REPORT REQUIREMENT

The Virginia IT Agency (VITA) submits this report pursuant to Item 93(F)(2) of the 2022 Appropriation Act, which concerns the State and Local Cybersecurity Grant Program and provides that VITA shall "report on the program's activities to the House Appropriations Committee and the Senate Finance and Appropriations Committee by October 1 of each year of the program."

CYBERSECURITY GRANT PROGRAM

Background and Purpose

The Infrastructure Investment and Jobs Act (IIJA) of 2021 (see section 70612) established the State and Local Cybersecurity Grant Program. The Program recognizes the threat that ransomware and other cybersecurity risks pose to state and local governments, which are often strapped for resources to address them. The Program appropriates approximately $1 billion over four years to help address cybersecurity risks and threats.

The Program has four overarching goals and objectives:

(1) develop and establish appropriate governance structures, as well as develop, implement, or revise cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations;
(2) ensure state and local governments understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments;
(3) implement security protections commensurate with risk (outcomes of Objectives 1 & 2); and
(4) ensure personnel are appropriately trained in cybersecurity, commensurate with their responsibilities.

The Program is designed to direct funding primarily to local entities, while encouraging a coordinated approach by requiring that states apply for and coordinate the grants. States will do that pursuant to a cybersecurity plan and priorities that are established at the state level and approved by an intergovernmental cybersecurity planning committee established according to state laws and procedures. The Program allocates 80% of the grant funds to local government, as subrecipients to grants applied for and administered by states. The Program specifically recognizes the challenges faced by rural jurisdictions, allocating 25% of funds to rural areas. No more than 5% of the funds may be used to cover administrative expenses related to the Program.

Involved Agencies and Stakeholders

On the federal side, the Program will be administered through the Federal Emergency Management Agency (FEMA), which will work together with the Cybersecurity & Infrastructure Security Agency (CISA) as the subject-matter expert in cybersecurity related issues.

At the state level, if a state does not already have an existing body, the state must form a Cybersecurity Planning Committee. The Committee will identify and prioritize efforts pursuant to a statewide cybersecurity plan. Membership of the Committee is left to each state, subject to certain requirements:

- The state chief information officer (CIO), or chief information security officer (CISO) as the CIO's designee, chairs the Committee.
- The Committee must include representatives from the state; counties, cities and towns; public education; public health; and rural, suburban, and high-population jurisdictions.
- At least half of the Committee members must have professional experience relating to cybersecurity or information technology.

The federal government encourages states to include members in the Cybersecurity Planning Committee from other governmental stakeholder communities, including judicial and legislative branches and elections administration.

States apply for and administer grants through their designated State Administrative Agencies (SAAs), which in Virginia is the Virginia Department of Emergency Management (VDEM).

The CIO of the Commonwealth, Robert Osmond, is VITA's agency head, and CISO Michael Watson will be his designee for purposes of the Cybersecurity Planning Committee.

Members of the Cybersecurity Planning Committee will be appointed by Governor Youngkin, pursuant to Item 93(F) of the 2022 Appropriation Act.

The Cybersecurity Plan

The Cybersecurity Planning Committee's duties include approving (along with the CIO/CISO) the Cybersecurity Plan, a statewide strategic planning document that must:

- Incorporate, to the extent practicable, any existing plans to protect against cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments.
- State how input and feedback from local governments and associations of local governments was incorporated;

- Include the 16 required elements (from Appendix C of the Notice of Funding Opportunity);
- Describe, to the extent practicable, the individual responsibilities of the state and local governments within the state in implementing the Cybersecurity Plan;
- Assess each of the required elements from an entity-wide perspective;
- Outline, to the extent practicable, the necessary resources and a timeline for implementing the plan;
- Summarize associated projects; and
- Identify metrics that the eligible entity will use to measure progress.

The Program encourages a holistic approach, with a plan that is statewide and spans two years (to start). The Program seeks to encourage focused investments that are sustainable over time, taking advantage of areas in which the state can be a leader and service provider and building on existing efforts.

CISA has stated that it will be looking for certain cybersecurity best practices in the Cybersecurity Plan, including multi-factor authentication, enhanced logging, data encryption at rest and in transit, cessation of use of unsupported and end of life software and hardware that is accessible from the Internet, prohibition of default and fixed passwords and credentials, backups that ensure the ability to reconstitute systems, and migration to the .gov domain.

Recent Information and Timeline Ahead

The federal government did not release many Program details until September 16, when it posted the 2022 Notice of Funding Opportunity on grants.gov, along with explanatory information on CISA's website at https://www.cisa.gov/cybergrants.

Each year there will be a new Notice of Funding Opportunity and application. Applications pursuant to the 2022 Notice are due November 15, 2022. Awards are then anticipated no later than December 31, 2022.

Grant applications should include a completed Cybersecurity Plan, capabilities assessment and individual projects approved by the Cybersecurity Planning Committee and CIO/CISO. States who are not able to complete a plan in time may still apply and receive a grant, after which they will need to complete their plan in year one before any funds are released. CISA and FEMA will review each submission, and CISA will approve final cybersecurity plans and projects.

Virginia's Efforts to Date

The release of the Notice of Funding Opportunity and program details two weeks before the due date of this report necessarily means that the necessary work is incomplete. The

Commonwealth has been preparing and is moving forward to complete the necessary work expeditiously.

During the 2022 General Assembly Session, the administration of Governor Glenn Youngkin and legislative leaders recognized the importance of cybersecurity and the promise of the State and Local Cybersecurity Grant Program. Virginia's 2022 Appropriation Act (Item 93(F)) appropriates the necessary state matching funds that are expected to be needed during the four-year duration of the Program. Virginia is expected to receive over $21 million over the course of the four-year Program, and the General Assembly appropriated in the current state fiscal year $5 million to cover all necessary matching funds.[1]

The budget language in Item 93(F) also charges VITA with taking the necessary action to receive funds and take advantage of the Program. Accordingly, VITA efforts are proceeding in three directions:

- Working with stakeholders on the cybersecurity plan.
- Facilitating appointments by Governor Youngkin's administration of members to the Cybersecurity Planning Committee.
- Coordinating with our partner agency, VDEM, on the administrative steps and arrangements that will be needed.

CONCLUSION

VITA appreciates the support for this important cybersecurity grant program from the General Assembly, Governor Youngkin, and state and local stakeholders. VITA looks forward to improving the cybersecurity of the Commonwealth in partnership with state and local stakeholders.

[1] States receive funding based on a base funding level, as well as their state population and rural population totals. States are required to provide a percentage of matching funds that begins at 10% in the first year and rises incrementally to 40% in the final year of the program.