INDUSTRY NAVIGATOR

State & Local Cybersecurity Grant Program

FUNDING OPPORTUNITY OVERVIEW

WHAT IT IS:

The $1 billion State and Local Cybersecurity Grant Program (SLCGP)

WHAT IT IS FOR:

The program was established by the Infrastructure Investment and Jobs Act (IIJA) to award grants to states, localities and tribal governments to address cybersecurity risks and cybersecurity threats to their information systems.

Funding total:
$185 million for FY 2022

Funding has also been authorized for:
FY 2023: $400 million
FY 2024: $300 million
FY 2025: $100 million

Eligible entities:
The States Administrative Agency (SAA) for states and territories are the only eligible applicants. In addition, two or more eligible entities may apply jointly for assistance as a multi-entity group.

Funding flows:
Each state received a base level of funding, including additional funds based on a combination of total population and rural population. Allocations are available here.

Once states receive their funds, they must deliver:
- 80% of the funds to local governments
  - at least 25% of that must be made available under a grant passed through local, rural communities
- Delivery needs to happen within 45 days of receipt of funds

Note: There is a cost sharing component for all eligible entities: 10% cost share for a single applicant. *There is an economic hardship provision.*

Deadline for $185 million (FY 2022) grant:
Nov. 15, 2022, at 5 pm ET
They anticipate awarding these funds by Dec. 31, 2022.

What the funds can be used for:
- Developing, implementing and revising the cyber plan
- Administration of the grant including training, hiring and the purchase of equipment
- Maintenance contracts or agreements
- Warranty coverage
- Licenses and user fees in support of a system or equipment

What states need to do:
- Establish a cybersecurity planning committee
- Develop a 2-3-year statewide cybersecurity plan
  - Not a requirement of the FY 2022 application but must be submitted for DHS review and approval by Sept. 30, 2023.
- The cybersecurity plan must discuss seven best practices:
  1. Multi-factor authentication
  2. Enhanced logging
  3. Data encryption for data at rest and in transit
  4. End use of unsupported/end of life software and hardware that are accessible from the Internet
  5. Prohibit use of known/fixed/default passwords and credentials
  6. The ability to reconstitute systems (backups)
  7. Migration to the .gov internet domain

CISA requirements
As a condition of receiving SLCGP funding, the grant recipient is required to sign up for a variety of CISA services, cyber hygiene services and the nationwide cybersecurity review (NCSR).
The first report will be due Jan. 30, 2023.

NEXT STEPS:

1. **Work with local agencies** to help them identify and prioritize their cyber gaps so they can align to the 16 applicable areas in the funding announcement and the 7 best practice areas for funding.
2. **Identify stakeholders** on the cybersecurity committee.
3. **Look for regional opportunities** to connect the dots – multi-jurisdictional approaches will be encouraged.
4. **Track updated guidance.** Industry Navigator will help you track the funds and latest news.

DEEPER DIVE LINKS:

Funding Announcement

Fact Sheet

State Allocations

FAQ