Virginia Cybersecurity Planning Committee

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Financial Update	Mary Fain
Phase 2 Updates	Mary Fain
Phase 3 Discussion and Recommendations	Discussion, led by Chair
Vote on Authorization of Spending	Staff
Public Comment Period	
Other Business	Staff
Adjourn	

Virginia Cybersecurity Planning Committee
January 21, 2026 – 10:00 a.m.
Virtual

Call to Order:
A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:01 am. Mr. Watson welcomed the members.

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

Members Participating Remotely:
Troy Adkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe
Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
Robbie Coates, Director of Grant Programs, Virginia Department of Emergency Management
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Charles Huntley, Director of Technology, County of Essex
Derek Kestner, Information Security Officer, Supreme Court of Virginia
Chris Mowry, Chief Information Technology Officer, Virginia State Police
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
Wesley D. Williams, Executive Director of Technology, Roanoke City Public Schools
Timothy Wyatt, Director of Information Technology, County of York

Members Not Present:
Charles DeKeyser, Major, Virginia Army National Guard
Uma Marques, Information Technology Director, Roanoke County Government
Brandon Smith, Chief Information Officer, Department of Elections

Staff Present:
Jaime Hoyle, Director of Legal and Legislative Services, 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
Matthew Umphlet, Security Solutions Manager, Virginia IT Agency

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

Project Updates
Financial Update
Ms. Fain presented the financial update. There are no significant changes for the finance update. Program Year 4 and award amounts for this year were added at $3.6M for total award, with 40% cost share for the state in year 4. The asset and data inventory allocations will have updated numbers in the coming months. Chair Watson confirmed that the allocated monies committed for spending. The available funds represented are not yet committed

Phase 2 Update

Ms. Fain shared that Asset Inventory, Data Inventory and Secure Remote Network Access are in the review and approval stage. More insight into the reasons for deferment of localities within the Asset Inventory area will be given at the next committee meeting. Firewall has the potential to be the largest expenditure. Ms. Carnohan inquired whether the firewall projects would include both hardware and software. Chair Watson stated that they may include both, but given the costs often associated with hardware, we will determine appropriate approval amounts, potentially based on providing an equal percentage or flat amount for devices. Endpoint Detection Response (EDR) and Vulnerability project status is green and within our threshold of plus or minus 10 percent variance. The selected implementation partner is moving forward with approved localities with signed consent agreements to begin the steps necessary to deploy the tools. The EDR project has 5 consent agreements outstanding and we must have these within a short timeframe to move forward. If that does not happen, they will be removed from the project deployment list. There has been a significant growth for signed consent and notifications in Asset and Data Inventory and this remains on track with the timeline.

Phase 3 Discussion and Recommendations

Ms. Fain presented the top five opportunities for improvement based on capability assessments. These areas of growth include NIST/NICE framework, Disaster Recovery (DR) continuity plan and third-party testing, risk assessments and mitigation planning, training for security personnel (to become cybersecurity specialists), and SOC implementation. Localities were sent a survey to rank the most important areas for them moving forward and they were NIST/NICE framework, cybersecurity role training, risk and mitigation planning, DR recovery, data encryption for at-rest data, and migrating to the .gov domain.

In response to the localities survey, 27% filled in an open text response. A few responses overlapped, but included governance and policy related issues, templates, standard operating procedures, data governance, and operations and monitoring. Chair Watson noted that there are disparate needs for localities, but that it was expected and that we need to get a more diverse set of responses from places like local education entities. He also stated that legislation concerning migrating to .gov domains might be something that is necessary from the General Assembly and is where a funding effort might be decided to maintain the .gov presence. The committee was asked to review these ideas for the next meeting so that a vote for investment decisions for Phase 3 can be made.

Approval of Electronic Participation Policy:

The policy was displayed on the screen and summarized by Ms. Gauldin. Upon a motion by Ms. Waller and seconded by Ms. Carnohan, the Committee unanimously voted to adopt the updated electronic participation policy.

Approval of Minutes:

The August 19, October 21, and December 11 meeting minutes were displayed on the screen. Upon a motion by Mr. Williams and seconded by Ms. Carnohan, the committee unanimously voted to approve all three meeting minutes.

Annual Review of Cybersecurity Plan:

Ms. Gauldin provided an overview of the changes to the cybersecurity plan. The edits were largely administrative non-substantive edits including:

- Beginning on the front page renaming the version and the date on the cover page of the document
- Updating the members of the committee
- Removing the Table of Contents
- Removing Web Application Scanning from CISA Services-this was removed from required services as of the 2023 NOFO

Upon a motion by Ms. Waller and seconded by Ms. Carnohan, the Committee unanimously voted to adopt the amended Cybersecurity Plan.

Officer Elections:

Chair Watson led the nomination and election of the Board Vice Chair, with the newly elected individuals to assume their roles at the next meeting in February. As previously discussed, nominations were solicited, and the position was uncontested.

Mr. Timothy Wyatt was nominated for the position of Vice Chair. A motion was made by Ms. Waller and seconded by Mr. Huntley to approve Mr. Wyatt as Vice Chair. There was no discussion, and the motion carried unanimously.

Public Comment Period:

There were no public comments.

Other Business:

Mr. Watson opened the floor for other business. Ms. Carnohan asked if there had been any discussion about VCPC with the new administration. Chair Watson stated that reappointments will be needed in the fall, but that he is not expecting any issues to arise. Mr. Huntley stated that he had received a reappointment email from the Secretary of Administration's office, but none of the other members stated that they had received it.

Mr. Watson noted the next meeting would be on February 18th, but that it may be cancelled dependent on updates available by then.

Adjourn

Upon a motion by Mr. Wyatt and seconded by Ms. Carnohan, the Committee meeting was adjourned at 10:47am.

VIRGINIA IT AGENCY

VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT

State and Local Cybersecurity Grant Program

Cybersecurity Plan Capability Assessment Project Update

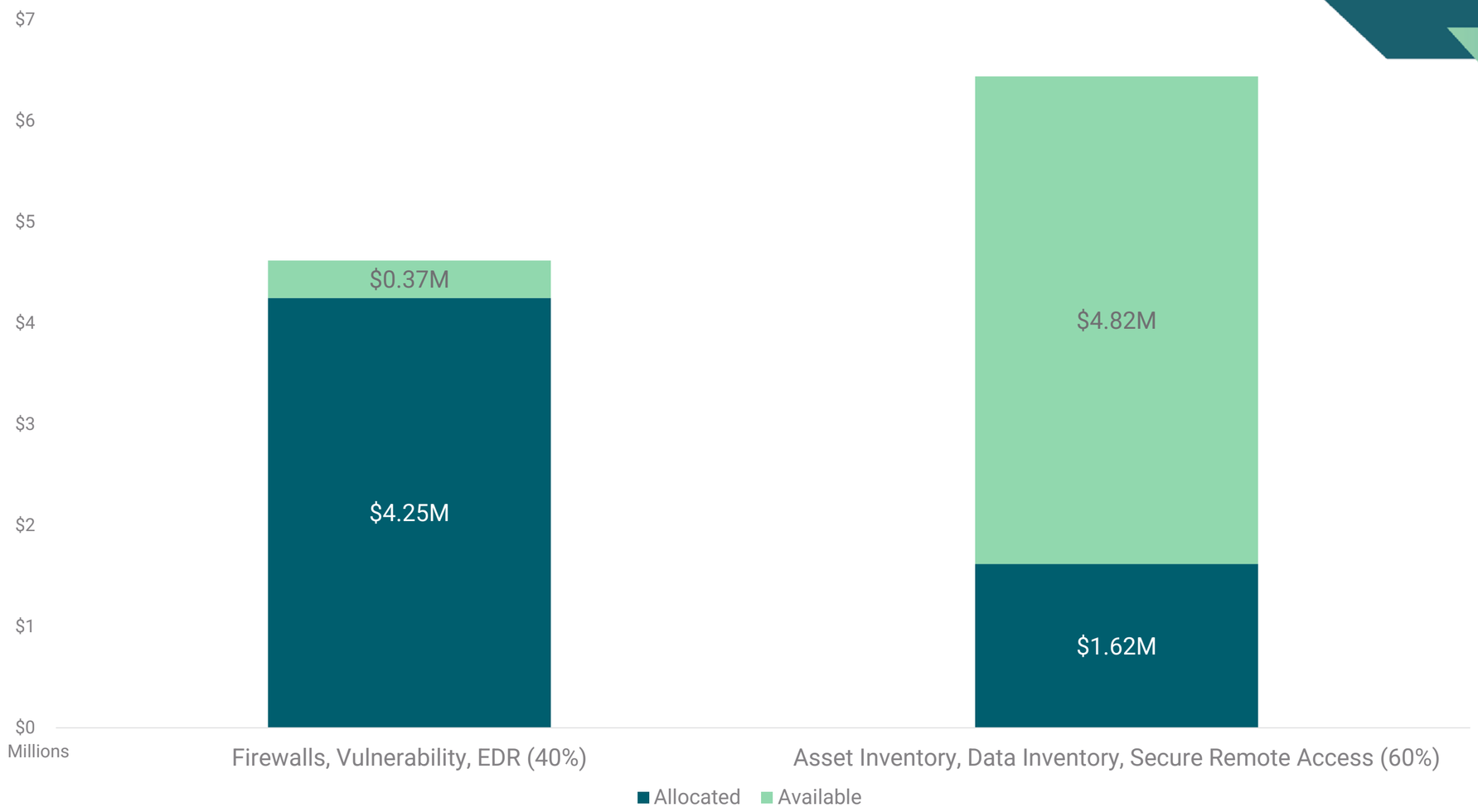
March 18, 2026

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							

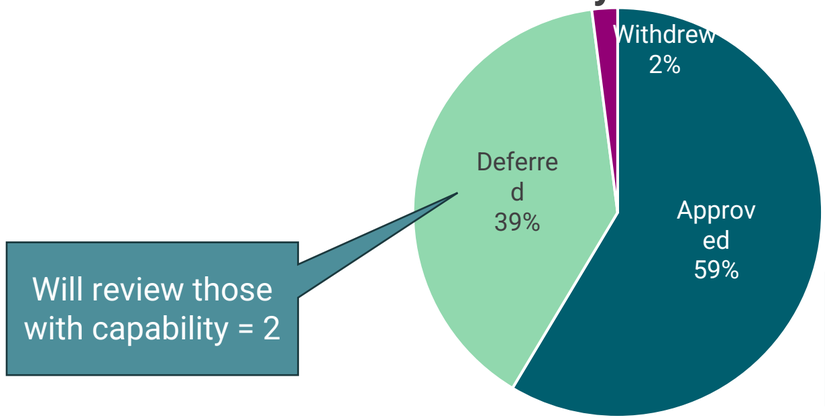
Phase 2 Allocation Tracking



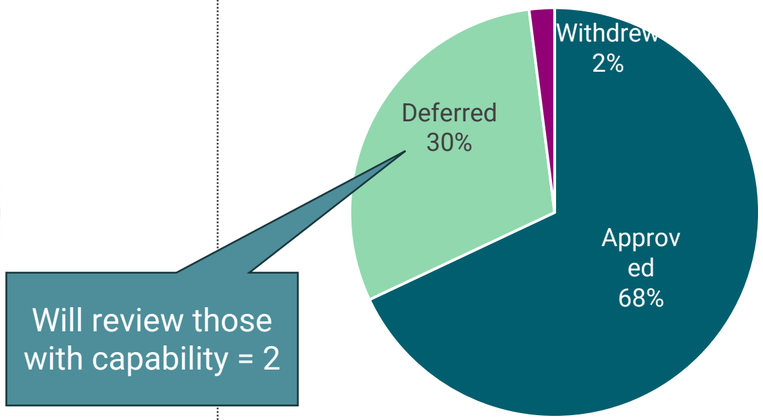
Phase 2 Update

Phase 2 Application Decision Outcomes

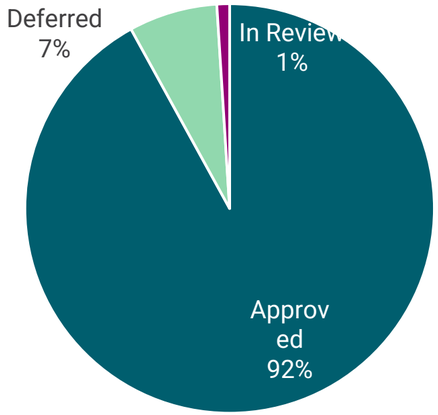
Asset Inventory



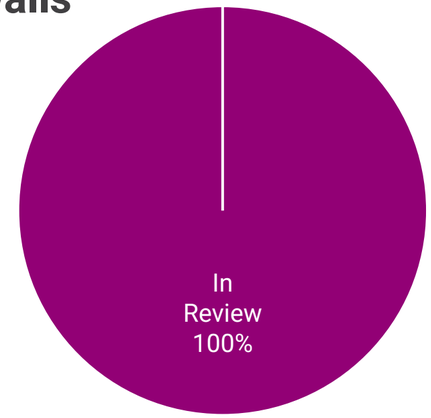
Secure Remote Network Access



Data Inventory



Firewalls



<u>Decision Criteria</u>
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

Deployment Pipeline Progress

Vulnerability

Pilot Initiated	Pilot Complete	Prod Deploy Initiated	Production Complete
95%	80%	80%	29%

12 localities complete

Endpoint Detection and Response

Pilot Initiated	Pilot Complete	Prod Deploy Initiated	Production Complete
82%	73%	55%	9%

1 locality complete

Progress vs. Actual

- On target to meet March 30 goals for both tools for majority of localities

Summary to Completion

- March – Drive remaining production deployments to completion
- April – Finalize deployments for delayed localities, perform necessary training and system fine-tuning, execute deployment confirmation and validation

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%	70%				N/A	34%	35%	10/30/2026	
CMDB	32	100%	87%			N/A		37%	40%	10/30/2026	
ITAM	41	100%	62%		N/A	N/A		41%	41%	10/30/2026	
ITSM	37	100%	65%		N/A	N/A		41%	43%	10/30/2026	
Network Monitoring	40	100%	70%		N/A	N/A		43%	42%	10/30/2026	
Software Asset Mgmt	43	100%	85%			N/A	N/A	46%	47%	10/30/2026	

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%	10/30/2026	
Data Loss Prevention	44	100%	72%			N/A		34%	38%	10/30/2026	
Data Loss IR	41	100%	62%		N/A	N/A		41%	43%	10/30/2026	
Device Encryption & Data Protection	40	100%	60%			N/A	N/A	40%	42%	10/30/2026	

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

Path to Green

Project	Path
N/A	N/A

Status Update: Secure Remote Network Access

Secure Remote Network Access	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Zero Trust Network Access	46	100%					N/A	20%		7/31/2026	
Multifactor Authentication	39	100%				N/A	N/A	25%		7/31/2026	

Note: A total of **85** applications were approved for secure remote network access. 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

All award notifications have been communicated.

Path to Green

Project	Path
N/A	N/A

Phase 2 Projected Implementation Timeline

Project Area	March	April	May	June	July	August	September	October	November	December	January
EDR	Deployment		Maintenance		Close						
VM	Deployment		Maintenance		Close						
Asset Inventory	Detailed Planning			Deployment and Configuration (3 tools)							Maintenance
Data Inventory	Detailed Planning				Deployment and Configuration				Maintenance		Close
SRNA	Detailed Planning					Deployment and Configuration (2 tools)				Maintenance	
Firewalls	Detailed Planning						Deployment and Configuration				Maintenance

Locality SOC Awarded Feb. 24

- **Locality SOC awarded to five organizations**
- **10-day protest period is complete**
- **Contracts are available on the statewide contract website**
  https://vita.cobblestonesystems.com/public/
- **SLCGP will conduct selection and contract negotiation process for grant program SOC partner during Q2 2026**
  Applications for participation will open during this time. All application announcements will be published via VDEM's listserv. To join the listserv, visit Virginia Department of Emergency Management (govdelivery.com), enter your email address, and then select the **State and Local Cybersecurity Grants Program** from the list (near the bottom)

Phase 3 Discussion and Recommendations

Phase 3 – Data for Consideration

SURVEY RANKINGS

1. NIST NICE Cybersecurity Skills Review
2. Training for Existing Personnel — Cyber Roles
3. Developing a Disaster Recovery Plan
4. End-User Cybersecurity Awareness Training
5. Risk Assessments / Mitigation Plan Review
6. Tabletop Exercises — DR / Business Continuity
7. Data Encryption for Data at Rest
8. Migrating to .gov Domain

FREETEXT THEMES

Zero Trust Architecture
5 respondents cited ZTA/ZTNA as a priority

Vulnerability Management
Pen testing, vulnerability reporting, patch mgmt

Policies and Documentation
NIST-based policies, SOPs, network architecture docs

Firewall and Infrastructure
Next-gen firewalls, firewall policy reviews

Incident Response and DR
Formalized DR planning, BIA development

Staffing and Services
Staff augmentation, MDR/managed services need

EDR / Platform Migrations
EDR vendor migration, M365 licensing

Network Monitoring
Lateral traffic monitoring, network visibility

ASSESSMENT CAPABILITY GAPS

Sub-Obj	Focus Area	Current	+Δ Gain	Total
5.1.3	Workforce Dev.	0.44	2.86	3.31
4.3.1	Threat Intelligence	0.78	2.48	3.26
5.1.1	Workforce Dev.	0.84	2.47	3.31
3.7.3	Network Security	1.16	2.19	3.34
2.4.1	Asset Management	1.09	2.09	3.18
1.3	Software Life cycle	1.33	1.96	3.30
3.9.2	Patch Management	1.34	1.96	3.30
4.1.1	Data Recovery	1.44	1.94	3.39

Data Informing Scope – Virginia Cybersecurity Plan Sub-Objectives and Metrics

Program Objectives	Program Sub-Objectives	Associated Metrics	Metric Description
5.1 Identify security gaps associated with program objectives which can be supported by the grant program	5.1.3 Obtain a service or have a third party provide a skills review for necessary cybersecurity skills in the environment based on the NIST NICE framework		
4.3 Implement disaster recovery and data recovery testing	4.3.1 Have a third party test the disaster recovery and/or business continuity plan	Successful recovery within plan established time frame	Frequency: Once Source: Disaster recovery plan information
5.1 Identify security gaps associated with program objectives which can be supported by the grant program	5.1.1 Have staff augmentation provide an assessment or have a third-party assessment of the technology environment for services supported by the grant program	Assessment completion within 120 days	Frequency: Quarterly
3.7 Centralized authentication and authorization (single sign-on)	3.7.3 Manage or have a third party manage single sign on solutions	Number of organization users with single sign on Number of Virginians with single sign on	Sources: User access list Frequency: Monthly
2.4 Audit log collection for all servers and systems hosting data in accordance with log management standards.	2.4.1 Establish data collection points for system audit logs	% of systems reporting logs % of event log sources compliant with standards	Frequency: Monthly Source: Asset inventory and log collection system
1.3 Upgrade or replace all software no longer receiving security maintenance/support.	1.3 Implement staff augmentation or third-party services to assess and/or upgrade software without support for security updates.	100% of targeted devices are updated	Frequency: Monthly Source: # of targets / # of upgrades
3.9 Ensure patch management program is implemented and up to date	3.9.2 Obtain licenses for vulnerability management software	Hosts scanned within 30 days Hosts updated to supported software within n-1 of most recent release	Source: Vulnerability software and asset inventory Frequency: Monthly
4.1 Establish and maintain a data recovery process	4.1.1 Develop or have a third party develop a business continuity plan and/or disaster recovery plan that enables the recovery of critical information systems that support business processes for all cloud based and locally stored data.	100% of Critical services will be brought online within 72 hours	Source: Asset inventory Frequency: Once

Phase 3 Options

A Workforce Development and Cybersecurity Training

- Highest-impact capability gaps: 5.1.1 & 5.1.3 (+2.47–2.86 improvement potential)
- Directly addresses Survey #1 (NIST NICE skills review) and #2 (personnel training)
- Builds internal capacity, reducing long-term reliance on contracted services
- *Discussion: Training outcomes*

B Patch Management Program

- Freetext explicitly cited patch management as a combined priority with pen testing
- Closes the remediation gap in the vulnerability lifecycle — identify, detect, and fix
- Sub-objective 3.9.2 (Patch Management) now appears directly in capability gaps — current 1.34, improvement +1.96
- *Discussion: Resources for "catch-up" vs. tool*

C Risk Assessment, Vulnerability and Pen Testing

- Supported by all three data sources
- Survey #5: Reviewing existing risk assessments / mitigation options; freetext: pen testing, BIA
- Aligns with sub-objectives 1.3 (software life cycle, +1.96) and 4.3.1 (threat intel, +2.48)

D Incident Response Planning and Resilience Exercises

- Would include SOC onboarding
- Survey #3 (disaster recovery plan) and #6 (tabletop exercises) both in top 6 priorities
- Freetext: Formalized DR planning, Business Impact Analysis, incident response capabilities
- Aligns with sub-objectives 4.1.1 (data recovery, +1.94) in capability gaps table

Projected Timeline for Phase 3 Decisions

April
- Application development and launch

May - June
- Application completion

June VCPC meeting
- Review preliminary application data
- Determine funding allocation

July VCPC meeting
- Final application data review

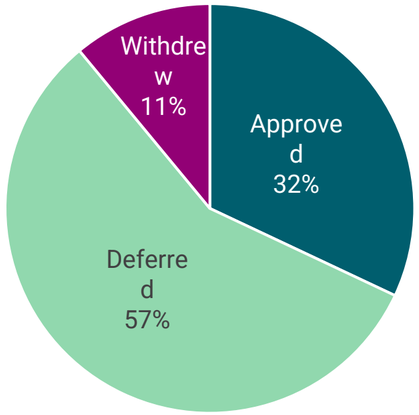
August VCPC meeting
- Funding allocation adjustments, if needed

September
- Potential launch of new project(s)

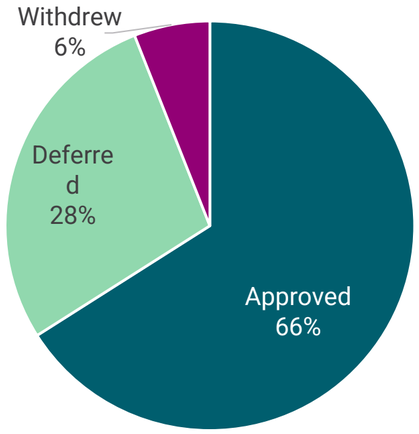
Appendix

Phase 2 Application Decision Outcomes

EDR



Vulnerability



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

VIRGINIA IT AGENCY

Virginia state and local cybersecurity grant program roadmap