VIRGINIA IT AGENCY

Cybersecurity Grant Program Report

Virginia Information Technologies Agency

vita.virginia.gov

September 2025

THIS REPORT

The Virginia Information Technologies Agency (VITA) submits this report pursuant to Item 81(F)(2) of the 2025 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 2024 – September 2025.

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. This Program appropriates approximately $1 billion over four years nationwide to help address cybersecurity risks and threats.

The Program is structured to prioritize funding primarily to local entities while promoting a coordinated, statewide approach. States are required to apply for and administer the grants in accordance with a state-level cybersecurity plan, which must developed and approved by an intergovernmental cybersecurity planning committee established according to state laws and procedures.

Under the program, 80% of the grant funds must be distributed to local governments as subrecipients. Of that amount, at least 25% is specifically designated for to rural areas, acknowledging the unique challenges they face. Additionally, no more than 5% of the funds may be used to cover administrative expenses related to the Program.

First in 2002 and then again in 2025, the General Assembly and Governor Youngkin have supported the Program by appropriating 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 14 Members:

- Michael Watson, Chair, Chief Information Security Officer (CISO) of the Commonwealth, VITA
- Troy Adkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe
- 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, Commonwealth of Virginia
- Charles Huntley, Director of Technology, County of Essex
- Derek Kestner, Information Security Officer, Supreme Court of Virginia
- Uma Marques, Information Technology Director, Roanoke County Government
- Glendon Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services
- Brandon Smith, Chief Information Officer, Department of Elections
- Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security

- Beth Burgin Waller, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
- Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

In June 2025, Michael Dent, Vice Chair, and Kenneth Pfeil, Chief Data Officer, Office of Data Governance and Analytics resigned from their positions on the VCPC. As of this report, both seats are remain vacant. The VCPC continues to engage regularly with stakeholders who possess relevant expertise in cybersecurity and information technology to support its mission.

COMMITTEE MEETINGS

Between October 2024 to September 2025, the VCPC convened on five occasions. Records of these meetings are publicly accessible through the Virginia Information Technologies Agency's website and the Virginia Regulatory Town Hall.

CYBERSECURITY PLAN

The Virginia Cybersecurity Plan, originally developed in 2023 with input from advisors, stakeholders, local governments, and related associations, was approved by FEMA and CISA on October 10, 2023.; As required by the grant, the plan was revised and updated during the 2024-2025 meeting cycle. Updated versions, building on prior investments, will continue to be submitted as needed to ensure a dynamic and evolving approach to cybersecurity. Thie plan is publicly available on the VITA website.

CYBERSECURITY PLAN CAPABILITY ASSESSMENT PROJECT

The Cybersecurity Plan Capability Assessment Project was completed in October 2024. Project participants included 170 local government entities. Further information about the characteristics of the participants can be found below.

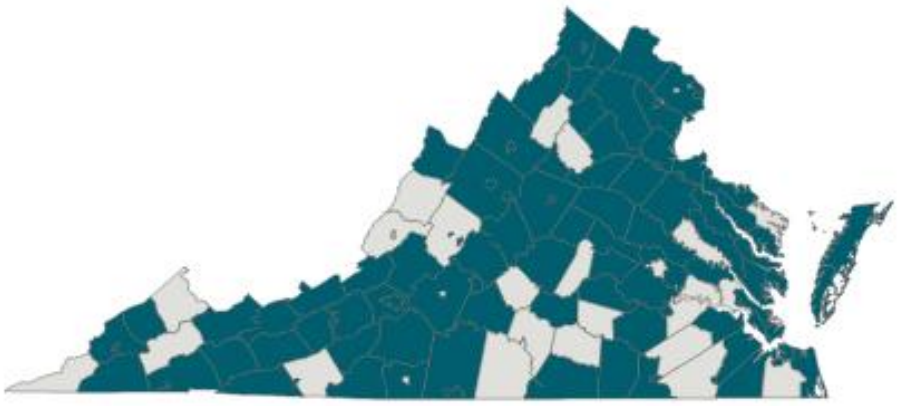


Figure 1 - Geographic distribution of Cybersecurity Plan Capability Assessment Local Government Entity Participants

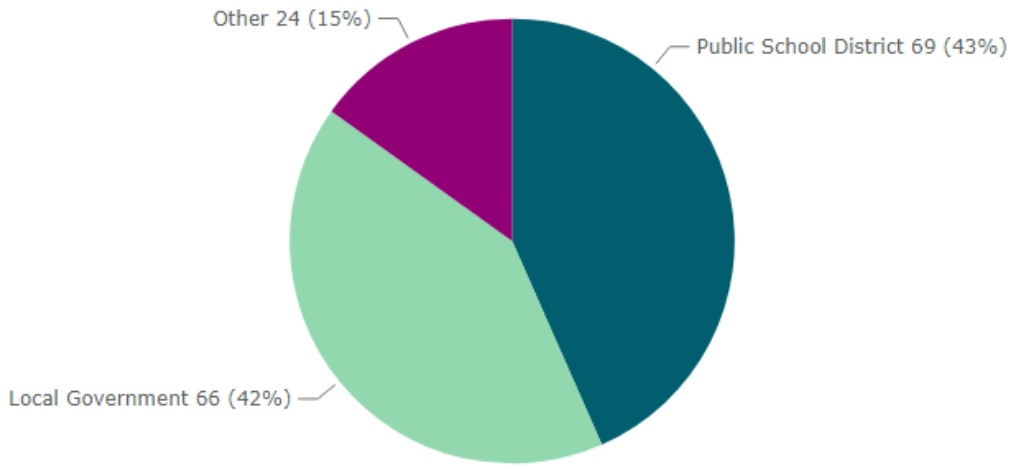


Figure 2 - Cybersecurity Plan Capability Assessment Participants by Entity Type

The SLCGP requires that 25% of local spending be targeted towards rural communities. This project exceeded the requirement by 37%, with 62% of the funds being spent on entities meeting the definition of rural per the Notice of Funding Opportunity.

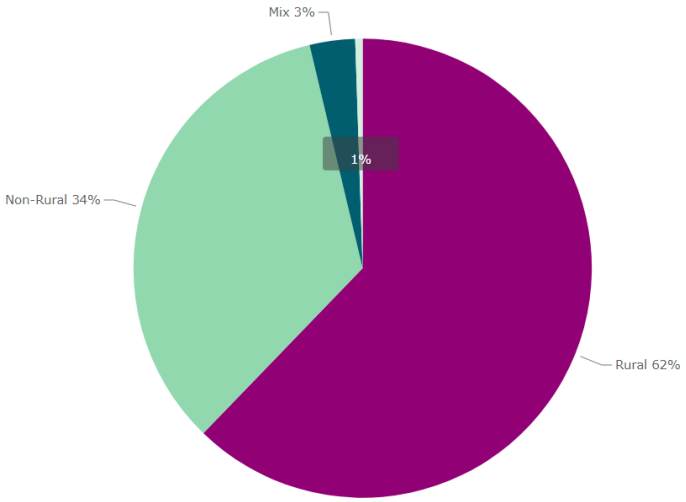


Figure 3 - Percentage of Cybersecurity Plan Capability Assessment Passed Through to Rural Entities

The Cybersecurity Plan Capability Assessment Project concluded with a presentation to the VCPC during their October 30, 2024 meeting.

During this presentation, committee members received an overview of the current state of cybersecurity capabilities outlined in the Virginia Cybersecurity Plan based on the 170 local government entity participants.

The committee also examined the potential future capabilities if improvements were implemented.

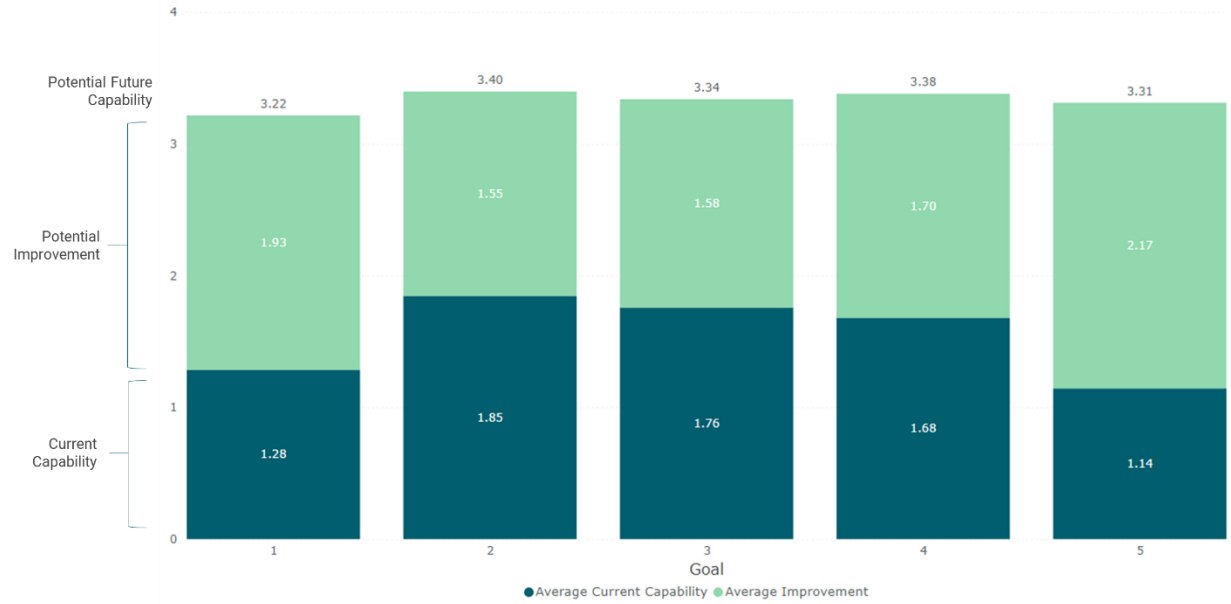


Figure 4 - Current and Future Capabilities per Virginia Cybersecurity Plan Goal

1

Based on their review of the assessment findings, the committee voted unanimously to prioritize spending of FY 2022 and FY 2023 funds on those goals/objectives with improvement areas, those that support a locality's participation in a SOC, and those that complemented prioritized objectives, which includes:

- Installing and maintaining vulnerability management software
- Implementing secure remote network access, including zero trust network access and multifactor authentication
- Creating and maintaining an enterprise asset inventory of all technology assets (including hardware and software)
- Establishing and maintaining a data inventory and performing data sensitivity analysis for all systems supporting the organization's business

[1] Capability Levels:

0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

- Deploying endpoint detection and response for all workstations and servers
- Implementing firewalls for ingress and egress points, end point devices, and web applications

Collectively, these areas are considered Phase 2 of Virginia's SLCGP.

PHASE 2

Applications were opened for Phase 2 projects early in 2024, and Phase 2 received 141 applications from qualified organizations across the commonwealth.

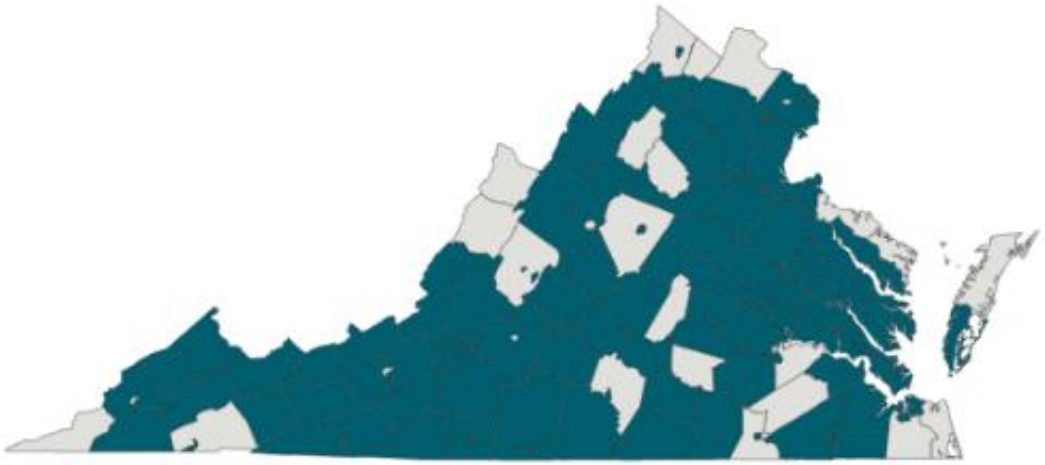
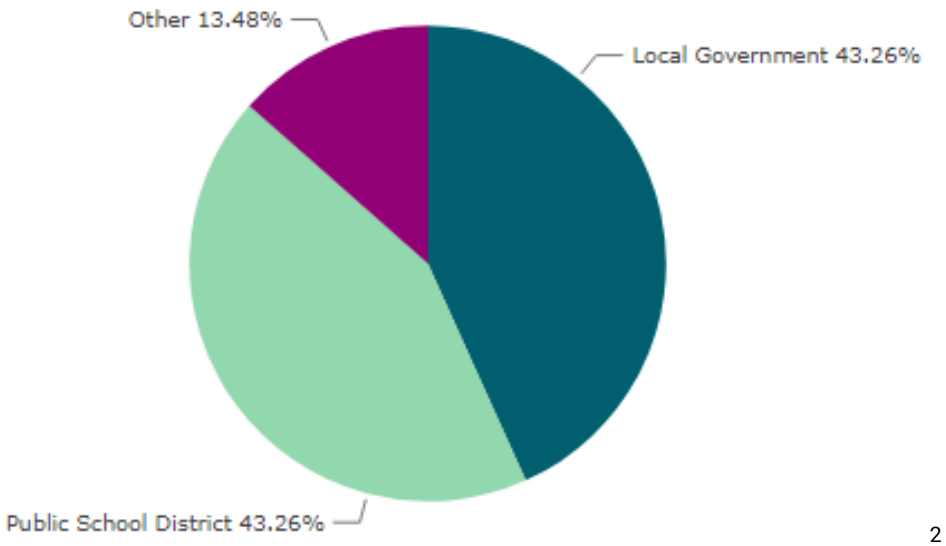


Figure 5 - Geographic distribution of applications



[2]

[2] Other includes tribal governments, authorities and other local government entities

Figure 6 - Applicant organization type

Virginia's participation in the SLCGP has been focused on:

- Achieving improvements for **as many qualified entities** as possible
- **Making it straightforward** for qualified entities to participate while meeting all requirements outlined in the Notice of Funding Opportunities associated with the federal grant program.

These two focus areas resulted in a program design that:

- Provides opportunities for qualified entities to participate **without taking on the burden** of federal grant management requirements
- Creates project execution types that **provide the resources needed** to implement and maintain improvements for qualified entities that may not have the staff to support
- Involves applications that are relatively **simple**

With this in mind, Phase 2 was designed to provide a preselected toolset coupled with the opportunity for local government entities to select the project implementation model that suited their organization best:

- Full service – includes installation, configuration and ongoing maintenance support provided for the local government entity
- Implementation only – provides resources for installation and configuration, with the local government entity taking responsibility for ongoing maintenance
- Contract only – provides access to volume-based pricing achieved through the SLCGP and grant funds to purchase licenses, with the local government entity responsible for installation, configuration and maintenance
- Additional license purchase – offered for localities that need additional financial resources to fully cover their environment with a particular security control

Entities that did not want to utilize a preselected toolset were able to submit an application for pass-through funding projects aligned with one of the six focus areas of the phase.

After collecting applications for Phase 2, the committee reviewed the distribution of locality interest across the 6 focus areas of Phase 2 together with requested execution types. Given this information, the committee authorized:

- Budget – to include all remaining local grant dollars from grant year 2022, all local grant dollars from grant year 2023 and 2024, representing up to $15.8MM in approved budget for Phase 2 projects. This amount was further allocated:
    - 60% - asset inventory, data inventory and secure remote network access project focus areas

    - 40% firewalls, vulnerability and endpoint detection and response
- Funding prioritization for applicants with the following characteristics:
    - Low current capability levels
    - High future capability levels
    - High likeliness of success
    - Federal requirements/prerequisites
    - Participation in the Cybersecurity Plan Capability Assessment project or completion of an equivalent assessment
    - Entities that choose either full service model or engage in necessary future resource planning if seeking a lesser level of services (such as implementation only)

Utilizing these characteristics, application review, decisioning and communication with localities is underway.

FUTURE PROGRAM PLANS AND STRATEGIES

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

- Successful implementation of the six focus areas of Phase 2 with approved local government entities
- Implentation of a security operations center to provide monitoring and auditing of the local government entity environments

FUTURE FEDERAL GRANT OPPORTUNITIES

The Virginia's Federal Fiscal Year 24 Application was approved by FEMA with:

- $6,548,801 federal share
- $2,806,629 cost share
- $9,355,430 total

The Federal Fiscal Year 25 (FFY25) grant application was submitted on August 15, 2025. The federal award amount is projected to be $2,109,252. The total award will be $3,515,756 with a match requirement of 40%. The period of performance (PoP) will be September 1, 2025, through August 31, 2029.

CONCLUSION

This report outlines the program's progress in its third operational year, including the use of funds for projects identified in the Cybersecurity Plan Capability Assessment. Through the SLCGP, the VCPC has collaborated with state and local governments to plan and implement cybersecurity improvements. Moving forward, VITA and its partners

will continue prioritize funding and support the execution of critical cybersecurity initiatives across the Commonwealth.