STATE AND LOCAL CYBERSECURITY GRANT PROGRAM
Agenda

- Introduction: CISA/FEMA Roles/Responsibilities
- Update: Summary of the State and Local Cybersecurity Grant Program
Roles and Responsibilities

- **CISA – Program Management and Subject Matter Expertise**
  - Identify the goals/objectives that define the overarching outcomes for the program;
  - Review and approve cybersecurity plans and projects; and
  - Establish measures of effectiveness that demonstrate achievement of goals/objectives.

- **FEMA – Grants Administration Subject Matter Expertise**
  - Conduct eligibility reviews, issue and programmatically/financially manage grant awards consistent with all applicable laws, regulations, and policies;
  - Place any special award terms and conditions, in coordination with CISA;
  - Monitor and document recipient progress, in coordination with CISA; and
  - Utilize existing grants and financial management systems for State and Local Cybersecurity Grant Program (SLCGP) awards.
Summary of State and Local Cybersecurity Grant Program

- Infrastructure Investment and Jobs Act (IIJA) amended Homeland Security Act of 2022 and appropriated $1B over 4 years
  - Funds appropriated to FEMA; CISA identified as subject matter expert
  - Baseline allocation plus population-based allocation formula
  - 80% passthrough to local entities
  - 25% of total state allocation must go to rural communities
  - Increasing SLTT cost share over time
- Eligible entities—States, territories, and tribes, with subawards made to local entities
- Multi-entity grants can be made to groups of eligible entities
- Defined uses of funds
  - Develop and revise Cybersecurity Plan
  - Implement Cybersecurity Plan (including individual projects)
  - Grant administration (5%)
  - Address imminent cybersecurity threats, as confirmed by the Secretary, acting through the Director of CISA
  - Fund any other appropriate activity determined by the Secretary, acting through the Director of CISA

<table>
<thead>
<tr>
<th>Appropriated Funding</th>
<th>Federal Cost Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY22: $200M</td>
<td>FY22: 90%</td>
</tr>
<tr>
<td>FY23: $400M</td>
<td>FY23: 80%</td>
</tr>
<tr>
<td>FY24: $300M</td>
<td>FY24: 70%</td>
</tr>
<tr>
<td>FY25: $100M</td>
<td>FY25: 60%</td>
</tr>
</tbody>
</table>
## State and Local Cybersecurity Grant Program Requirements

### Roles
- Develop, implement, and revise Cybersecurity Plans
- Approve Cybersecurity Plans
- Assist with determination of effective funding priorities (i.e., individual projects)

### Required membership
- Eligible entity
- Local/counties (if eligible entity is a state)
- Representatives from varying densities
- Public education
- Public health
- 50% of members must have professional experience relating to cybersecurity or information technology

### Mandates Cybersecurity Plan submission, approved by planning committee and state Chief Information Officer (CIO)
- 16 cyber-specific elements, including list of projects for SLCGP funding
- Description of SLTT roles in overarching plan
- Assessment of capabilities (16 elements)
- Resources and timeline for implementing plan
- Metrics
Strategic Approach Leverages Feedback Loops

**Inputs**
- Statutory Requirements
- E.O. 14028
- SLTT Engagements

**CISA & FEMA Grant Program Management**
- GOAL & OBJECTIVES, BEST PRACTICES, POLICY GUIDANCE, & EVALUATION PLANNING
- ANNUAL NOTICE OF FUNDING OPPORTUNITY
- REVIEW PLAN & PRIORITY INVESTMENTS
- TRACK & REPORT RESULTS, & EVALUATION

**SLTT Grant Applicants**
- PLANNING COMMITTEE
- CYBERSECURITY PLAN
- IMPLEMENT PLAN & PROJECTS

---

July 28, 2022
Grant Program Goal & Objectives

**GOAL:** Assist SLTT governments with managing and reducing systemic cyber risk.

**Objective 1 - Governance & Planning**
- Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- Establish cybersecurity governance structures and implement a program to evaluate maturity of the cybersecurity program aligned to Cybersecurity Performance Goals established by CISA and National Institute of Standards and Technology (NIST).
- Implement and test cybersecurity response plans with clearly defined roles and responsibilities.
- Asset (e.g., devices, data, software) protections and recovery actions are prioritized based on the asset’s criticality and business value.

**Objective 2 - Assessment & Evaluation**
- SLTT governments understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- Physical devices and systems, as well software platforms and applications, are inventoried.
- Cybersecurity risk to the organization’s operations and assets are understood.
- Vulnerability scans are performed, and a risk-based vulnerability management plan is developed and implemented.
- Capabilities are in place to monitor assets to identify cybersecurity events.
- Processes are in place to action insights derived from deployed capabilities.

**Objective 3 - Mitigation**
- Implement security protections commensurate with risk (outcomes of Objectives 1 & 2)
- SLTT agencies adopt fundamental cybersecurity best practices.
- Reduce gaps identified through assessment and planning process and apply increasingly sophisticated security protections commensurate with risk.

**Objective 4 - Workforce Development**
- Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.
Requirements and Policies

- Proposed Notice of Funding Opportunity (NOFO) Requirements
  - Existing State Administrative Agency will serve as state-level applicant
  - Strongly encourages CIO, Chief Information Security Officer (CISO), or an equivalent official be on planning committee
  - Specific best practices that must be in Cybersecurity Plan and projects

- Policy Areas of Emphasis
  - Holistic approach to the Cybersecurity Plan
  - Focused investments, sustainable over time
  - Strong planning committees
  - State role as leader and service provider
Recipients may be required to include adoption of specific cybersecurity best practices in their Cybersecurity Plans.

Individual projects support implementation over time, as appropriate:

- 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.
Required Services

- All SLCGP grant recipients and sub-recipients will be required to participate in a limited number of free services and memberships sponsored by CISA. Participation in these services and memberships are not required for submission and approval of a grant.

- Memberships in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) are highly recommended but not required.

- NOFO will include descriptions and instructions.

- CISA will prioritize service delivery for awardee/sub-awardee applications.