Virginia Cybersecurity Planning Committee

Agenda

Call to Order and Welcome	Mike Watson Chief Information Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Financial Update	Mary Fain
Phase 2 Updates	Janet Logan
Survey Results	Mary Fain
Phase 3 Follow Up	Discussion, led by Chair
Post Federal Grant Planning	Discussion, led by Chair
Public Comment Period	
Other Business	Staff
Adjourn	

Virginia Cybersecurity Planning Committee
March 18, 2026 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,
Richmond, VA, 23225

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 Present:
Timothy Wyatt, Committee Vice Chair, Director of Information Technology, County of York
Troy Adkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe
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
Brandon Smith, Chief Information Officer, Department of Elections
Wesley D. Williams, Executive Director of Technology, Roanoke City Public Schools

Members Not Present:
Robbie Coates, Director, Grant Management and Recovery, Virginia Department of Emergency Management
Derek Kestner, Information Security Officer, Supreme Court of Virginia
Uma Marques, Information Technology Director, Roanoke County Government.
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black

Staff Present:
April Gauldin, Legal & Legislative Services Coordinator, Virginia IT Agency
Mary Fain, Director of Information Security Programs, Virginia IT Agency
Jaime Hoyle, Director of Legal and Legislative Services, Virginia IT Agency
Ephfrom Walker, Legal Compliance and Policy Specialist, 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 January 21 meeting minutes were displayed on the screen. Upon a motion by Mr. Williams and duly seconded by Mr. Smith, the committee unanimously voted to approve the January 21 meeting minutes.

Finances
Ms. Fain presented the financial update. There are no significant changes from the last meeting. With regards to allocation tracking, firewall, vulnerability and Endpoint Detection Response (EDR) are allocated $4.25 million, with $370, 000 available. For Asset and Data inventory and Secure Remote Access, $1.62 million is allocated with $482,000 available. The increase in firewalls, vulnerability, and EDR is to reflect the contractor support costs associated with full-service support. Chair Watson noted that Firewall tools are in process and that suppliers have been giving good pricing deals with a long-term business outlook

for when localities eventually take over. He appreciates the cooperation from the private sector and is hoping for that for the remainder of the negotiations. We are currently finalizing pricing for Asset Inventory tools that have been identified to allow us to cover the six domains with three tools. Tool minimization whenever possible is also the plan for Data Inventory. Looking ahead, the numbers will flip when allocated and implementation costs are included in the next update. The only concern is that of Federal reimbursement-with the possibility of pulling from Commonwealth funds during the current shutdown Department of Homeland Security (DHS). We will have to pivot if the freeze continues.

Phase 2 Project Update

Ms. Fain discussed Phase 2 project status. Applications are being reviewed for decision statuses (approved/deferred). Asset inventory is at 60% approved, firewalls are currently in review, data inventory is 92% approved, Secure Remote Network Access (SRNA) is at 68% approved. Thirty applications have been deferred but will be reviewed with capacity. Both Asset Inventory and SRNA deferred applications are driven by their current state capability levels. After the Asset Inventory, Data Inventory, and SRNA pricing is completed, the final amount will be det for final decisions on firewalls and asset review. For EDR and Vulnerability Management, we are currently working with a third party who is working with localities to get it out into the environments. During the deployment pipeline, a pilot will be initiated first, followed by the production environment. Vulnerability Management is 95% pilot initiated, with 80% of the pilot complete, 80% of the production initiated, and 29% of the production complete. EDR is 82% pilot initiated, 73% pilot complete, 55% production initiated, and 9% production complete. We are currently on target to meet the March 30 goals for both tools for the majority of localities. In April, the deployments for delayed localities will be finalized and necessary training and system fine-tuning will be performed with deployment confirmation and validation. Asset and Data Inventory are currently in the process of completing decisions and signed consent agreements are being received. Soon the process to choose implementation vendors will begin. The consent process for Zero Trust Network Access (ZTNA) and Multifactor Authentication will begin later this month. The process will be staggered so as to not overwhelm localities. Asset Inventory, Data Inventory, SRNA, and Firewalls are sticking to a 90-day deployment with a contingency window. Detail planning and Statement of Work (SOW) with implementation partners will wrap up at the end of June. The Locality Security Operations Center (SOC) was awarded on February 24 to five organizations that have completed the 10-day protest period. The contracts are available on the statewide contract site. Selections and contract negotiations will be conducted for the grant program SOC partner during Q2 2026. Applications for participation, either by contracting your own or full service through VITA. Chair Watson mentioned that the Request for Product (RFP) process took longer than anticipated. These five entities will be contacted to set up structure for target audiences, requests for joining SOC and collecting inventory. Mr. Wyatt asked if the federal grants for hardware allocations can be communicated to the localities. Chair Watson stated that hardware will have to be tied to option 4 or 5 or a reimbursement option. The risk of complications is high, so we won't do full implementation with these entities.

Phase 3 Discussion and Recommendations

Ms. Fain presented data for consideration concerning Phase 3. A survey was sent out to localities, state government, and education and over 100 responses were received. The survey asked respondents to rank a set list of items for consideration during Phase 3 and included a free text field. The survey rankings were consistent, with NIST/NICE assessment skill review and skill gaps for cyber roles taking the top two spots and going hand in hand. Developing a Disaster Recovery Plan rose towards the number 3 ranking closer to the end of the survey period. Included in the free text themes were Zero Trust Architecture, Vulnerability Management and Policies and Documentation. The assessment capability gaps showed a theme of skills assessment, disaster recovery (DR) testing, and single sign-on.

Ms. Fain presented four options for Phase 3. Option A is Workforce Development and Cybersecurity Training; this includes training options for outcomes and aligns with the Notice of Funding Opportunity (NOFO). Option B is Patch Management Program; this provides resources for "catch up" vs. tools and helps close vulnerability management. Option C is Risk Assessment, Vulnerability and Penetration

Testing; this option hits all the data sources. Option D is Incident Response Planning and Resilience Exercises; this option will most likely be folded into the SOC onboarding.

Chair Watson explained that the technical tools are out, and they are recognizing that organizations need help with personnel and training/soft skills and remediation. Workforce development and training came through as a top choice on the surveys from respondents. Chair Watson stated that we could do regional training with FEMA or virtual/computer-based training, but suggested that is probably not the best choice. Chair Watson asked the committee what makes the most sense in this case. Mr. Williams asked how much money was allocated for this process. He elaborated that for Option A, the monies could be paid for 3-year personnel that would work on identifying and training. This option might not be relevant to the environment. A separate survey might be needed to find out what key training skills are needed in the environment. Another option is a roving cyberteam that would go to each locality and do the work. Part of the problem is capacity, and this does not fix this and may not fill this need. Chair Watson noted that he was surprised that this option was chosen first because he thought localities would want an individual person as the security person, but in practice, this could be difficult as they would be down a resource. There are many options for segmenting tasks and having multiple sessions in different locations. The most difficult aspect would be resourcing and staffing. Major Dekeyser suggested not having someone to come in to do the work for them but perhaps have someone to come in to assess what needs to be done and plan workforce development. Ms. Doherty had concerns about training to what end, to get to the SOC, and any other skilled firewall and cyber issues that may arise. Mr. Huntley noted that having a system administrator in a training program creates challenges locality implementation, especially in smaller localities. Ms. Carnohan suggested that we implement in three phases, similar to what we have already done for this project. Breaking down the training into full service, implementation, and contract addresses the different needs of localities, otherwise the process might not work for every locality and environment. Chair Watson asked if we need to go back out with an additional survey to get more information and more details for the localities. The committee agreed that it was necessary. Chair Watson broke that down into staff augmentation, specific training or broad training. Mr. Huntley asked if there was a breakdown in trends between the size differences of localities. Ms. Fain stated that the initial survey was basic and only broke down between local government and education. Chair Watson agreed that we need a new, more detailed survey because Phase 3 will use up the rest of the funds. The Pillar Act will continue 50% of the funding in theory, but it has still not passed. If it has not passed within the next 12-18 months, the committee will need to figure out other funding options. The new survey will be drafted and sent to the committee members for feedback. Ms. Carnohan suggested that there needs to be some sort of commitment from the people who are trained so that they don't leave within a short period of time after they receive the training. Chair Watson stated that the only problem with that would be that it might put the locality on the hook for funding, but it will be included in the new survey.

Chair Watson began discussing Option B, Patch Management Program. He asked if Vulnerability Management covers this or do we need additional support. For instance, do we need tools for patching or for catching up? Do we need tools for management or are we more comfortable with pass through tools? Ms. Carnohan commented that this is an everyday occurrence. Chair Watson suggested that we could allocate funds, for example the localities could get around five thousand dollars for a Windows upgrade, or do we have tech assistance come to the locality. Ms. Carnohan argued that this also goes back to staff augmentation of bringing someone in to come up to date. Chair Watson stated that the vulnerability life cycle is difficult to deal with and may be too large for localities to manage. Mr. Wyatt shared that he has seen that maintaining and then catching up is what he has seen mostly, which could include supplementing the complex, current patching needs. Chair Watson decided to add this issue to the new survey as well. Mr. Smith noted that once localities are caught up on patch management, there needs to be a Standard Operating Procedure (SOP) to maintain and that there might be the need for someone to go into the localities with that knowledge and help develop that. Chair Watson agreed and stated that can be added to the assessment and implementation plan.

Chair Watson moved to discuss Option C: Risk Assessment, Vulnerability and Penetration Testing. He argued that these items are core, but they only tell you what to do. If the localities don't have the resources, these items won't be completed. He also believes that these items are all foundational pieces of security architecture and asked if we want to include all these items. Major Dekeyser stated that penetration testing needs to stay and that tabletop exercises are needed that are designed for locality supervisors to be involved. Many committee members argued that locality board members will not attend these types of sessions due to time constraints. Another potential problem is that they don't understand the need, especially without funding. A suggestion is to have other locality supervisors share their experiences with ransomware attacks with their counterparts and why these items are important. Mr. Smith suggested having attendance in these events be a subset requirement to get funding in Phase 3. Chair Watson suggested that we could coordinate across the Commonwealth and do one giant exercise or some sort of regional gatherings. This could be used to dovetail assessment into that for localities and be used as a pitch to get more money from the General Assembly. Since this will deplete the rest of the money, we must position to get funds for localities through federal or state level. Major Dekeyser suggested that this includes a VIP Day with local decision makers to drive locality decisions regarding the funding for cyber needs. Chair Watson sees two problems at this point: funding/exposure and understanding the problem. Another piece is participation and prioritization by locality administrators for dedicated funds. We need to design marketing communication for what will be most convincing while still being sensitive to local issues to make sure this happens. Chair Watson also suggested that localities must be at a certain maturity level to be able to participate in Option C, otherwise it is not worthwhile for the locality. Option C could be pulled apart and divided into Options B and D. This will be looked at after the new survey with plans and money allocated.

Chair Watson discussed the options that will be included in the new survey to be sent out to localities. Ms. Fain will draft the questionnaire, and it will be sent to the committee for review before being sent to the localities.

Vote on Authorization of Scope:

Due to the need for additional information and the creation of a new, more detailed survey, the vote on authorization of scope for Phase 3 will be moved to a later meeting.

Public Comment Period:

There were no public comments.

Other Business:

Chair Watson opened the floor for other business. Mr. Williams asked if expediting the timeline for Phase 2 is an option, as his locality is ready to move forward more quickly. There is a concern for imminent threats that are emerging and it would be a benefit to have this in place. Chair Watson stated that we can't expedite because localities need time to finish out work during the summer. There is the potential to move those who are ready to move as they are prepared.

Ms. Gauldin discussed travel forms. Chair Watson noted the next meeting will be April 15th at 1pm, but could potentially be cancelled depending on the responses that we receive from the new survey.

Adjourn

Upon a motion by Mr. Wyatt and duly seconded by Mr. Adkins, the Committee meeting was adjourned at 11:33 am.

VIRGINIA IT AGENCY

VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT

State and Local Cybersecurity Grant Program

Cybersecurity Plan Capability Assessment Project Update

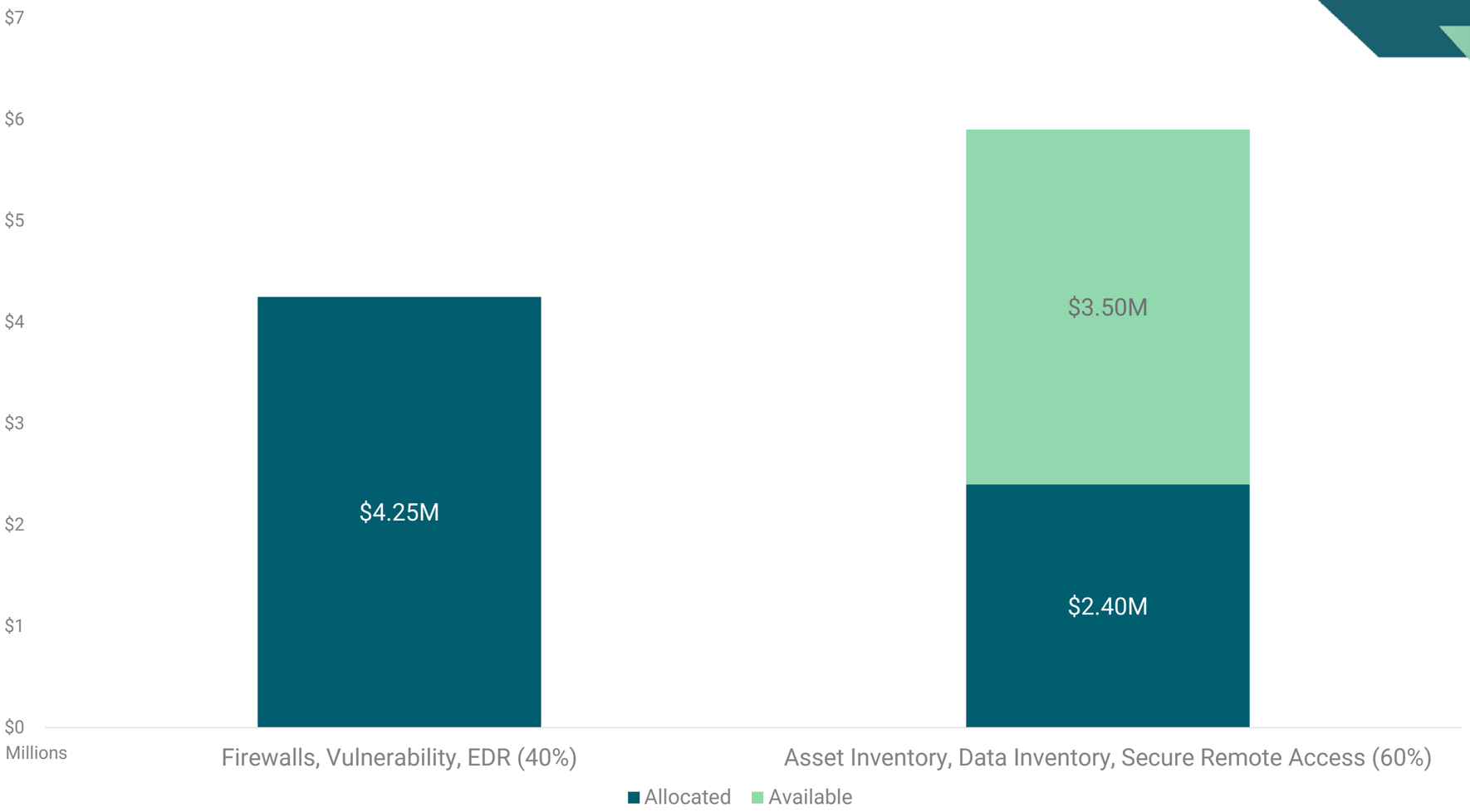
May 20, 2026

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							

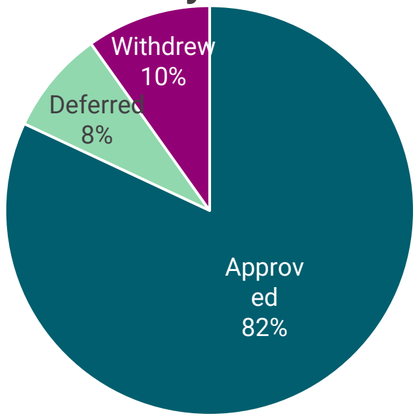
Phase 2 Allocation Tracking



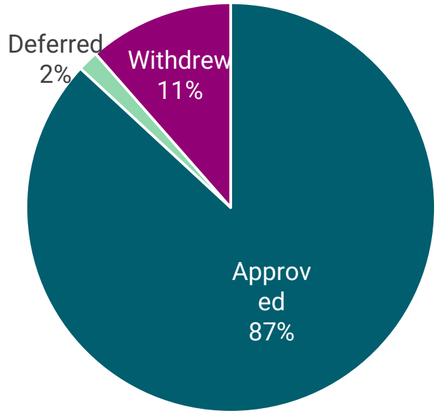
Phase 2 Update

Phase 2 Application Decision Outcomes

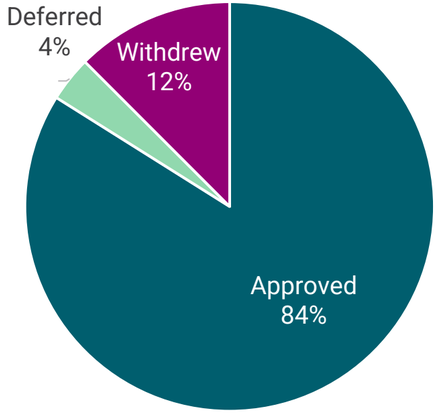
Asset Inventory



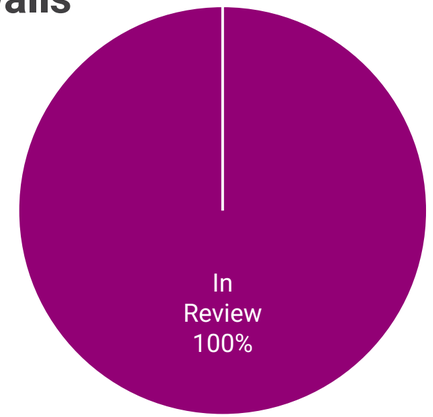
Secure Remote Network Access



Data Inventory



Firewalls

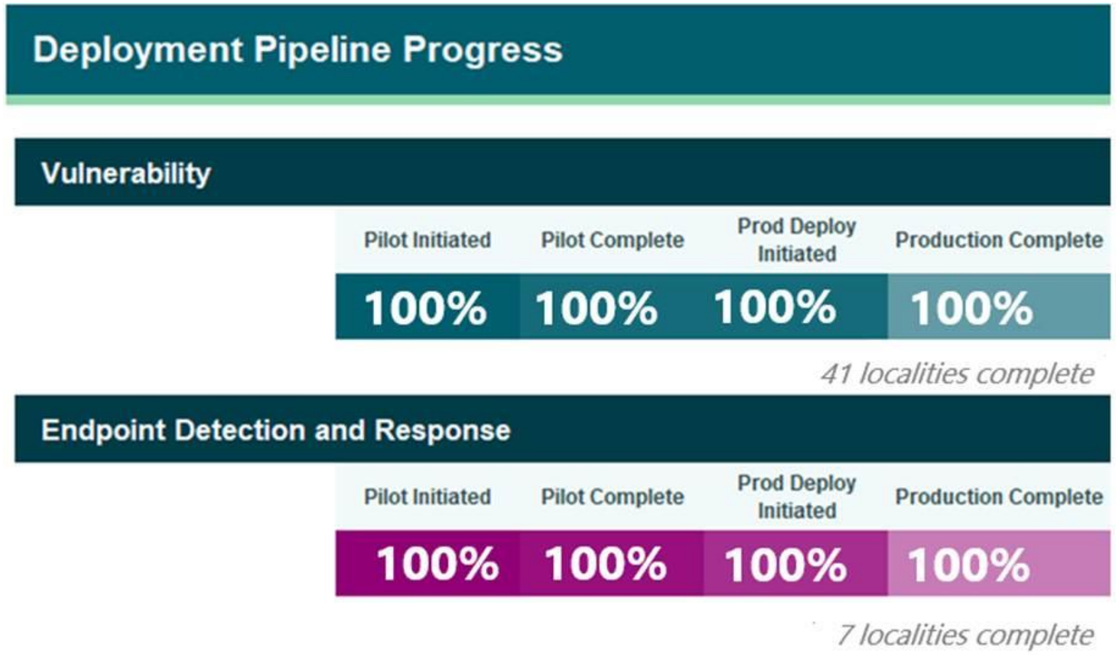


<u>Decision Criteria</u>
Current capability = 0 - 1
Future capability = 3 - 4
Likeliness of Success = High or application review indicated likeliness of success

Phase 2 Projected Implementation Timeline

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

Status Update: EDR and Vulnerability Management



EDR & Vulnerability Management Phase 2 Finalization

- All deployments finalized
- Training provided to all localities
- System fine-tuning performed as needed
- For EDR deployments, Falcon Complete was also deployed
- Deployment Confirmation and Validation conducted

Status Update: Asset Inventory and Data Inventory

Asset Inventory	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Total % Complete	Planned Completion Date	Status
Asset Discovery	39	100%	77%	50%			N/A	45%	12/31/2026	
CMDB	33	100%	73%	50%		N/A		45%	12/31/2026	
ITAM	43	100%	72%	50%	N/A	N/A		56%	12/31/2026	
ITSM	36	100%	78%	50%	N/A	N/A		57%	12/31/2026	
Network Monitoring	38	100%	68%	50%	N/A	N/A		55%	12/31/2026	
Software Asset Mgmt	42	100%	76%	50%		N/A	N/A	57%	12/31/2026	

Data Inventory	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Total % Complete	Planned Completion Date	Status
Data Discovery	40	100%	75%	30%			N/A	41%	11/30/2026	
Data Loss Prevention	39	100%	69%	30%		N/A		40%	11/30/2026	
Data Loss IR	37	100%	73%	30%	N/A	N/A		51%	11/30/2026	
Device Encryption & Data Protection	36	100%	72%	30%		N/A	N/A	51%	11/30/2026	

Note: A total of **50** applications were approved for asset inventory and **47** 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	Total % Complete	Planned Completion Date	Status
Zero Trust Network Access	39	100%	44%				N/A	29%	12/31/2026	
Multifactor Authentication	36	100%	47%			N/A	N/A	37%	12/31/2026	

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

Path to Green

Project	Path
N/A	N/A

Locality SOC Update

- **Selection and contract negotiation for grant program SOC in Progress**

- **CrowdStrike Falcon Complete will serve as in interim solution to the Locality SOC**
  - Enables monitoring to receive real-time alerts on suspicious end point activity.
  - Falcon Complete subscription will be in place for up to one year.

- **Applications for participation**
  Applications for participation will open during Q2 2026. 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 Options Reviewed During March 2026 meeting

A Workforce Development & 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 & 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 lifecycle, +1.96) and 4.3.1 (threat intel, +2.48)

D Incident Response Planning & 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

March Meeting Questions Addressed in the Survey

Training

- Which workforce approach best fits localities: training existing staff, staff augmentation, a roving cybersecurity resource, or a flexible model?
- Can localities realistically sustain a funded cybersecurity position or shared resource after the grant period ends?
- Can IT staff be released for training without disrupting day-to-day operations?
- Should training focus on Phase 2 tools already deployed, foundational cybersecurity frameworks, or both?
- What cybersecurity skill areas would deliver the most value for locality IT staff?
- Would localities be willing and able to require trained staff to remain employed for a defined period after training?
- Can localities plan for salary adjustments when staff complete funded training or earn certifications?

Patch Management

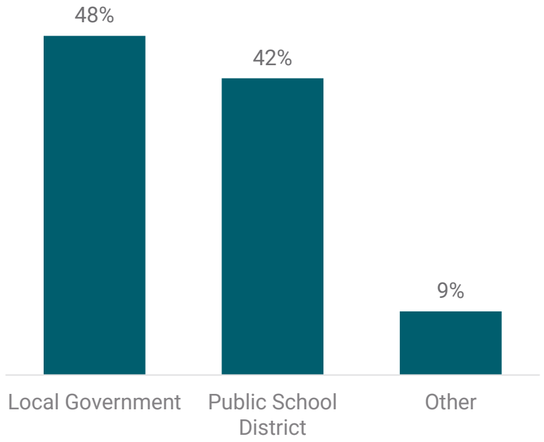
- What type of patch management support do localities need most: catch-up remediation, SOP development, or both?
- What is the biggest barrier to consistent patch management in local government environments?

Interest

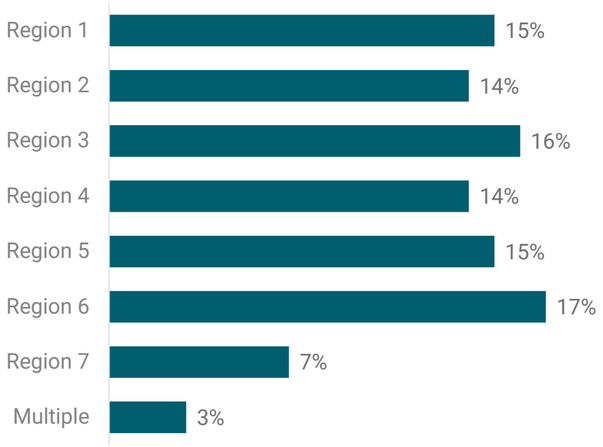
- How ready are localities to commit to a Phase 3 patch management or training program?
- What constraints would most limit participation?

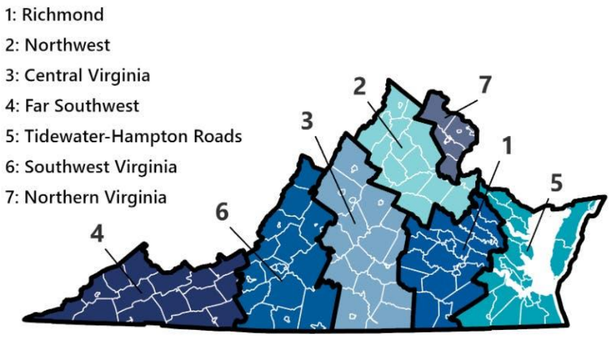
Survey Participant Demographics

Organization Type

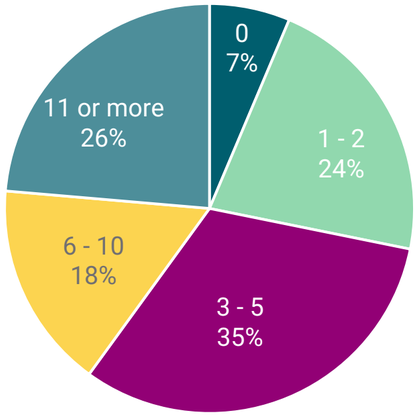


VDEM Region

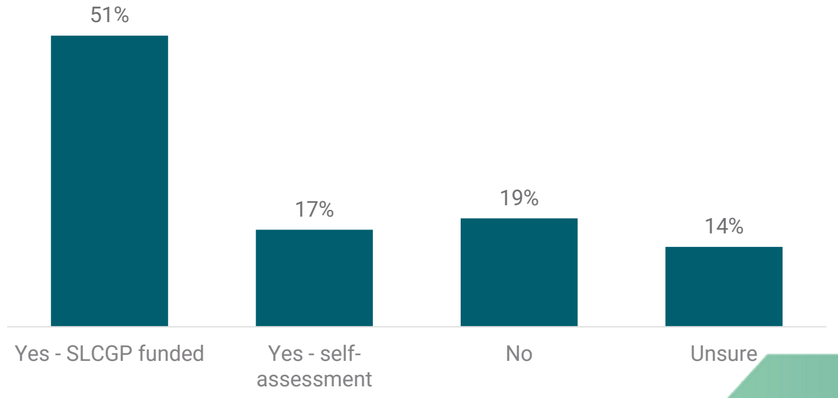




IT Staff Size

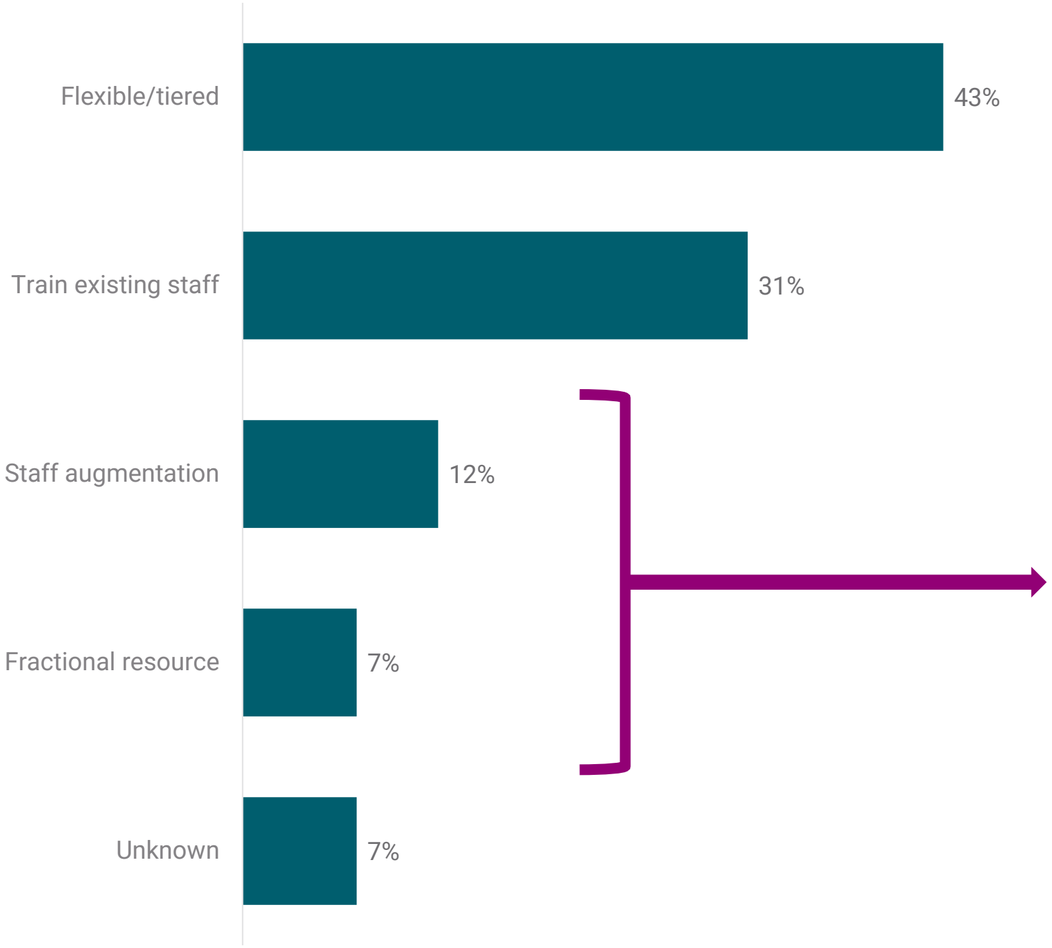


Cybersecurity Assessment Status

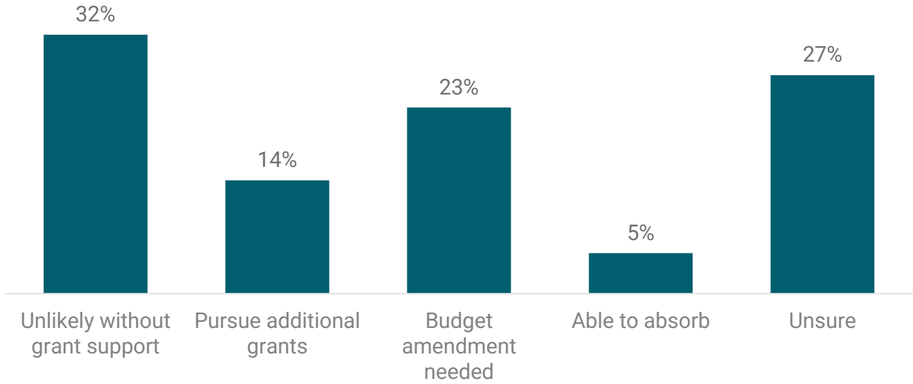


Workforce Approach

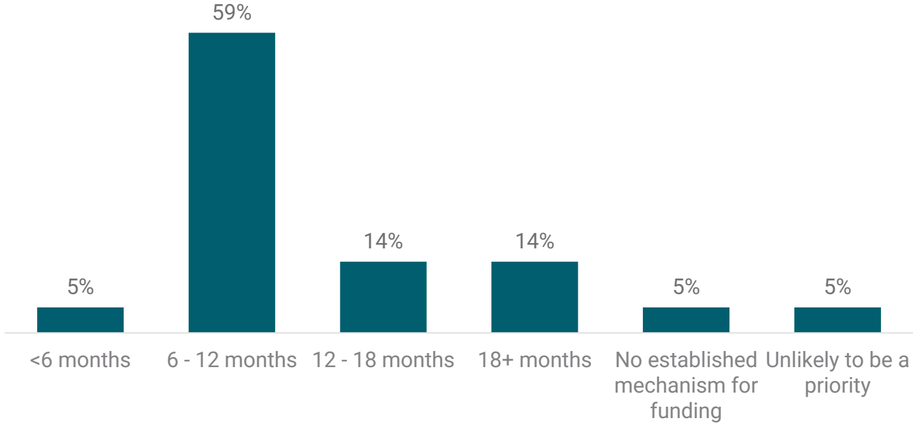
Preferred Approach



Post SLCGP Sustainability Plan

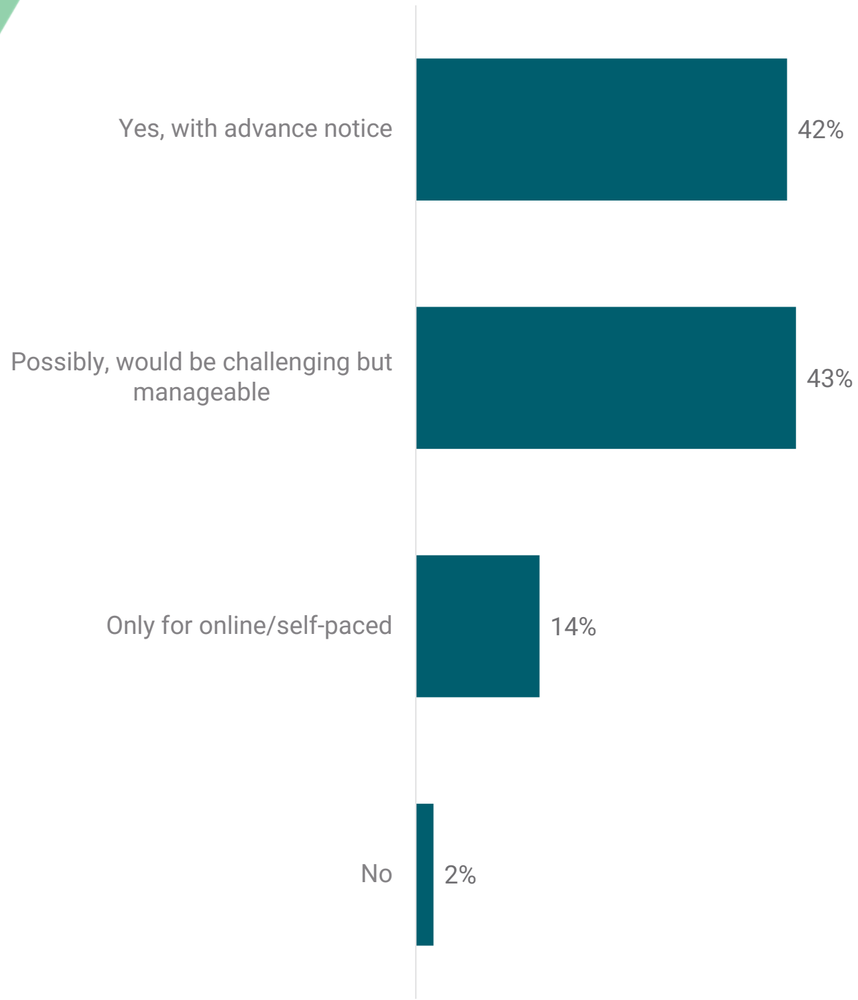


Lead Time Required

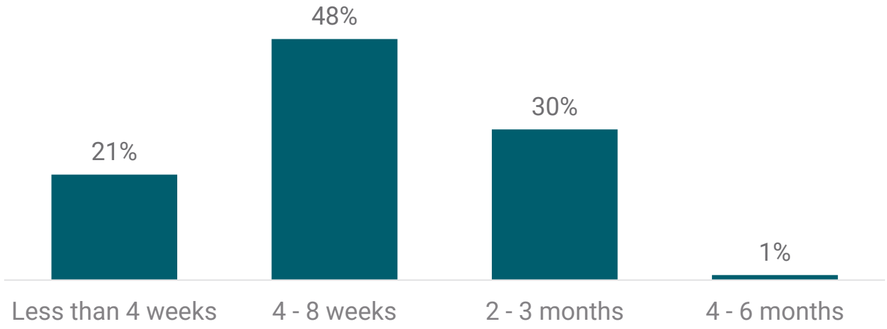


Operational Impacts of Training

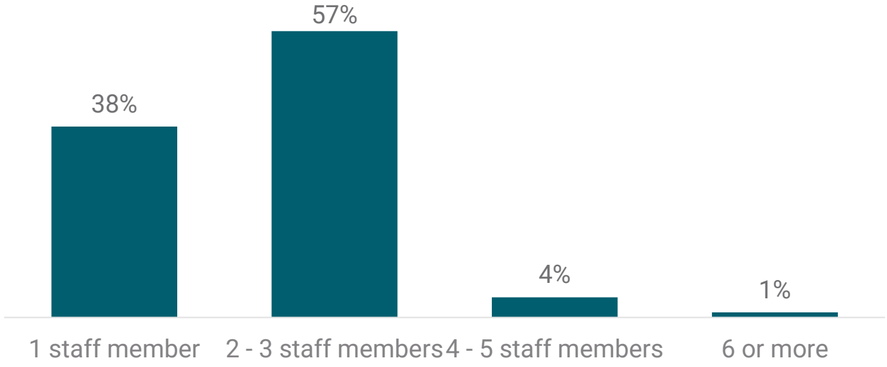
Ability to Release Staff for Training



Lead Time Needed

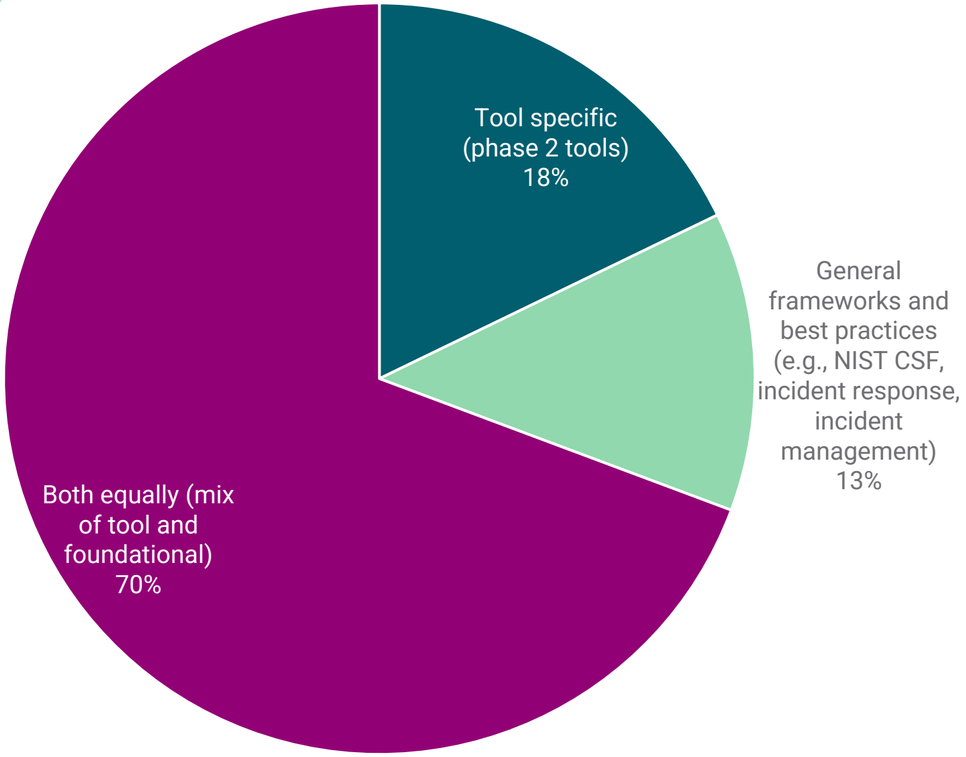


Number of Staff in Training Simultaneously

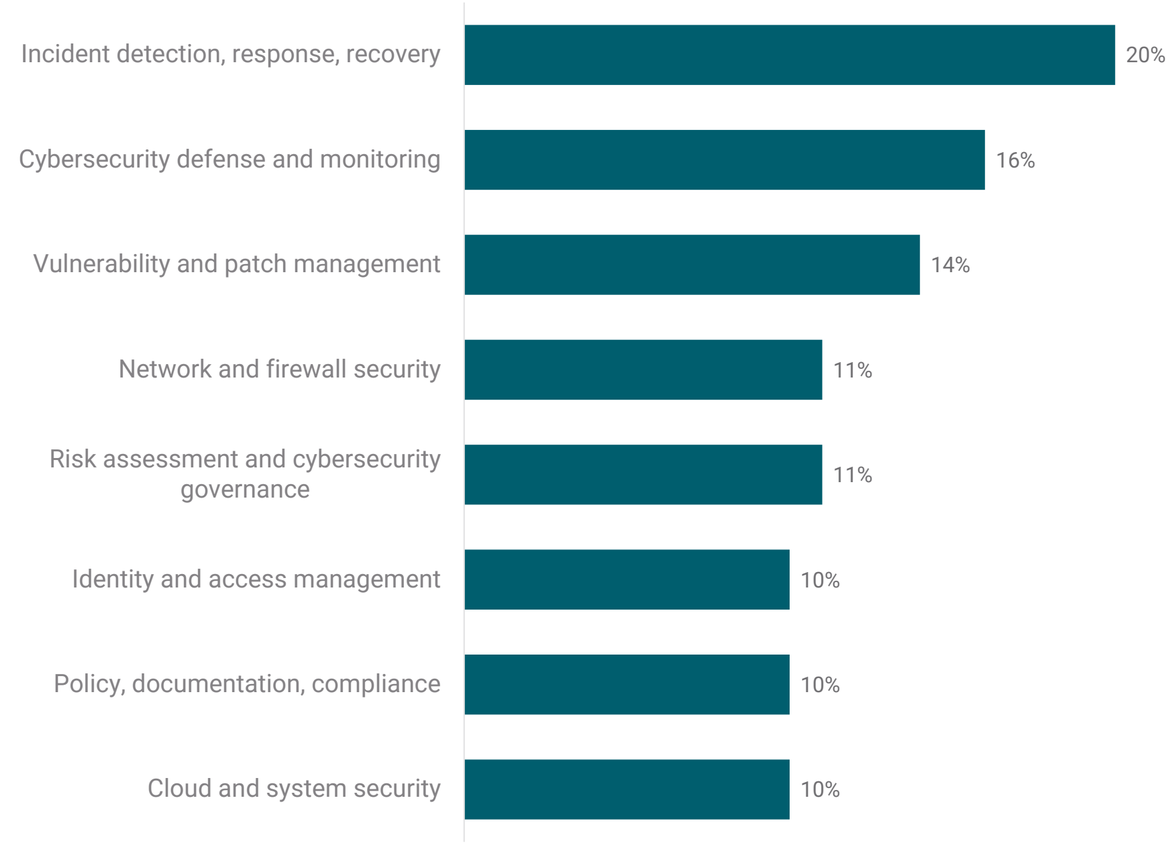


Training Areas

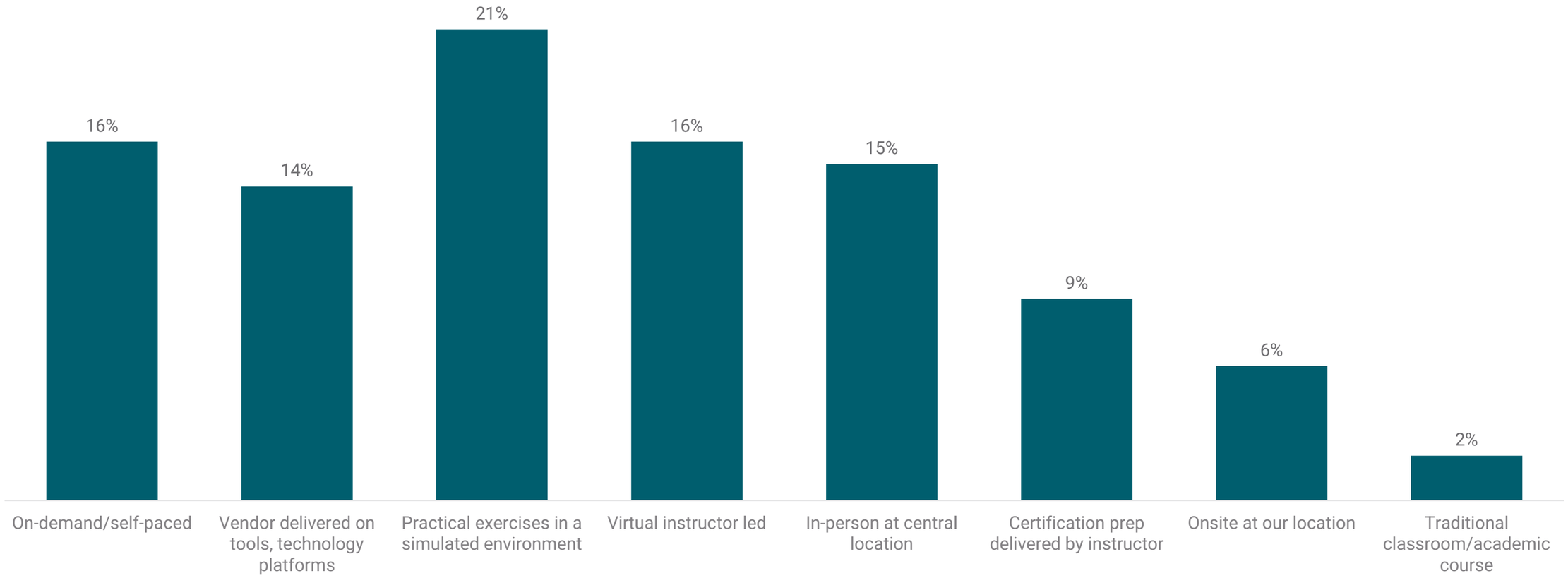
Training Focus



Most Valuable Skill Development Areas

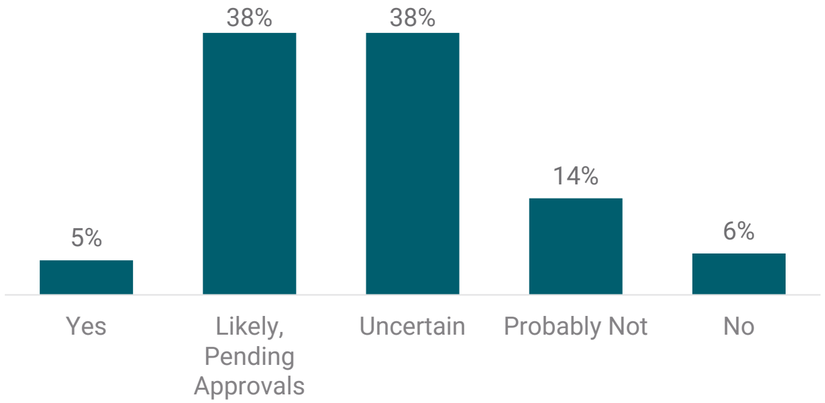


Training Delivery Format

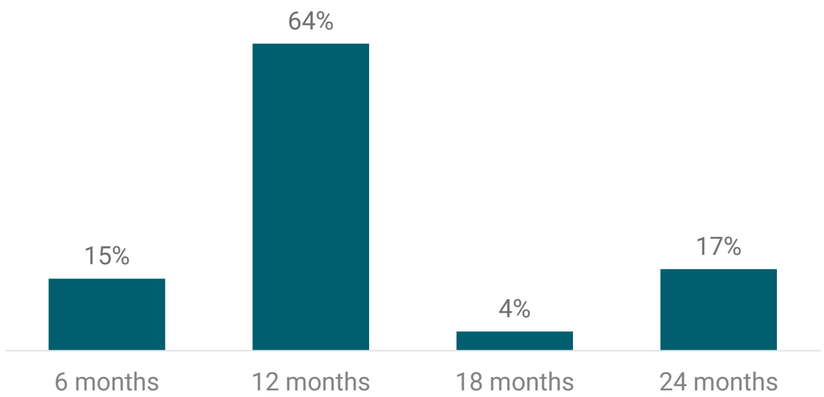


Ability to Make Retention and Compensation Commitments

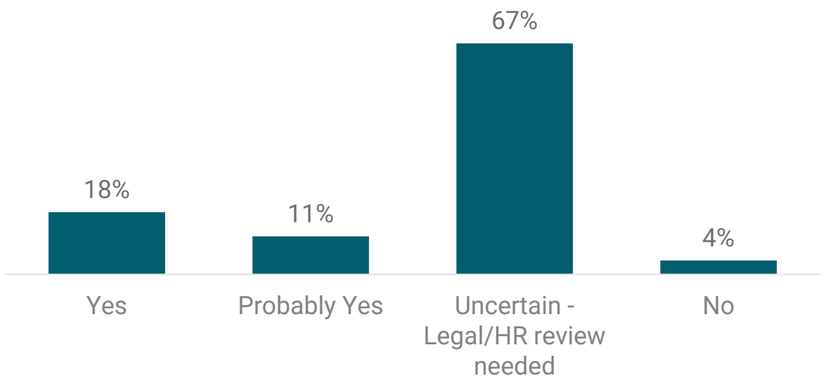
Retention Willingness



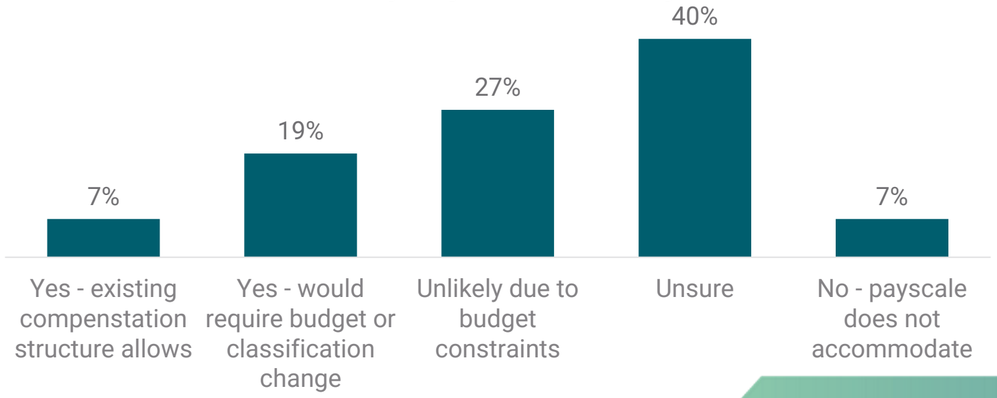
Realistic Retention Period



Retention Commitment Authority

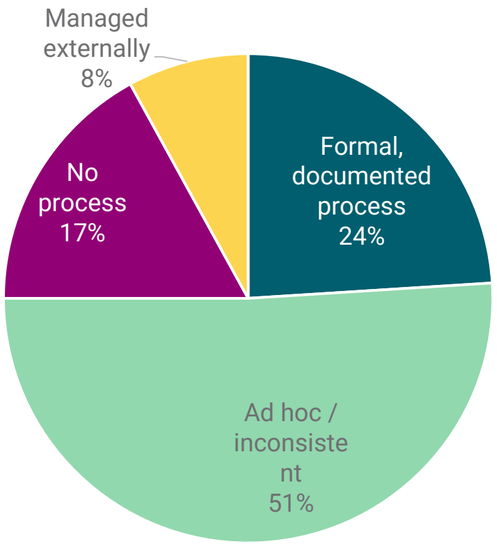


Salary Adjustment Ability

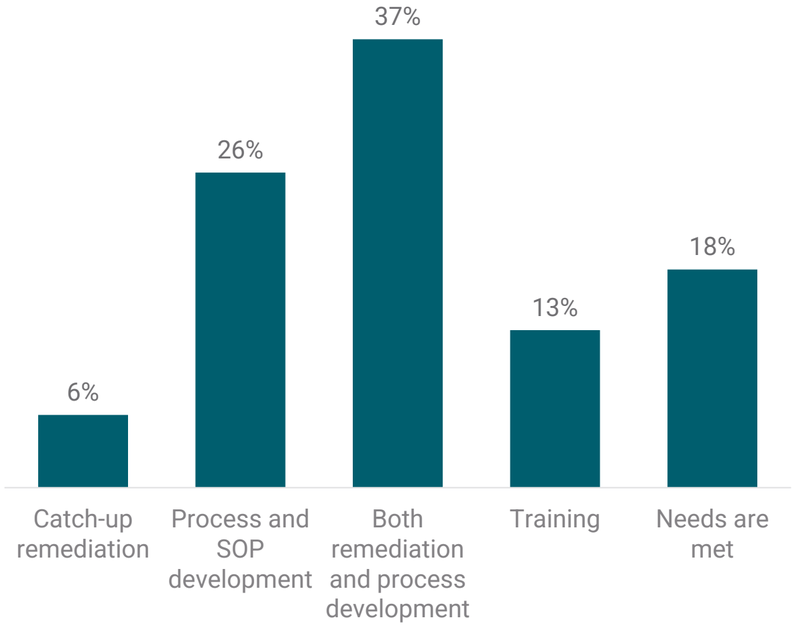


Patch Management

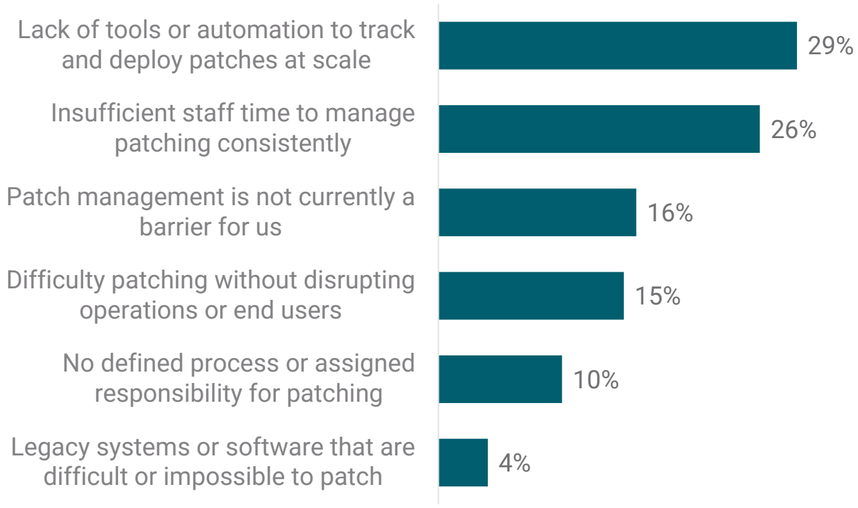
Current Process



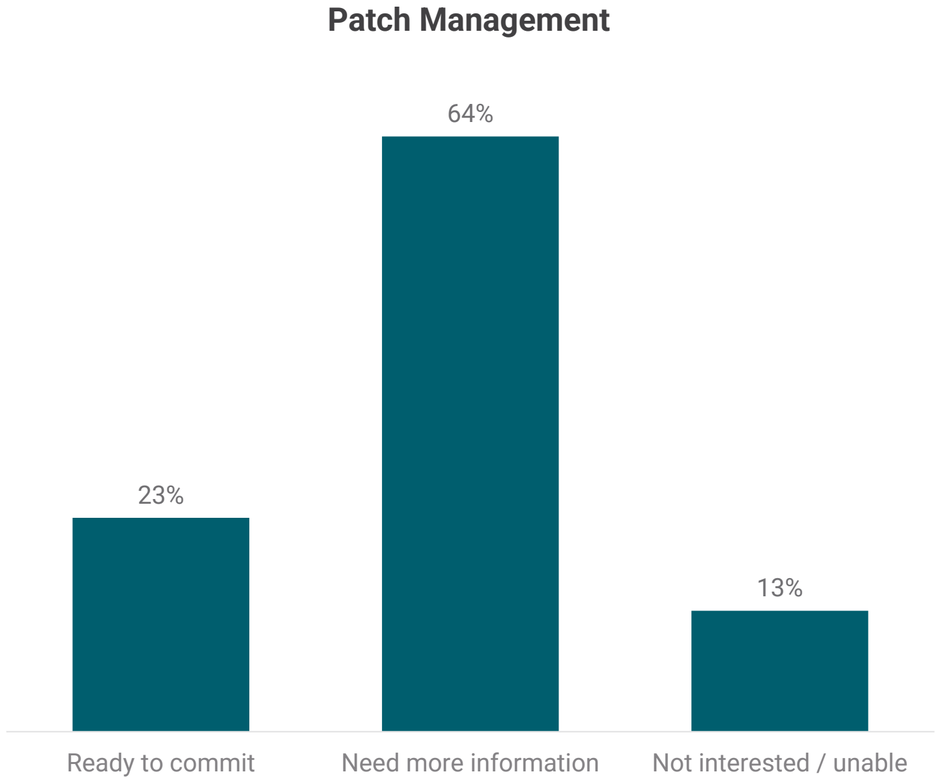
Assistance Needed



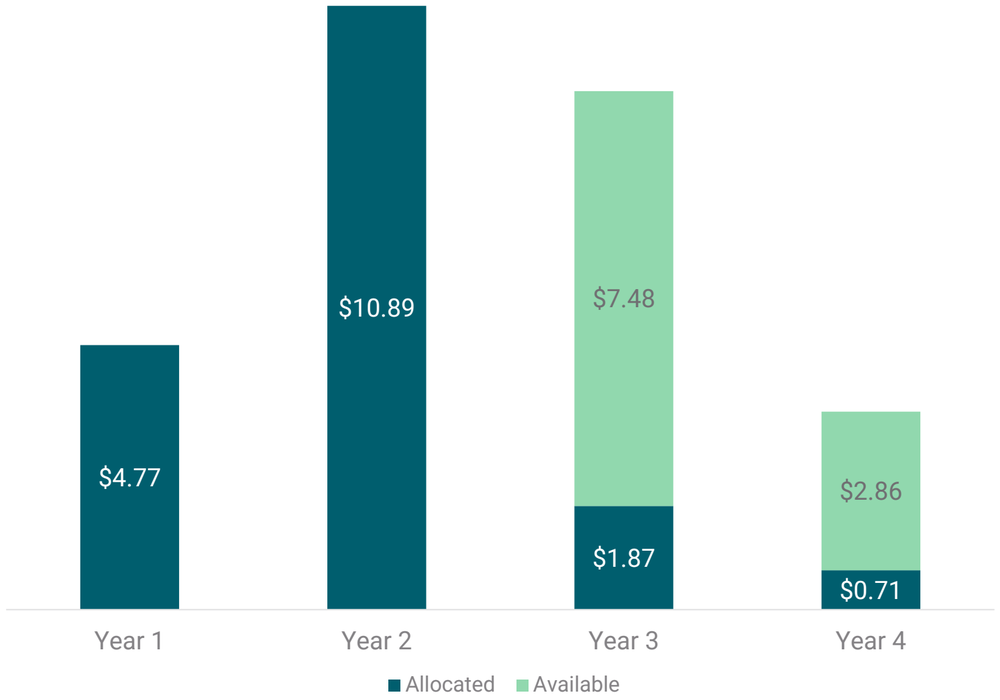
Barriers



Program Interest



SLCGP Budget Allocations



Allocation Assumptions

Project	Amount
M&A	$1.43M
Program Support	$1.25M *Assumption: source – statewide funds*
Locality SOC	$3.04M *Assumption: utilize statewide funds not spent on program support*
Plan and Assessments	$1.80M
Phase 2	$10.72M

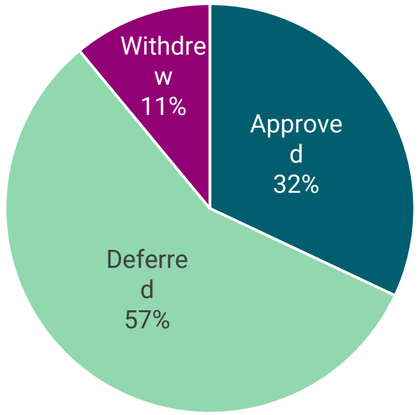
Available for allocation $10.35M

Post Federal Grant Planning

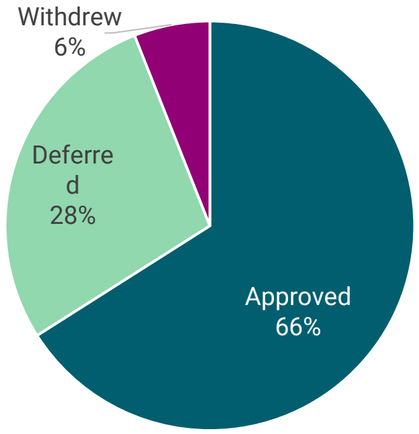
Appendix

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