VIRGINIA IT AGENCY

Cybersecurity Grant Program Report

Virginia Information Technologies Agency

vita.virginia.gov

October 2023

THIS REPORT

The Virginia Information Technologies Agency (VITA) submits this report pursuant to Item 93(F)(2) of the 2023 Appropriation Act, as amended, which concerns the State and Local Cybersecurity Grant Program (SLCGP) 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." This report covers November 2022 – September 2023.

BACKGROUND AND PURPOSE

Recognizing the threat that ransomware and other cybersecurity risks pose to state and local governments, which are often strapped for resources to address them, the Infrastructure Investment and Jobs Act (IIJA) of 2021 (*see* § 70612) established the State and Local Cybersecurity Grant Program. 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 governments, as subrecipients to grants applied for and administered by states. The Program specifically recognizes the challenges faced by rural jurisdictions, allocating 25% of funds of the 80% to rural areas. No more than 5% of the funds may be used to cover administrative expenses related to the Program.

The General Assembly and Governor Youngkin acted quickly to support the Program, enacting Item 93(F) in the 2022 Appropriation Act, including the requisite matching funds.

PARTICIPATING ORGANIZATIONS AND STAKEHOLDERS

Federal administration of the Program involves collaboration between the Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA), with CISA serving as the subject-matter expert in cybersecurity matters.

On the state level, the interagency partnership is similar: VITA has subject matter expertise and works closely with the Virginia Department of Emergency Management (VDEM), which is the State Administrative Agency (SAA) for federal grants.

REPORT

VIRGINIA CYBERSECURITY PLANNING COMMITTEE (VCPC)

The VCPC was formed to manage and further the objectives of the SLCGP, in accordance with its Charter, Bylaws, and Electronic Participation Policy, all of which were adopted at its initial meeting and are available on VITA's website. Its responsibilities include aiding in the creation, execution, and revision of the Commonwealth's cybersecurity plan, as well as approving the plan. It also assists in determining funding priorities, collaborating with stakeholders to enhance coordination, and establishing a unified network to implement cybersecurity initiatives.

Members of the Virginia Cybersecurity Planning Committee were appointed by Governor Youngkin in November 2022.

Under both federal and state law, at least half of the members must possess professional expertise in cybersecurity or information technology, and the VCPC exceeds that minimum. The VCPC includes representation from each of the following: the Chief Information Security Officer (CISO), who chairs the committee; Virginia Department of Emergency Management, the state administrative agency (SAA) for federal grant purposes; representatives from localities in the Commonwealth; public education institutions; public health institutions; representatives of rural, suburban, and high population jurisdictions; judicial entities; the legislative branch; election infrastructure officials; the Virginia State Police; the Virginia National Guard; and others with expertise and skillsets that best represent the cybersecurity interests.

The VCPC currently consists of 15 Members:

- Michael Watson, Chair, Chief Information Security Officer (CISO) of the Commonwealth, VITA
- Michael Dent, Vice Chair, Chief Information Security Officer, Fairfax County Department of Information Technology
- Aliscia Andrews, Office of the Governor
- Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
- Robbie Coates, Director, Grant Management and Recovery, VDEM

- Adrian Compton, Tribal Administrator, Monacan Indian Nation
- Charles DeKeyser, Major, Virginia Army National Guard
- Brenna Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
- Major Eric Gowin, Virginia State Police
- John Harrison, IT Director, Franklin County
- Derek Kestner, Information Security Officer, Supreme Court of Virginia
- Benjamin Shumaker, Cybersecurity Specialist, King William County Government
- Beth Burgin Waller, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
- Wesley Williams, Executive Director of Technology, Roanoke City Public Schools
- Stephanie Williams-Hayes, Chief Information Security Officer, Virginia Department of Health

Filling the 16th seat, for an elections official, is pending.

The VCPC also regularly consults with a group of advisors with relevant expertise in cybersecurity and information technology.

CYBERSECURITY PLAN

The Virginia Cybersecurity Planning Committee convened on seven occasions spanning from November 2022 to August 2023. Records from the meetings are available on VITA's website and the Virginia Regulatory Town Hall.

The VCPC worked on developing a comprehensive cybersecurity plan, in collaboration with advisors and other stakeholders in the areas they represent. Additional input and feedback from local governments and related associations have been integrated into the plan's development. This plan adheres to the inclusion of all specific required elements as detailed below:

1. Manage, monitor, and track information systems, applications, and user accounts
2. Monitor, audit, and track network traffic and activity
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk
5. Adopt and use best practices and methodologies to enhance cybersecurity (references National Institute of Standards and Technology (NIST))
    a. Implement multifactor authentication
    b. Implement enhanced logging

    c. Data encryption for data at rest and in transit
    d. End use of unsupported/end-of-life software and hardware that are accessible from the internet
    e. Prohibit use of known/fixed/default passwords and credentials
    f. Ensure the ability to reconstitute systems (backups)
    g. Migration to the .gov internet domain
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain
7. Ensure continuity of operations including by conducting exercises
8. Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks
10. Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department of Homeland Security
12. Leverage cybersecurity services offered by the Department of Homeland Security
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
15. Ensure rural communities have adequate access to, and participation in plan activities
16. Distribute funds, items, services, capabilities, or activities to local governments

The committee successfully completed the plan, approving it at the July 2023 meeting. The plan received approval from FEMA and CISA on October 10, 2023. Updates building on prior investments will be submitted as needed during the program, ensuring a continuous and evolving approach to cybersecurity.

SURVEY OF INTEREST

The Virginia Cybersecurity Planning Committee, through VDEM's email list for the program, sent a survey to assess interest and readiness for potential grant funding initiatives, aligned with goals and objectives in the Virginia Cybersecurity Plan. The interest survey closed September 22, 2023. The results will assist the VCPC with understanding interest

levels, building awareness, offering services that meet the interests expressed, and tailoring the grant applications in order to better meet localities' needs.

FUTURE PLANS AND STRATEGIES

During the next year, the program's focus will be on several crucial objectives.

Following the results of the survey of interest, the Virginia Cybersecurity Planning Committee will work to assess and determine priorities for use of the year one (federal Fiscal Year 2022) funding. This process will involve a comprehensive consideration of the most pressing cybersecurity needs of localities.

Additionally, VITA will work in conjunction with VDEM and the VCPC to create an application for the localities to apply for SLCGP funding, ensuring that applications align seamlessly with the identified priorities and objectives.

FEMA and CISA also have released the notice of funding opportunity for year two (federal Fiscal Year 2023) of the SLCGP. VITA and VDEM have completed that application.

CONCLUSION

This report outlined the key milestones and collaborative efforts undertaken to advance the State and Local Cybersecurity Grant Program. VITA is pleased to provide this comprehensive overview of the progress, including the formation of the Virginia Cybersecurity Planning Committee, development and adoption of the Virginia Cybersecurity Plan, the assessment of locality readiness and interest, and alignment with the program objectives. Moving forward, VITA and our state partners are dedicated to determining funding priorities, facilitating locality applications and receipt of funding, and continuing to foster strong partnerships with localities to improve cybersecurity through a whole of the Commonwealth approach.