Published on *The National Law Review* https://natlawreview.com

Cybersecurity Resiliency Funding for U.S. States and Territories

Article By:

C. Bradford Ellison

The Department of Homeland Security has announced a Notice of Funding Opportunity ("NOFO") for the fiscal year ("FY") 2023 State and Local Cybersecurity Grant Program ("SLCGP"). This program makes approximately $374.9 million available in funding available to help state, local and territorial governments manage and reduce systemic cyber risks through focused investments.

Background

Following the widespread cyberattack on SolarWinds' Orion software, lawmakers have increasingly looked to make the private sector more responsible for fortifying the United States' cybersecurity resiliency. The National Cybersecurity Strategy, issued by the Biden administration in March 2023, specifically called for a "fundamental shift" from relying on individuals and small organizations, including "state and local governments," to ensure national cybersecurity. Adding to this sense of responsibility on the private sector, Senator Ron Wyden (D-OR), Chair of the Senate Committee on Finance, more recently urged the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Justice, and Federal Trade Commission "to hold Microsoft responsible for its [allegedly] negligent cybersecurity practices, which enabled a successful Chinese espionage campaign against the United States government."

Still, lawmakers recognize the integral role state, local, and territorial governments play in achieving the National Cybersecurity Strategy's goals – particularly to defend critical infrastructure, disrupt and dismantle threat actors, and invest in a resilient future. In the leadup to the *Infrastructure Investment and Jobs Act's* ("IIJA") passage in November 2021, House and Senate committees in the 117th Congress held several hearings highlighting the crippling effect of ransomware attacks across the country. For reference, the U.K. based research firm Comparitech, which monitors ransomware attacks globally, estimates from 2018 to October 2022 there were over 300 ransomware attacks on state, local and territorial government agencies, potentially impacting over 230 million individuals' data and over $70 billion in costs.

The SLCGP was established under Section 2218 of the IIJA to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or territorial governments. Congress's first interest in establishing the SLCGP was to ensure each U.S. state and territory has a "Cybersecurity Plan" that CISA determines effectively meets 16

elements[1] outlined in IIJA Section 2218(e)(2). Governments have been directed to establish a cybersecurity planning committee, develop a state-wide Cybersecurity Plan, or implement or revise an existing Cybersecurity Plan.

FY 2023 SLCGP Overview

The FY 2023 SLCGP makes $374,981,324 available for cybersecurity planning and exercising, hiring cyber personnel, and improving critical cyber infrastructure. On the program's launch, DHS Secretary Alejandro Mayorkas emphasized "any locality is vulnerable to a devastating cyberattack targeted at a hospital, school, water, or other system" by malign actors.

Who is Eligible and What is Available?

All 56 U.S. states and territories are eligible to apply for FY 2023 SLCGP funds. States and territories may collaborate to form multi-entity projects under the program. A base allowance of $4,082,282 (1 percent of the funds appropriated to DHS for FY 2023) is allocated for each U.S. state, Puerto Rico, and the District of Columbia ("D.C."). A base allowance of $1,020,570 (0.25 percent of the funds apportioned to DHS for FY 2023) is allocated for each of the other four territories—American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands. Additionally, the program requires states—here excluding D.C. and the five territories—to pass through a total dollar value of at least 25% of the federal funds provided under the grant to rural areas, meaning "any area with a population of less than 50,000 individuals."

Overview of the Application Process

Only state and local government entities' governor-designated SLCGP State Administrative Agency (SAA) may submit the SLCGP application. Applicants must submit a Cybersecurity Plan, Cybersecurity Planning Committee Membership List, and a Cybersecurity Charter that align with the NOFO's priorities along with an FY 2023 SLCGP application if they did not participate in the FY 2022 SLCGP. The CISA must approve an applicant's Cybersecurity Plan before DHS will release funds to the applicant.

FY 2023 SLCGP applications are required to address the following program objectives:

- Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments;
- Implement security protections commensurate with risks; and,
- Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

Applicants are encouraged to begin preparing their submissions as soon as possible. DHS notes the application process can take up to four weeks, so it is essential organizations apply for or update their Unique Entity Identifier (UEI) number from SAM.gov and Employer Identification Number (EIN) from the Internal Revenue Service in advance.

Initial applications will be processed via grants.gov. Final applications must be completed and submitted through the Federal Emergency Management Agency (FEMA) ND Grants System. FEMA encourages applicants to submit their initial applications at least one week before they submit their final application. Review the NOFO here for additional directions.

The NOFO's period of performance is 48 months, However, SLCGP recipients may formally request to extend this period of performance in writing to their assigned FEMA Preparedness Officer. These requests must contain justifications explaining why the extension is necessary.

What's Next

The SLCGP application deadline is October 6, 2023, at 5:00 p.m. ET. DHS plans to grant awards by December 1, 2023.

DHS notes that "for FY 2024, states and territories can anticipate additional guidance to update their Cybersecurity Planning Committees and Cybersecurity Plans," which reflects the expectation that these plans are agile (i.e. capable of adapting swiftly to new learnings and changing risks). State and local governments should be mindful that the non-federal cost share percentage is expected to increase in FY 2024 and 2025 to 30% and 40%, respectively.

Dominic Braithwaite also contributed to this article.

National Law Review, Volume XIII, Number 241