Virginia Cybersecurity Planning Committee

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Readoption of Remote Participation Policy	Staff
Approval of Minutes	Staff
Locality SOC update	Staff
Project Update	Mary Fain
Phase 3 Discussion and Recommendations	Mr. Watson
Annual Review of Cybersecurity Plan	Staff
Officer Election	Staff
Public Comment Period	
Other Business	Staff
Adjourn	

The following is the remote or electronic participation policy of the Virginia Cybersecurity Planning Committee (VCPC).

Member Remote Participation

Individual VCPC members may participate in meetings of VCPC by electronic communication means to the full extent permitted by applicable law, including § 2.2-3708.3 of the Code of Virginia. (As of July 2024, when such individual participation is due to a personal matter, such participation is limited by law to two meetings per calendar year or 25 percent of the meetings held per calendar year rounded up to the next whole number, whichever is greater.)

This shall apply to the entire membership and without regard to the identity of the member requesting remote participation or the matters that will be considered or voted on at the meeting. VCPC advisors may also participate by electronic communication means.

Whenever a member wishes to participate from a remote location, the law requires a quorum of VCPC to be physically assembled at the primary or central meeting location.

Virtual Meetings

VCPC may hold all-virtual public meetings to the full extent permitted by applicable law, including Virginia Code § 2.2-3708.3(C). (As of July 2024, such all-virtual public meetings are limited by law to two meetings per calendar year or 50 percent of the meetings held per calendar year rounded up to the next whole number, whichever is greater, and may not be held consecutively with another all-virtual public meeting. When audio-visual technology is available, a member of a public body shall, for purposes of a quorum, be considered absent from any portion of the meeting during which visual communication with the member is voluntarily disconnected or otherwise fails or during which audio communication involuntarily fails.)

Requests

Requests for remote participation or for the VCPC to conduct an all-virtual public meeting shall be conveyed to VITA staff who shall then relay such requests to the Chair of the VCPC. A record of such a request should be submitted via email to cybercommittee@vita.virginia.gov. If a request is made in another manner, staff shall ensure a record exists of the request and its handling.

The Chair shall approve individual participation from a remote location unless a member asserts that such participation would violate this policy or the provisions of the Virginia Freedom of Information Act (Va. Code § 2.2-3700 *et seq.*). If a member's participation from a remote location is challenged, then VCPC shall vote whether to allow such participation.

The request for remote participation or that VCPC conduct an all-virtual public meeting shall be recorded in the minutes of the meeting. If VCPC votes to disapprove of the member's participation because such participation would violate this policy, such disapproval shall be recorded in the minutes with specificity. The minutes shall include other information as required by law (see Va. Code §§ 2.2-3707 and 2.2-3708.3), depending on the type of remote participation or all-virtual public meeting.

This policy was originally adopted at the VCPC meeting on August 21, 2024, and shall be reviewed and adopted annually by recorded vote at a public meeting.

_____

The following additional explanation is intended to be informative as to current requirements and is not required by this policy independent of the requirements of law.

Additional Explanation of Current Requirements for Remote Participation by Members

When a meeting is scheduled to be held in person, there are four circumstances set out in § 2.2-3708.3(B) where individual members of VCPC may participate from a remote location instead of participating in person. In order to use these provisions, the member must notify the chair of the public body of one of the following four reasons for remote participation:

1. The member has a temporary or permanent disability or other medical condition that prevents the member's physical attendance. (For purposes of determining whether a quorum is physically assembled, an individual member of a public body who is a person with a disability as defined in § 51.5-40.1 and uses remote participation counts toward the quorum as if the individual was physically present.)
2. A medical condition of a member of the member's family requires the member to provide care that prevents the member's physical attendance or the member is a

caregiver who must provide care for a person with a disability at the time the public meeting is being held thereby preventing the member's physical attendance. (For purposes of determining whether a quorum is physically assembled, an individual member of a public body who is a caregiver for a person with a disability and uses remote participation counts toward the quorum as if the individual was physically present.)

3. The member's principal residence is more than 60 miles from the meeting location identified in the required notice for such meeting.

   or

4. The member is unable to attend the meeting due to a personal matter and identifies with specificity the nature of the personal matter. However, the member may not use remote participation due to personal matters more than two meetings per calendar year or 25 percent of the meetings held per calendar year rounded up to the next whole number, whichever is greater.

The limitations to two meetings per calendar year or 25 percent of the meetings held per calendar year does not apply to the first three types of remote participation above; it only applies when the member participates due to personal matter.

Additional Explanation of Current Requirements for Minutes

- If an individual member remotely participates in a meeting, a general description of the remote location must be included in the minutes (it does not need to be an exact address— for example, the minutes might read that "[Member] participated from his home in [locality]" or that "[Member] participated from her office in [locality]."). The remote location does not have to be open to the public.
- If a member remotely participates due to a (i) temporary or permanent disability or other medical condition that prevented the member's physical attendance or (ii) family member's medical condition that required the member to provide care for such family member, thereby preventing the member's physical attendance, that fact must be included in the minutes. The requirement is to record in the minutes the fact that a disability or medical condition prevents the member's physical attendance; to the minutes need not identify the specific disability or medical condition.
- If a member remotely participates because the member's principal residence is more than 60 miles from the meeting location, the minutes must include that fact.
- If a member remotely participates due to a personal matter, the minutes must include the specific nature of the personal matter cited by the member.
- As stated above, if remote participation by a member is disapproved because it would violate the participation policy adopted by the public body, such disapproval must be recorded in the minutes with specificity. Note that even if remote participation is disapproved, the member may continue to monitor the

meeting from the remote location but may not participate and may not be counted as present at the meeting.

Examples of disability or medical condition that prevents physical attendance:

- Temporary hospitalization or confinement to home;
- Contagious illness; or
- Any temporary or permanent physical disability that physically prevents travel to the meeting location.

Examples of personal matters that may prevent physical attendance:

- Flat tire or other mechanical failure on the way to the meeting;
- Traffic congestion or stoppage;
- Personal, family, or business emergency;
- Blizzard, flood, or other severe weather conditions that prevent travel to the meeting location;
- Business trip;
- Family trip; or
- Scheduling conflict.

Additional Explanation of Current Requirements for All-Virtual Meetings

In accordance with Virginia Code § 2.2-3708.3(C) and other applicable law, the following must be met for all-virtual meetings:

1. An indication of whether the meeting will be an in-person or all-virtual public meeting is included in the required meeting notice along with a statement notifying the public that the method by which a public body chooses to meet shall not be changed unless the public body provides a new meeting notice in accordance with the provisions of § 2.2-3707;
2. Public access to the all-virtual public meeting is provided via electronic communication means;
3. The electronic communication means used allows the public to hear all members of the public body participating in the all-virtual public meeting and, when audio-visual technology is available, to see the members of the public body as well;
4. A phone number or other live contact information is provided to alert the public body if the audio or video transmission of the meeting provided by the public body fails, the public body monitors such designated means of communication during the meeting, and the public body takes a recess until public access is restored if the transmission fails for the public;
5. A copy of the proposed agenda and all agenda packets and, unless exempt, all materials furnished to members of a public body for a meeting is made available to the public in electronic format at the same time that such materials are provided to members of the public body;

6. The public is afforded the opportunity to comment through electronic means, including by way of written comments, at those public meetings when public comment is customarily received;
7. No more than two members of the public body are together in any one remote location unless that remote location is open to the public to physically access it;
8. If a closed session is held during an all-virtual public meeting, transmission of the meeting to the public resumes before the public body votes to certify the closed meeting as required by subsection D of § 2.2-3712;
9. The public body does not convene an all-virtual public meeting (i) more than two times per calendar year or 50 percent of the meetings held per calendar year rounded up to the next whole number, whichever is greater, or (ii) consecutively with another all-virtual public meeting; and
10. Minutes of all-virtual public meetings held by electronic communication means are taken as required by § 2.2-3707 and include the fact that the meeting was held by electronic communication means and the type of electronic communication means by which the meeting was held. If a member's participation from a remote location pursuant to these requirements is disapproved because such participation would violate the policy adopted pursuant to § 2.2-3708.3(D), such disapproval shall be recorded in the minutes with specificity.

If an individual member had already reached his limit on participation due to personal matters, but the public body scheduled an all-virtual public meeting, the member could still participate in all virtual public meeting because these numerical limits are counted separately for the different types of electronic meetings.

Virginia Cybersecurity Planning Committee
August 19, 2025 – 1:00 p.m.
Virtual

Call to Order:
A meeting of the Virginia Cybersecurity Planning Committee was called to order at 1:01 pm. Mr. Watson welcomed the members.

Presiding:
Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present:
Robbie Coates, Director, Grant Management and Recovery, Virginia Department of Emergency Management

Members Participating Remotely:
Troy Adkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe
Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Charles Huntley, Director of Technology, County of Essex
Glenn Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
Wesley D. Williams, Executive Director of Technology, Roanoke City Public Schools
Uma Marques, Information Technology Director, Roanoke County Government
Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security, Office of the Governor
Brandon Smith, Chief Information Officer, Department of Elections
Derek Kestner, Information Security Officer, Supreme Court of Virginia

Members Not Present:
Charles DeKeyser, Major, Virginia Army National Guard

Staff Present:
Joshua Heslinga, Director of Legal and Legislative Services, Virginia IT Agency
Mylam Ly, Policy & Governmental Affairs Manager, Virginia IT Agency
Harper Minarik, CAO Associate, Virginia IT Agency
April Gauldin, Legal and Legislative Services Coordinator, Virginia IT Agency
Mary Fain, Project Manager, Virginia IT Agency
Janet Logan, Contractor, Virginia IT Agency
Sam Taylor, Communications Specialist, Virginia IT Agency

Review of Agenda:
Ms. Gauldin provided an overview of the agenda.

Approval of Minutes:
The June 24 meeting minutes were displayed on the screen. Upon a motion by Mr. Smith and seconded by Ms. Marques, the committee unanimously voted to approve the June 24 meeting minutes.

Cybersecurity Plan Development Report

Budget Update
Ms. Fain presented the financial update. Administrative expenses include meeting expenses and the addition of a staff program manager to support grant implementation throughout the full life cycle of project deliverables aligned with grant objectives. This position was introduced as a new item in the upcoming budget year. The committee discussed the process for submitting official project amendments to FEMA, which are required to estimate costs and request the release of funds. These amendments are based on projected phases of incoming work. A meeting with FEMA and CISA is being planned to review current progress and discuss future spending plans.

FY25 Grant Application Update
Mr. Coates discussed the two-week turnaround for the year 4 (Federal Fiscal Year (FFY) 2025) grant application. The federal amount will be $2,109,252, with a 60/40 match this year. The total award will be $3,515,756. The period of performance (PoP) will be September 1, 2025, through August 31, 2029. Year 3 (FFY2024) runs through January 31, 2029. An updated slide for the cost share percentage will be updated at a later date.

Phase 2 Project Updates
Ms. Fain discussed Endpoint Detection and Response (EDR) applications, which include government, school districts, authorities, and Community Service Boards (CSBs). Of the applications received, 34% of the applications were approved and 66% of the applications were deferred due to existing capabilities at or above level 2. Deferred applicants required additional documentation and had higher cost application requests. Three applicants withdrew after pursuing alternative solutions. Regarding vulnerability applications, 5% are on hold due to high funding requests and licensing issues; these applicants will be contacted to work on feasible solutions. Most applications are requesting either full service or implementation-only services. Ms. Fain outlined the commitment period, detailed planning, rollout schedule, and transition to maintenance. Full-service applications are progressing more quickly, while implementation-only applications have been slower to confirm commitments. One vendor will provide full-service applications, while multiple vendors will handle implementation-only applications based on locality timelines. EDR is currently in the commitment phase (confirming locality commitments in line with their prior applications), followed by detailed planning and deployment. Contract signing delays and locality blackout dates are expected to extend the timeline to maximize tool utilization. This phased process will be repeated for asset inventory, data inventory, and secure remote network access firewalls, with adjustments based on project complexity. EDR and Vulnerability projects are being prioritized due to their rapid deployment. Projects currently in flight can be repeated if needed.

Public Comment Period:
There were no public comments.

Other Business:
Mr. Watson opened the floor for other business. Mr. Smith requested a visual representation of localities ties to the planned state SOC.

Mr. Watson noted the September meeting is canceled. The next meeting will be on October 21 at 10am.

Adjourn
Upon a motion by Mr. Williams and seconded by Mr. Kestner, the Committee meeting was adjourned at 1:44 pm.

Virginia Cybersecurity Planning Committee
October 21, 2025 - 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,

Call to Order:
A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:00 am. Mr. Watson welcomed the members.

Presiding:
Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present:
Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
Charles DeKeyser, Major, Virginia Army National Guard
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Charles Huntley, Director of Technology, County of Essex

Members Participating Remotely:
Troy Adkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe.
Uma Marques, Information Technology Director, Roanoke County Government.
Wesley D. Williams, Executive Director of Technology, Roanoke City Public Schools
Glenn Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services

Mr. Adkins, Ms. Marques, and Mr. Williams participated from their principal residences as it is more than 60 miles from the meeting location. Mr. Schmitz participated remotely due to work reasons.

Members Not Present:
Brandon Smith, Chief Information Officer, Department of Elections
Derek Kestner, Information Security Officer, Supreme Court of Virginia
Robbie Coates, Director, Grant Management and Recovery, Virginia Department of Emergency Management
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black

Staff Present:
Mylam Ly, Policy & Governmental Affairs Manager, Virginia IT Agency
Harper Minarik, CAO Associate, Virginia IT Agency
April Gauldin, Legal & Legislative Services Coordinator, Virginia IT Agency
Mary Fain, Director of Information Security Programs, Virginia IT Agency
Janet Logan, Project Manager, Virginia IT Agency
Erica Bland, IT Security Governance & Compliance Manager, Virginia IT Agency
Sam Taylor, Communications Specialist, Virginia IT Agency
Alexandra Ramirez Randazzo, Legal Compliance & Policy Manager, Virginia IT Agency

Review of Agenda:
Ms. Minarik provided an overview of the agenda.

Approval of Minutes:

As a physical quorum was not present, a vote to approve the minutes could not be conducted. This item will be carried forward to the agenda for the next meeting.

Finances

Ms. Fain presented the financial update. The program is currently working through Federal Fiscal Year (FFY) 2026 monies. The funds for FFY 2022 will be expended by the end of calendar year 2025 on licensing purchases. There have not been any significant changes in Year 2 and Year 3 plans. Ms. Fain discussed the Phase 2 allocation for firewalls, vulnerability endpoint detection and response (EDR) and asset inventory, data inventory, and secure remote access. Currently, the Security Operations Center (SOC) is still in process but taking longer than anticipated due to the procurement process. Chair Watson stated that there is consideration for upgrading the EDR licenses to Falcon Complete to address the timing difference. Ms. Fain reported that there were not as many requests from localities for firewalls and that Network Firewalls are currently under review. Asset and inventory price quotes will be committed to by the end of the calendar year.

Phase 2 Updates

Ms. Fain discussed Phase 2 application decision outcomes. There was a large pool of deferred applications for EDR. For these applications, 93% already had something comparable and sufficient in place. In addition, 48% of these applicants were at a 3 or higher (intermediary or higher current capability level). These applications will be reviewed to see if the localities were denied across the board or just for EDR. Applications for Secure Remote Network Access (SRNA) and Firewalls are currently in review. The review for SRNA will be completed by the end of November and for Firewalls will be completed by the end of December. For firewalls, cost and management are the challenge. Schools need Network Firewalls, but Web Application Firewalls (WAF) are easier to implement. Ms. Fain added that they will be working with applicants to see if WAF is an option to minimize costs. There was discussion on who would manage the WAF. Chair Watson noted that the locality SOC would provide advice and general information, but the localities would manage this. Ms. Fain reported that there were currently no concerns regarding implementation status. The timeline for the project areas EDR and response vulnerability, asset inventory, and secure remote access firewalls was reviewed. The implementation roadmap was then presented to the committee from Virginia Cybersecurity Plan through to Virginia Cybersecurity Ecosystem. A discussion was held on whether there was a possibility of Virginia taking on additional funds that have been unspent by other states in their grant programs. Chair Watson stated that it is a discussion that can be addressed later about re-allocation of those funds. The committee then discussed how to reach out to localities on firewalls. Chair Watson noted that there will be internal discussion first, and then we can reach out to the localities to discuss options. If there is a re-allocation of funds, this would be ideal to implement these larger purchases. Ms. Fain added that there needed to be further conversations with rural localities to determine project viability.

Public Comment Period:

There were no public comments.

Other Business:

Chair Watson opened the floor for other business. There was a discussion about the board responsibilities for the upcoming legislative session. It was also noted that a federal bill is currently pending to extend the State and Local Cybersecurity Grant Program (SLCGP) with a 60/40 funding split.

There is currently a bill waiting to extend the SLCGP with a 60/40 split. Ms. Ly confirmed that the next reappointment for seats on the committee is October 2026. Ms. Gauldin discussed travel forms and noted the November meeting is cancelled and that the next meeting is on December 11 at 10am. Ms. Gauldin circulated the dates for the committee meetings in 2026.

Adjourn

Upon a motion by Major Dekeyser and duly seconded by Ms. Doherty, the Committee meeting was adjourned at 10:51 am.

Virginia Cybersecurity Planning Committee
December 11, 2025 - 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,

Call to Order:
A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:00 am. Mr. Watson welcomed the members. Mr. Watson welcomed a new member, Timothy Wyatt, who is replacing Michael Dent in the seat for local government.

Presiding:
Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present:
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, Virginia Department of Emergency Management
Charles DeKeyser, Major, Virginia Army National Guard
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Charles Huntley, Director of Technology, County of Essex

Members Participating Remotely:
Derek Kestner, Information Security Officer, Supreme Court of Virginia
Uma Marques, Information Technology Director, Roanoke County Government.
Wesley D. Williams, Executive Director of Technology, Roanoke City Public Schools
Timothy Wyatt, Director of Information Technology, County of York

Ms. Marques, Mr. Williams and Mr. Wyatt participated from their principal residences as it is more than 60 miles from the meeting location. Mr. Kestner participated remotely due to work-related commitments.

Members Not Present:
Brandon Smith, Chief Information Officer, Department of Elections
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black

Staff Present:
Mylam Ly, Policy & Governmental Affairs Manager, Virginia IT Agency
April Gauldin, Legal & Legislative Services Coordinator, Virginia IT Agency
Mary Fain, Director of Information Security Programs, Virginia IT Agency
Janet Logan, Project Manager, Virginia IT Agency

Review of Agenda:
Ms. Gauldin provided an overview of the agenda.

Readoption of Remote Participation Policy and Approval of Minutes:
As a physical quorum was not present, a vote to approve the minutes could not be conducted. These items will be carried forward to the agenda for the next meeting.

Finances

Ms. Fain presented the financial update. The program is well positioned for Phase 2 after having used a single tool across all domains to save costs. So far, 2 million dollars of Phase 2 monies have been fully spent, with 1.58 million dollars of 2023 Phase 2 monies spent. Ms. Fain stated that they are currently gathering quotes for ongoing maintenance for full service and the next generation of implementations.

Phase 2 Project Status

Ms. Fain discussed Phase 2 project status. Endpoint Detection Response (EDR) and Vulnerability workstream completed the consent process and entered the detailed planning phase. The asset and data inventory workstream has been moved from approvals to the consent process. The final workstream is secure remote access and firewalls, which is currently in the approvals process. Deferred applications were discussed and the potential for them to be accepted at a later date. For the EDR deferred applicants, some already have a toolset that is at or better than the selected tool. There may be a chance to revisit and have an opportunity to include deferred applicants if there is additional funding. Additionally, a second round for another product may be more attractive to deferred applicants and could potentially be another path. The introduction meeting with localities and implementation vendors is projected to be in January. Deployment is currently on track to be completed in March from a locality perspective. Asset inventory and Data inventory have a planned completion date of April 30th. There is currently not an update on secure remote access or firewall. Ms. Fain discussed the projected implementation timeline and reviewed the timeline for the projected areas. For EDR and vulnerability, detailed planning with the vendor is currently being wrapped up and will be deploying between January and April. EDR and vulnerability will be monitored in May and June and will be formally closed out in July. For asset and data inventory, detailed planning with selected vendors will begin in January. The overall project is targeted to closed by the end of June.

Phase 2 Projected Outcomes and Next Steps

Ms. Fain discussed in detail the Phase 2 applicants. Starting with all applicants, the capability improvement impacts indicate that most of the applicants can get to enterprise cybersecurity levels. The disaster recovery implementation will be tackled at a later stage because it involves communications for recovery and that is different from the other technical solutions that are currently being worked on. It is not certain if it will have a scaled implementation and what the execution paths will be, whether some sort of large contract or a direct pass through. The Phase 2 applicants that were approved are currently lower than enterprise security level but will be brought up to that level after implementation. For the assessment population post Phase 2 Implementation, a level two is the minimum but a level three is optimal. The locality SOC and locality ISO service related objectives will be addressed once the procurement finishes. There was a discussion about ongoing assessment to help with program support and the need for documentation and where the ongoing costs are going to come from. Members also discussed possible ways to increase locality participation with funding and education. The members then discussed what the exit plan looks like when we reach the end of the program. Members discussed the possibility of legislation and Chair Watson agreed that this is the point that this discussion needs to begin. Chair Watson asked the members to think of questions that they want to see asked of the localities to be able to monitor and assess after the initial implementation.

Public Comment Period:

There were no public comments.

Other Business:

Chair Watson opened the floor for other business.

Ms. Gauldin discussed travel forms. Chair Watson noted the next meeting will be January 21st at 10am and will be all virtual. Chair Watson also let the members know that the committee will be voting on a new Vice Chair in January. If any of the members are interested in the position, they were instructed to send that interest by email. If there are no interested members, Chair Watson will be picking a candidate

to be voted on at the next meeting. Chair Watson stated that the February meeting will most likely be cancelled.

Adjourn

Upon a motion by Ms. Carnohan and duly seconded by Mr. Kestner, the Committee meeting was adjourned at 11:12 am.

VIRGINIA IT AGENCY

State and Local Cybersecurity Grant Program

Cybersecurity Plan Capability Assessment Project Update

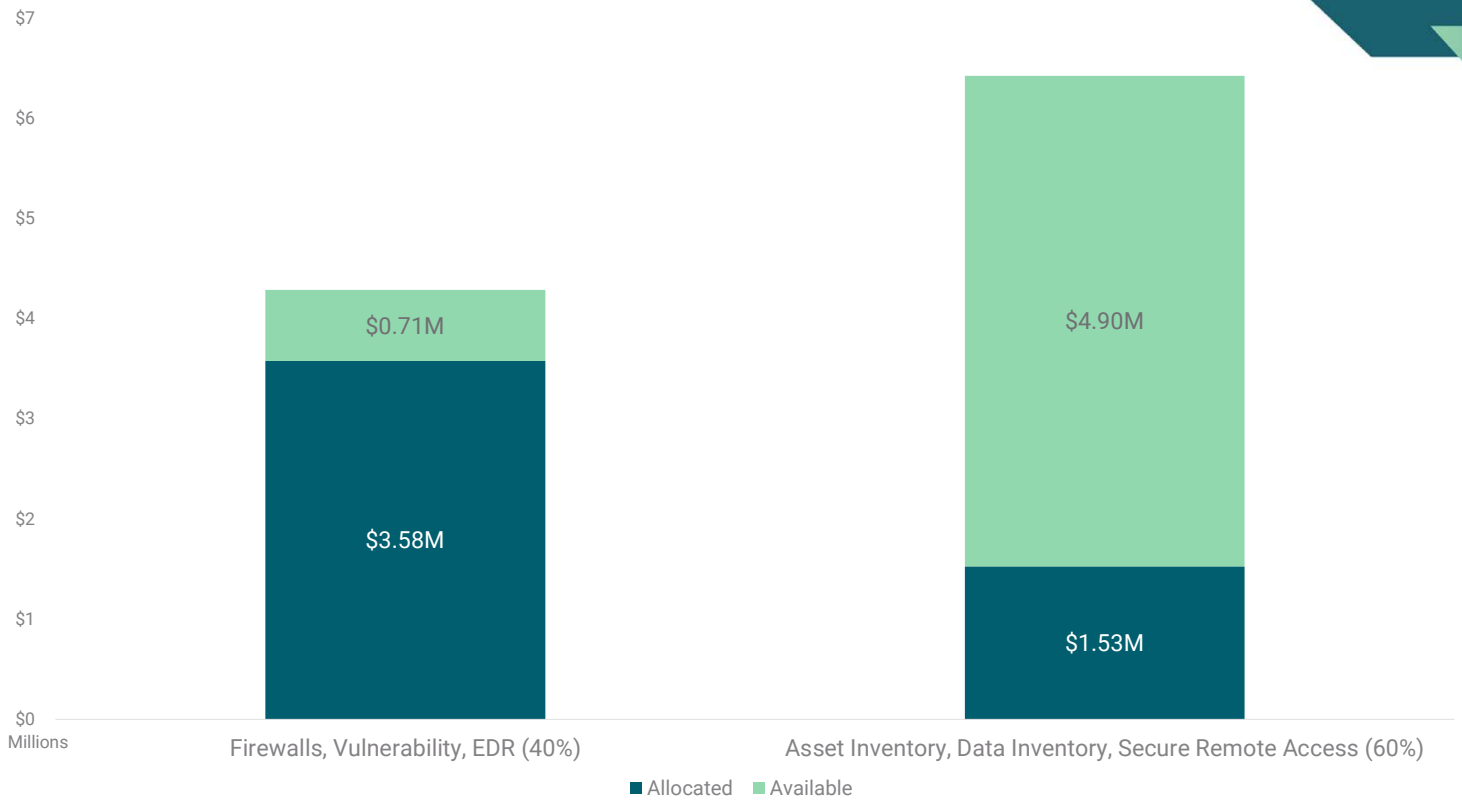
Jan. 21, 2025

Financial Update

Financial Update

Program Year	Total Award	Federal	State Cost Share	Cost Share %	Program Category	Category Amount	Project	Project Budget	Project Budget by State Fiscal Year 2024	2025	2026	2027	2028
1 (FFY 22) Period of Performance: Dec. 1, 2022 - Nov. 30, 2026	$ 4,768,252	$4,291,426	$ 476,826	10%	M&A (5%)	$ 238,413	M&A	$ 238,413	$74,146	$ 164,267			
					Statewide (15%)	$ 715,238	Locality SOC	$ 702,963			$ 702,963		
							Cybersecurity Plan and Assessments	$ 9,600		$ 7,691	$ 4,584		
					Local (80%)	$ 3,814,602	Cybersecurity Plan and Assessments	$ 12,275		$ 58,120			
							Assessment Project	$ 1,798,520		$1,750,001			
							Phase 2	$ 2,006,482			$2,006,480		
2 (FFY 23) Period of Performance: Dec. 1, 2023 - Nov. 30, 2027	$ 10,890,904	$8,712,723	$2,178,181	20%	M&A (5%)	$ 544,545	M&A	$ 544,545			$ 181,515	$ 181,515	$ 181,515
					Statewide (15%)	$ 1,633,636	Locality SOC	$ 1,123,636			$ 374,545	$ 374,545	$ 374,545
							Oversight and Program Management	$ 510,000			$ 170,000	$ 170,000	$ 170,000
					Local (80%)	$ 8,712,723	Phase 2	$ 8,712,723			$2,904,241	$2,904,241	$2,904,241
3 (FFY 24) Period of Performance: Feb. 1, 2025 - Jan. 31, 2029	$ 9,355,430	$6,548,801	$2,806,629	30%	M&A (5%)	$ 467,772	M&A	$ 467,772					
					Statewide (15%)	$ 1,403,315							
					Local (80%)	$ 7,484,344							
4 (FFY 25) Projected Period of Performance: Sept. 1, 2025 - Aug. 31, 2029	$ 3,571,752	$2,143,051	$1,428,701	40%	M&A (5%)	$ 178,588	M&A	$ 178,588					
					Statewide (15%)	$ 535,763							
					Local (80%)	$ 2,857,402							

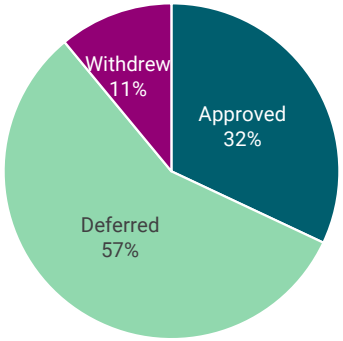
Phase 2 Allocation Tracking



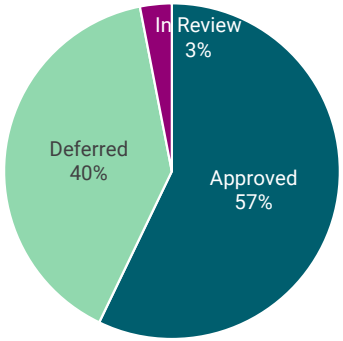
Phase 2 Update

Phase 2 Application Decision Outcomes

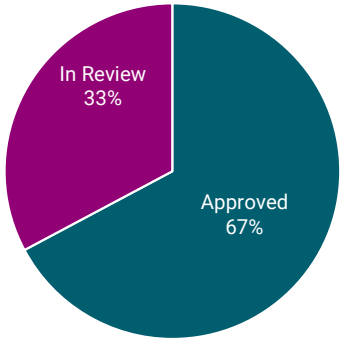
EDR



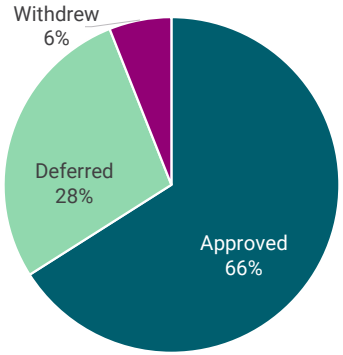
Asset Inventory



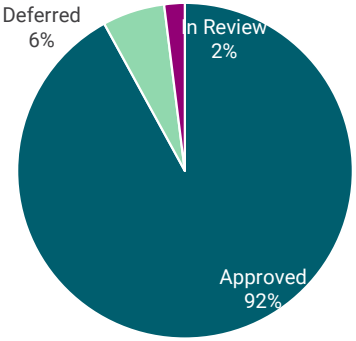
Secure Remote Network Access



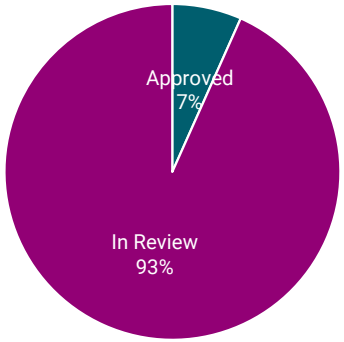
Vulnerability



Data Inventory



Firewalls



Decision Criteria
Current capability = 0 - 1
Future capability = 3 - 4
Likeliness of Success = High or application review indicated likeliness of success

Status Update: EDR and Vulnerability Management

EDR	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Full Service	11	100%	73%				N/A	43%	43%	3/31/2026	
Implementation	3	100%	67%			N/A		42%	42%	3/31/2026	
Contract Only	2	100%	100%		N/A	N/A		50%	50%	3/31/2026	
Additional licenses	3	100%	100%		N/A	N/A		50%	50%	3/31/2026	
Pass-through project	0	100%	N/A	N/A	N/A	N/A	N/A	100%	100%	3/31/2026	

Vulnerability	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Full Service	35	100%	100%				N/A	50%	50%	3/31/2026	
Implementation	16	100%	75%			N/A		35%	44%	3/31/2026	
Contract Only	2	100%	100%		N/A	N/A		50%	50%	3/31/2026	
Additional licenses	4	100%	100%		N/A	N/A		50%	50%	3/31/2026	
Pass-through project	1	100%	100%			N/A	N/A	50%	50%	3/31/2026	

Significant changes since prior report

None

Path to Green

Project	Path
N/A	N/A

Status Update: Asset Inventory and Data Inventory

Asset Inventory	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Asset Discovery	40	100%	60%				N/A	32%	35%	6/30/2026	
CMDB	32	100%	84%			N/A		37%	40%	6/30/2026	
ITAM	41	100%	60%		N/A	N/A		40%	41%	6/30/2026	
ITSM	37	100%	62%		N/A	N/A		41%	43%	6/30/2026	
Network Monitoring	40	100%	60%		N/A	N/A		40%	42%	6/30/2026	
Software Asset Mgmt	43	100%	81%			N/A	N/A	45%	47%	6/30/2026	

Data Inventory	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Data Discovery	43	100%	60%				N/A	32%	35%	6/30/2026	
Data Loss Prevention	44	100%	70%			N/A		34%	38%	6/30/2026	
Data Loss IR	41	100%	61%		N/A	N/A		40%	43%	6/30/2026	
Device Encryption & Data Protection	40	100%	58%			N/A	N/A	40%	42%	6/30/2026	

Note: A total of **61** applications were approved for asset inventory and **54** for data inventory. Each project area has multiple sub-areas. A locality may be approved for one or more sub-areas. The tables above provide a breakdown of each the applications for each sub-area.

Significant changes since prior report

Initial report

Path to Green

Project	Path
N/A	N/A

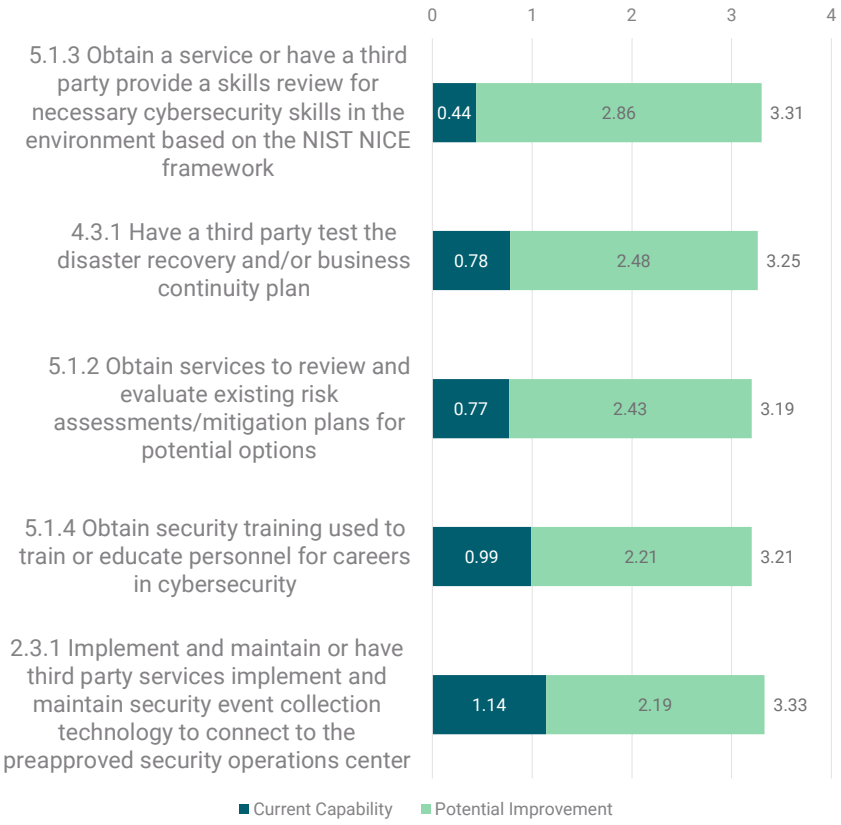
Phase 2 Projected Implementation Timeline

Project Area	January	February	March	April	May	June	July	August	September	October	November
EDR	Deployment				Maintenance		Close				
VM	Deployment				Maintenance		Close				
Asset Inventory		Detailed Planning		Deployment			Maintenance		Close		
Data Inventory		Detailed Planning		Deployment			Maintenance		Close		
SRNA				Detailed Planning	Deployment			Maintenance	Close		
Firewalls				Detailed Planning	Deployment			Maintenance	Close		

Phase 3 Discussion and Recommendations

Areas of Consideration for Phase 3

Top 5 Improvement Opportunities Based on Capability Assessments



*Survey areas of opportunity selected based on grant performance measure categories, prior VCPC discussions, exclusion of current projects, and assessment results

Survey Rankings

Rank	Area of Opportunity*
1	Reviewing cybersecurity skills for your environment based on the NIST NICE framework
2	Training used to educate and prepare existing personnel for cybersecurity roles and responsibilities
3	Reviewing and evaluating existing risk assessments/mitigation plans for potential options
4	Developing a disaster recovery plan
5	End-user cybersecurity awareness training
6	Conducting tabletop exercise(s) for disaster recovery/business continuity
7	Data encryption for data at rest
8	Migrating to the .gov domain

Other Prioritization Areas – Free Text Response

- ~27% of respondents provided responses to the question "Are there any other areas for prioritization consideration that were not listed above"
- Top themes:
  - Governance and policy, such as NIST-aligned policies, documentation templates, standard operating procedures, data governance
  - Operations and monitoring – Tier 3 NOC to assist with alerts and traffic analysis, log reviews, tracking, audit readiness

Appendix

Virginia SLCGP Implementation Roadmap

Virginia SLCGP Implementation Roadmap