currently being prioritized. Not all 16 elements are required to be aligned to projects and have associated funding. These determinations should be addressed in accordance with capability gaps and vulnerabilities identified through an objective assessment process.

Required Elements

If there are any existing plans that meet the required elements, references to them may be used in lieu of incorporating them in their entirety. The Cybersecurity Plan must describe, to the extent practicable, how the state plans to address the below elements. The Cybersecurity Plan is a strategic document, looking broadly across the entire jurisdiction. The description should support the vision, mission and other strategic guidance set by the Cybersecurity Planning Committee.

1. Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2. Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3. Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4. Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address

cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.

5. Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below:
    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); and
    g. Migration to the .gov internet domain.
6. Promote the delivery of safe, recognizable, and trustworthy online services by the state or local governments within the state, including through the use of the .gov internet domain.
7. Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.
8. Use the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity developed by NIST to identify and mitigate any gaps in the cybersecurity workforces of the state or local governments within the state, enhance recruitment and retention efforts for those workforces, and bolster the knowledge, skills, and abilities of personnel of the state or local governments within the state, to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training.
9. Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the state.
11. Enhance capabilities to share cyber threat indicators and related information between the state, local governments within the state, and CISA.
12. Leverage cybersecurity services offered by the Department (See Appendix G for additional information on CISA resources and required services and membership).
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between

information technology and operational technology cybersecurity objectives.

14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats. Local governments and associations of local governments within the state should be consulted. Cybersecurity Planning Committees should also consider consulting neighboring entities, including adjacent states and countries.
15. Ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas within the state.
16. Distribute funds, items, services, capabilities, or activities to local governments.