Alaska Cybersecurity Plan

State and Local Cybersecurity Grant Program

Background

Infrastructure Investments and Jobs Act (IIJA) Public Law 117-58

State and Local Cybersecurity Improvement Act, section 70612 established the State and Local Cybersecurity Grant Program (SLCGP), and appropriated $1 billion to be awarded over four years.

The goal of the SLCGP is to assist state, local, and tribal governments with managing and reducing systemic cyber risk.

"Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense." – President Joe Biden

National Cybersecurity Strategy March 2023

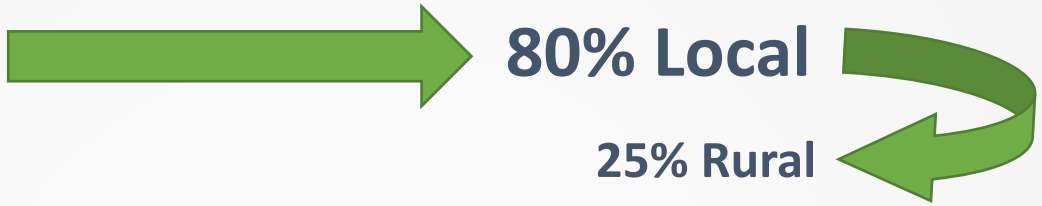
What is SLCGP?

SLCGP is a federal grant program focused on eligible entities to address cybersecurity risk and cybersecurity threats to information systems owned or operated, or on behalf of, State, local, or Tribal governments.

Primarily a pass through grant, requiring 80% of funding to be awarded to local governments.

In addition, 25% of those funds must be passed through to "rural areas"

A rural area is defined in 49 U.S.C. § 5302 as an area encompassing a population of less than 50,000 people that has not been designated in the most recent decennial census as an "urbanized area".



Who is Administering SLCGP?

FEDERAL:

STATE:

Alaska Department of Administration
Office of Information Technology

Office of Information Technology/State CIO

- Leads development of the Statewide Cybersecurity Plan
  - Contracted with CTG, Chad Alessi
- OIT Chief Information Security Officer
- Final approval of Statewide Cybersecurity Plan
  - *Home Rule State
  - Also requires approval of Cybersecurity Planning Committee
- Integration with State of Alaska Executive Branch Cybersecurity Initiatives

State Administrative Agency

- SLCGP Grant Recipient
- Sub-recipient Grant Administrator
- Final Approval of sub-recipient project applications
  - Based on allocation recommendations of the Cybersecurity Planning Committee/Multi-Agency External Review Committee
- Grant Monitoring and Reporting

Cybersecurity Planning Committee

Duties:

- Assist with the development, implementation, and revision of the Cybersecurity Plan
- Approve the Cybersecurity Plan
- Assist with the determination of effective **funding priorities** for a grant under the program.

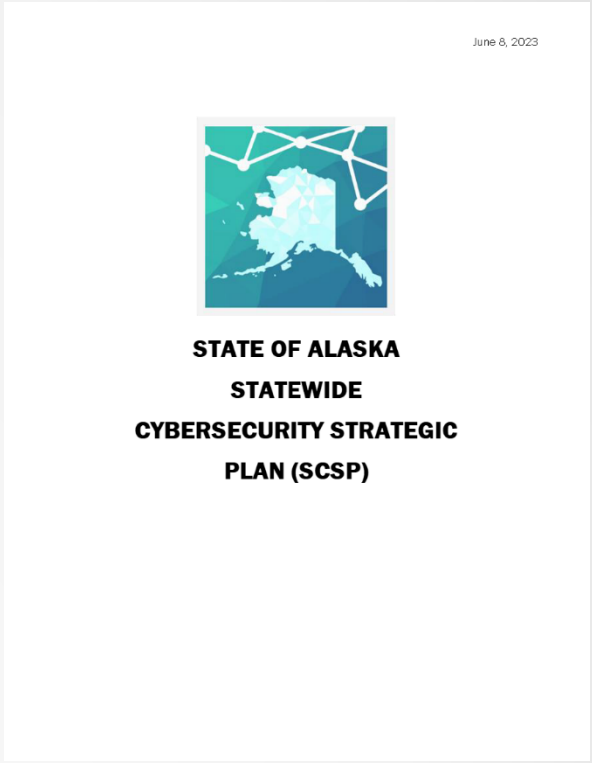
Composition:

- CIO and SAA
- Boroughs, cities, and towns (+Tribal representation)
- Institutions of public education and health
- Rural, suburban, and high-population jurisdictions
- >= 50% of representatives shall have professional experience relating to cybersecurity or information technology

Statewide Cybersecurity Plan

****Statewide Plan, not a State of Alaska executive branch plan****

- Plan approved by FEMA and CISA 8/24/2023
- Comprehensive strategic plan to reduce cybersecurity risk and increase capability across the entity
- Entity-wide plan, not a single entity
- Must include required elements, with discretion to add other elements as necessary
- Must be approved by the Cybersecurity Committee and CIO/CISO/Equivalent
- CISA approves for DHS
- Plans are initially approved for 2 years; annually thereafter



Statewide Cybersecurity Plan
Vision and Mission

Vision:

Create a secure and resilient cybersecurity environment for the State of Alaska, where all state, local, and tribal governments work together seamlessly to protect against cybersecurity risks and threats to information systems owned or operated by, or on behalf of, our public sector agencies, and in the public interest.

Statewide Cybersecurity Plan Vision and Mission

Mission:

Develop and implement a comprehensive cybersecurity plan for the State of Alaska that incorporates existing plans and feedback from local governments, promotes the adoption of best practices and methodologies, and ensures the continuity of operations in the event of a cybersecurity incident. The outcomes from this planning effort and implementation will include: assessment of the capabilities of the eligible entity relating to the actions described in the plan and identify and mitigate any gaps in the cybersecurity workforce, enhancement of the delivery of safe and trustworthy online services and work to establish strong partnerships to improve information sharing and collaboration. , and collaboratively striving to achieve measurable progress towards reducing cybersecurity risks and identifying, responding to, and recovering from

Goals/Objectives

1. **Enhance Cybersecurity Resilience and Interoperability**
    1. Support and encourage cybersecurity risk assessment
    2. Support and encourage the implementation of a continuous monitoring program
2. **Foster a Cybersecurity Culture**
    1. Development and delivery of cybersecurity awareness and training programs
    2. Establishment of a cybersecurity awareness program to educate citizens
3. **Enhance Cybersecurity Collaboration and Partnerships**
    1. Develop and implement cybersecurity information sharing program
    2. Foster partnerships with the private sector, academic institutions, and non-profits
4. **Improve Cybersecurity Incident Management and Response Capabilities**
    1. Establish cybersecurity incident response team
    2. Development and implementation if a cybersecurity incident management plan

Best Practices

- 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)
- Migrate to the .gov internet domain
- Implement network boundary filtering capabilities where practicable (e.g., DNS, URL, email)
- Implement cybersecurity awareness training program
- Implement authentication and privileged account access
- Implement Patch Management Solution

Alaska Cybersecurity Plan

State and Local Cybersecurity Grant Program

Contact Information:

Bill Smith – bill.smith@alaska.gov
Leonard Robertson – leonard.robertson@alaska.gov
Bryan Fisher – b.fisher@alaska.gov