VIRGINIA
IT AGENCY

Cybersecurity Grant Program Report

Virginia Information Technologies Agency

vita.virginia.gov

September 2024

THIS REPORT

The Virginia Information Technologies Agency (VITA) submits this report pursuant to Item 81(F)(2) of the 2024 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 October 2023 – September 2024.

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 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 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 a substantial amount of the required 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. VITA and VDEM signed an interagency Memorandum of Understanding (MOU) in 2024. This MOU defines the responsibilities of each agency in delivering results for the Program.

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.

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; representatives from localities in the Commonwealth; public education institutions; public health institutions; representatives of rural, suburban, and high population jurisdictions; the judicial branch; the legislative branch; election infrastructure officials; public safety agencies; 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
- Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
- Robbie Coates, Director, Grant Management and Recovery, VDEM
- Charles DeKeyser, Major, Virginia Army National Guard
- Brenna Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
- Derek Kestner, Information Security Officer, Supreme Court of Virginia
- Charles Huntley, Director of Technology, County of Essex
- Beth Burgin Waller, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
- Wesley Williams, Executive Director of Technology, Roanoke City Public Schools
- Glendon Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services
- Brandon Smith, Chief Information Officer, Department of Elections

- Kenneth Pfeil, Chief Data Officer, Office of Data Governance and Analytics
- Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security
- Uma Marques, Information Technology Director, Roanoke County Government

Mr. Adrian Compton, appointed while tribal administrator for the Monacan Indian Nation, resigned in August 2024 after leaving employment, and the tribal representative seat is currently vacant.

The VCPC also regularly consults with other stakeholders with relevant expertise in cybersecurity and information technology.

CYBERSECURITY PLAN

Records from the meetings of the Virginia Cybersecurity Planning Committee 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 were integrated into the plan's development.

The Virginia Cybersecurity Plan, which is available to the public via VITA's website, was approved by FEMA and CISA on October 10, 2023. Subsequently, updated plans 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. There were 140 respondents to the survey, of which 1% were tribal government and 2% were vendors. After reviewing the survey responses, the Virginia Cybersecurity Planning Committee prioritized conducting assessments of localities as compared to Virginia's Cybersecurity Plan. The committee felt that assessments would help public bodies understand their cybersecurity maturity level, provide a baseline, and inform the needs and future investments of the program.

CYBERSECURITY PLAN CAPABILITY ASSESSMENT PROJECT

In January 2024, the Virginia Cybersecurity Planning Committee voted to release the application for the Cybersecurity Plan Capability Assessment Project. The committee also voted to authorize VITA and VDEM to complete the necessary administrative grant work to proceed with the project.

The Cybersecurity Plan Capability Assessment Project provides an independent assessment of eligible local government entities cybersecurity capabilities as compared to the standards outlined in Virginia's Cybersecurity Plan. Collectively, the assessments also provide data to the committee, which will be used to determine prioritization of future projects funded by SLCGP grant awards and 2022 Appropriate Act funds.

Eligible entities, per the Notice of Funding Opportunity (NOFO), include "local government" as defined in 6 U.S.C. § 101(13). Further, educational institutions were generally eligible to receive assistance under SLCGP if it is an agency or instrumentality of a state or local government under state and/or local law.

As of May 15, 2024, the Cybersecurity Plan Capability Assessment Project received applications from 172 eligible entities. 85% of Virginia counties and cities had at least one local government entity apply to participate in the project.

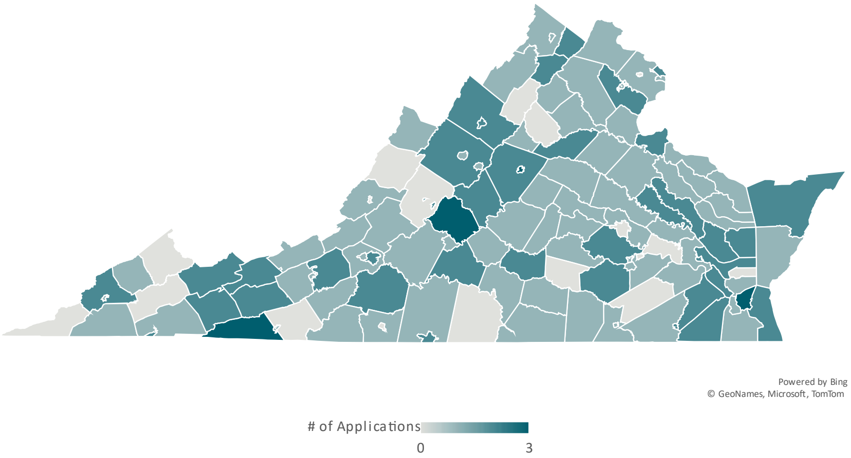

Figure 1: Geographic Reach of Qualified Local Government Applicants[1]

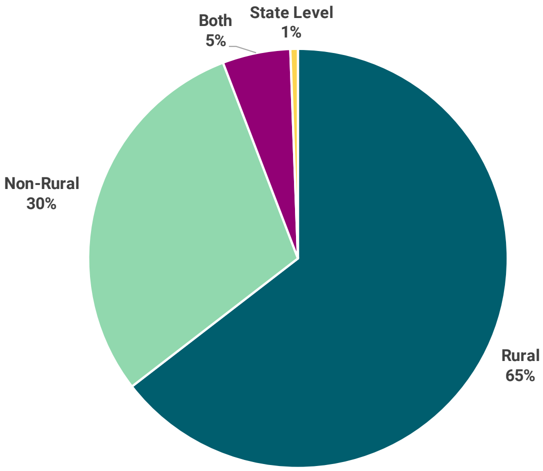

Figure 2: Rural vs. Non-Rural Applicants[2]

65% of eligible applicants (as of May 15, 2024) met the NOFO's definition of rural. Based on this, the Committee is confident of meeting the 25% rural passthrough requirement for the grant.

[1] Includes: Local governments, tribal governments, public school districts, regional government entities (e.g., regional libraries and park systems), regional schools, and colleges/universities.

[2] Both – regional entities with both rural/non-rural counties and cities within their service area; state level – colleges/universities

Eligible applicants consist primarily of local governments (42%) and school districts (40%):

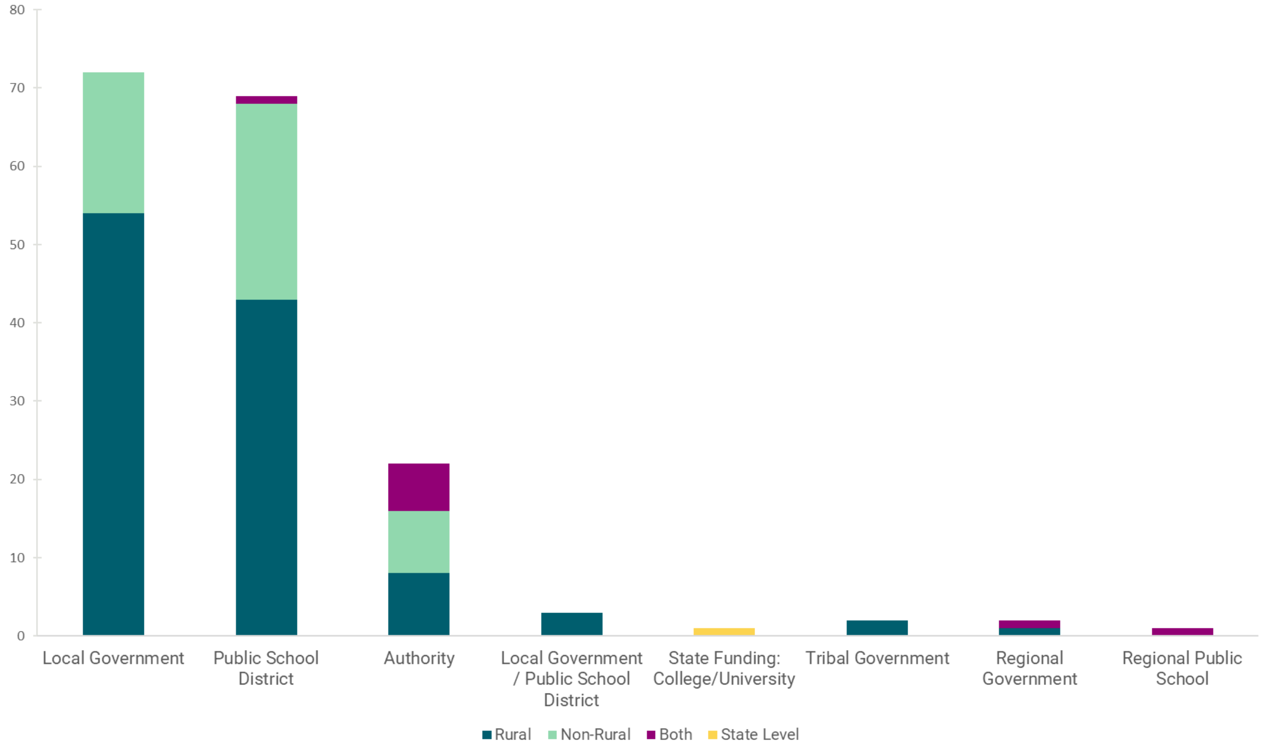

Figure 3: Applicants by Entity Type

STRATEGIC AND PROGRAMMATIC MONITORING BY CISA/FEMA

In August 2024, VDEM and VITA participated in a virtual desk review meeting with representatives from FEMA and CISA. The agenda for the review focused primarily on general grant program questions, cybersecurity topics, and metrics and evaluation. The review did not identify any compliance findings or corrective action points.

STATE AND LOCAL CYBERSECURITY GRANT PROGRAM YEAR 2

VITA and VDEM applied for and was awarded $10,890,904 to continue cybersecurity efforts in the Commonwealth. The period of performance for this award year is from December 1, 2023 – November 27, 2027. The year 2 Notice of Funding Opportunity requested applicants to focus on objectives 2 – 4 of the SLCGP:

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.

COST SHARING WAIVER REQUEST

In August 2024, VDEM submitted a cost sharing waiver request to FEMA and CISA for the cost share requirement for the Cybersecurity Plan Capability Assessment Project.

The request utilized the economic hardship category cited in the FY22 SLCGP NOFO Appendix H – "for local governments only, demonstration that those localities have areas within them that are designated as either 'high' or 'very high' on the Centers for Disease Control and Prevention's (CDC) Social Vulnerability Index (SVI)" – to request a $60,642 cost share waiver.

VITA and VDEM believe that minimizing the direct financial impact to localities is critical to participation and ultimately to the improvement of Virginia's whole of state cybersecurity posture. By minimizing or eliminating barriers to project participation, locality engagement in projects increases, as demonstrated by the more than 170 applications received for the Cybersecurity Plan Capability Assessment Project. For local government entities participating in this project, there was no cost to participate, no need to seek reimbursement after the project, and no requirements for federal grant reporting.

PROGRAM FUNDING

As stated in the 2022, 2023, and 2024 Appropriation Acts, the $4,921,400 in general funds appropriated for the SLCGP was "intended to serve as the full program match for grant availability under this program." That amount was necessarily an estimate in the 2022 Session, given that the initial program NOFO was not released until fall 2022. Moreover, the amounts available to Virginia each year under the program can vary based on the participation of other eligible entities.

Subsequent review of the SLCGP has revealed that the general funds appropriated in 2022 are not actually sufficient to provide the full program match for all program years. At present, VDEM and VITA estimate a shortfall of approximately $1.86 million, which will begin to be felt in year three of the program.

VDEM and VITA are currently working to narrow that gap using strategies such as the cost waiver request discussed above. The Commonwealth may also be able to reduce the amount of necessary matching funds by providing services. VITA anticipates next year's report providing an update on the funding gap, which can inform policymakers' consideration of the future of state support for local government cybersecurity beginning in the 2026 Session.

FUTURE PROGRAM PLANS AND STRATEGIES

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

Following the results of the Cybersecurity Plan Capability Assessment Project, the Virginia Cybersecurity Planning Committee will determine funding priorities and subsequent projects. The priorities and projects will be informed by the risks and vulnerabilities uncovered through the assessments.

VITA will also focus on implementing the security operations center, and support local governments as they begin to utilize this service.

VITA and VDEM also will apply for available funds in year three (federal Fiscal Year 2024) of the SLCGP. It is anticipated that the application will be released in early calendar year fourth quarter.

CONCLUSION

The support of Governor Youngkin’s administration and the General Assembly for the State and Local Cybersecurity Grant Program has already achieved significant results. The Virginia Cybersecurity Planning Committee has successfully established an ongoing collaborative relationship between state and local government in the area of cybersecurity, an important and new development in Virginia. The approved Virginia Cybersecurity Plan represents the first whole-of-the-Commonwealth cybersecurity planning and prioritization.

This report provides an overview of the program’s status and progress in its second operational year, including the first substantial use of program funds across the Commonwealth through the cybersecurity assessments project. Moving forward, VITA and our state and local partners will continue determining funding priorities, facilitating locality applications and receipt of funding, and carrying out the management and operational work of program cybersecurity projects.