

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM OVERVIEW: IJJA

I. BACKGROUND

As part of the \$1.2 trillion Infrastructure Investment and Jobs Act signed into law on November 6, 2021 (Public Law No. 117-58), the State and Local Cybersecurity Improvement Act authorizes a new Department of Homeland Security (DHS) grant program to address cybersecurity risks and threats to information systems owned and operated by, or on behalf of state, local or tribal governments.

The National Association of State Chief Information Officers (NASCIO) released the following statement on the passage of the Infrastructure Investment and Jobs Act: “Dedicated cybersecurity funding for state and local governments, with an emphasis of increased collaboration between state and local governments with our federal counterparts, has been a long standing priority of our association. The creation of this grant program is a significant step toward improving the cyber resilience for state and local governments across the county. The state CIOs and CISOs look forward to playing an important role in the implementation of this program.”¹

II. AWARD DETAILS

An eligible entity under this grant is defined as a state or tribal government. This program is appropriated:

- For federal fiscal year 2022, \$200,000,000
- For federal fiscal year 2023, \$400,000,000
- For federal fiscal year 2024, \$300,000,000
- For federal fiscal year 2025, \$100,000,000

The match requirement for eligible entities will increase annually. In the case of a grant to a single entity/multi-entities:

- For federal fiscal year 2022, 10 percent/0 percent
- For federal fiscal year 2023, 20 percent/10 percent
- For federal fiscal year 2024, 30 percent/20 percent
- For federal fiscal year 2025, 40 percent/30 percent

Not less than 80% of the funds available under this grant shall be made available to local governments within the jurisdiction of the eligible entity.

¹ NASCIO Statement on Passage of Infrastructure Investment and Jobs Act, November 8, 2021

III. **TIMELINE**

The State and Local Cybersecurity Grant Notice of Funding Opportunity (NOFO) is reportedly going to be released within the first quarter of 2022. At this time, the Federal Emergency Management Agency, Grants Preparedness Division did not have any further information on projected grant timelines.

With other federal preparedness grant, like the FFY 2021 Homeland Security Grant Program, states are normally given 12 weeks to complete the application. The anticipated award date will be prior to August 31, 2022 since federal grant performance period aligns with the beginning of the federal fiscal year.

The authorization for this grant expires on September 30, 2025.

IV. **USE OF FUNDS**

An eligible entity that receives funding under this grant and a local government that receives funds from a grant shall use to the grant to:

1. Implement the Cybersecurity Plan of the eligible entity.
2. Develop or revise the Cybersecurity Plan of the eligible entity.
3. Pay for expenses directly related to administration of the grant, but not to exceed 5% of the amount of the grant.
4. Assist with approved activities that address imminent cyber threats.
5. Fund any other activity approved by the DHS Secretary.

V. **STATE FINANCIAL CONSIDERATIONS**

The state match requirement discussed in Section II, Award Details, requires the Commonwealth of Pennsylvania to commit to, at minimum, meeting the state match requirement for the first year of the four-year grant program.

On-going sustainment of this grant program following September 30, 2025 may fall to the state with the majority of those funds going to local governments.

V. **FEDERAL STATUTORY REQUIREMENTS**

A. **CYBERSECURITY PLANNING COMMITTEE**

An eligible entity applying for this grant must establish a Cybersecurity Planning Committee to assist the determination of state and local government cybersecurity funding priorities, and participate in the development, finalization and approval of the Cybersecurity Plan. finalized.

A Cybersecurity Planning Committee must be comprised of representatives from the state government, local governments and public education and health institutions. The

committee must include representatives of rural, suburban and high population jurisdictions. Not less than one-half the representatives of the committee must have professional experience related to cybersecurity or information technology.

B. CYBERSECURITY PLAN

Before an eligible entity may receive funding under this grant, the grantee must submit for federal approval a Cybersecurity Plan which *to the extent practical* includes but is not limited to the following requirements:

1. Enhance state and local government capabilities to identify and mitigate network cybersecurity vulnerabilities.
2. Provide for consistent monitoring and tracking of network traffic to identify cyber threats.
3. Implement processes to provide for continuous cybersecurity vulnerability assessments and threat mitigation practices to include information and operational technology systems.
4. Promote the delivery of safe, recognizable and trustworthy on-line services to include local government adoption of the .gov internet domain.
5. Promote continuity of operations of state and local government information systems in case of a cyber incident.
6. Enhance state and local cybersecurity information sharing capabilities.
7. Develop and coordinate strategies to address cybersecurity risks and threats.

Prior to submission, the Cybersecurity Plan must be approved by the Cybersecurity Planning Committee and the State Chief Information Officer, Chief Information Security Officer, or an equivalent state officer.

VI GRANT PREPAREDNESS ACTION PLAN

Following the publication of Public Law No. 117-58, the Governor's Office of Homeland Security set-up a meeting with representatives of the Office of Administration/Enterprise Information Security Office (OA/EISO), Pennsylvania Emergency Management (PEMA) and Pennsylvania State Police (PSP) to discuss the State and Local Cybersecurity Improvement Act.

The following provisions of this action plan were agreed as necessary steps to further prepare the Commonwealth of Pennsylvania for the anticipated release of the Notice of Funding Opportunity for State and Local Cybersecurity Grant Program:

- A. Establish a Cybersecurity Planning Steering Committee comprised of the following state representatives, and local government associations:
 - a. Office of Administration/Enterprise Information Security Office
 - b. Governor's Office of Homeland Security
 - c. Pennsylvania Emergency Management Agency
 - d. Pennsylvania State Police
 - e. *Future Add-ons*: County Commissioners Association of Pennsylvania (CCAP)
 - f. *To be Discussed*: PA Association of Intermediate Units (PAIU)

- B. PEMA will brief the Governor's Office on the provisions of this federal grant program and secure approval to implement the action plan.
- C. PEMA will secure authorization to serve as the State Administrative Agency for the grant program.
- D. With the Governor's approval, PEMA will discuss state match requirements with the Office of the Budget (OB). OB's approval will be on a year-to-year basis.
- E. Upon receipt of a state funding commitment, the OA/EISO will reach out to CCAP and request their support and assistance to help establish the local government components of the Cybersecurity Planning Committee.
- F. PEMA will invite local government representatives, to include representatives of the Regional Counterterrorism Task Forces and representatives from Philadelphia and Pittsburgh, to join the Cybersecurity Planning Committee.
- G. PEMA will schedule an initial Cybersecurity Planning Committee meeting to discuss the State and Local Government Grant Program and local government cybersecurity priorities and needs.
- H. Gathering information from the planning meeting, the Cybersecurity Planning Steering Committee will identify strategic drivers to guide the further development and approval of the Cybersecurity Plan.
- I. Upon receipt of the Notice of Funding Opportunity for State and Local Cybersecurity Grant Program, PEMA will work with the Cybersecurity Planning Steering Committee to complete the draft state application for the grant. Prior to federal submission, the state application will be provided to Cybersecurity Planning Committee for review and approval.

Prepared by the Governor's Office of Homeland Security