Guidance Document

Baseline Cybersecurity Best Practices:

An Overview for Success in Applying for the State and Local Cybersecurity Program

ATARC State and Local Cyber Grants Working Group

March 2023

Introduction

The integrity of an organization's information systems and data is essential for its overall success. Cybersecurity threats are becoming increasingly sophisticated, and it is important for organizations to implement strong security measures to protect against them. In this document are common baseline security best practices that organizations should implement to help greater protect their infrastructure. Additionally, we have combined this with an overview and the requirements the Cybersecurity and Infrastructure Security Agency (CISA) considers important when applying for the Infrastructure Investment and Jobs Act (IIJA) State and Local Cybersecurity Grant Program.

Information Security Best Practices

1. **Strong Password Policies:** Implement a strong password policy that requires complex passwords, regular password changes, and require multi-factor authentication.
2. **Regular Security Training:** Conduct regular security training for employees to increase their awareness of cybersecurity threats and how to protect against them.
3. **Patch Management:** Implement a robust patch management program that ensures all software and operating systems are up to date with the latest security patches.
4. **Encryption:** Use encryption for sensitive data at rest and in transit to prevent unauthorized access.
5. **Physical Security**: Implement physical security measures, such as secure access controls, to prevent unauthorized access to sensitive areas and equipment.
6. **Incident Response Plan:** Develop and regularly test an incident response plan to ensure a timely and effective response to security incidents.
7. **Least Privilege:** Limit access to sensitive data and systems to only those who absolutely need it.
8. **Backups:** Regularly back up important data organizational and store backups in a secure, off-line location.
9. **Endpoint Detection and Response:** Install EDR software on endpoint devices, such as laptops, desktops, servers, and mobile devices that detects, investigates, and responds to security incidents.
10. **End of Life / End of Support**: Implement strict policies for removing and disposing of old or unused hardware and devices that have reached their end of life or end of support.

IIJA State and Local Cybersecurity Grant Program (SLCGP) Overview

In September of 2022, the Department of Homeland Security (DHS) announced a first-of-its-kind cybersecurity grant program focusing on enhancing information technology (IT) cybersecurity in critical infrastructure, including transportation, energy, water utilities, and state, local and tribal governments. This unique cybersecurity grant was established through the Infrastructure Investment and Jobs Act (IIJA) of 2021. In the IIJA, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program, appropriating $1 billion to be awarded over four years.

CISA will serve as the subject-matter expert in cybersecurity related issues, and FEMA will provide grant administration and oversight for appropriated funds. States and territories will use their State Administrative Agencies (SAAs) to receive the funds from the Federal Government.

The established SAA for states and territories will be the only entities that can apply for grant awards under the SLCGP. Local entities receive sub-awards through their state's SAA. The legislation requires states to distribute at least 80% of funds to local governments, with a minimum of 25% of the allocated funds distributed to rural areas.

There is a matching requirement for the SLCGP.

- for fiscal year 2022, 10 percent
- for fiscal year 2023, 20 percent
- for fiscal year 2024, 30 percent
- for fiscal year 2025, 40 percent

Cybersecurity Plans submitted by the SAAs to CISA must address how the best practices listed below and the 16 required cybersecurity elements will be implemented across State, Local, Tribal, and Territorial (SLTT) entities. Adoption is not required immediately, nor by all SLTT entities. Instead, the Cybersecurity Plan should detail the implementation approach over time and how the following will be consistent with the program goal and objectives. The Cybersecurity Plan should establish high level goals and finite objectives to reduce specific cybersecurity risks across the eligible entity.

CISA's mentioned best practices:

- Multi-factor authentication;
- 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;
- The ability to reconstitute systems (backups); and
- Migration to the .gov internet domain.

In addition to CISA's mentioned best practices, Cybersecurity planning committees in states, territories, and tribes must explain how they will address 16 cybersecurity elements.

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.
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST).
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 DHS CISA.
12. Leverage cybersecurity services offered by the DHS CISA.
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.

Finally, SLTTs should not use SLCGP grant funds to:

- Supplanting state or local funds;
- Recipient cost-sharing contributions;
- Payment of a ransom from cyberattacks;
- Recreational or social purposes, or for any purpose that does not address cybersecurity risks or cybersecurity threats on SLTT information systems;
- Lobbying or intervention in federal regulatory or adjudicatory proceedings;
- Suing the federal government or any other government entity;
- Acquiring land or constructing, remodeling, or altering buildings or other physical facilities; or
- Cybersecurity Insurance; or
- Any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the eligible entity or a local government within the jurisdiction of the eligible entity.

Implementing strong security measures like information security best practices is essential to protect an organization's information systems and data from ever evolving cyber threats. This also ensures your organization meets the requirements set forth to apply and receive funding from the IIJA State and Local Cybersecurity Grant Program.

Disclaimer: This document was prepared by the members of the ATARC State and Local Cyber Grants Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with, and shall not be used for advertisement or product endorsement purposes.