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
Phase 3 Follow-Up	Mary Fain
Post Federal Grant Planning	Discussion, led by Chair
Public Comment Period	
Other Business	Staff
Adjourn	

Virginia Cybersecurity Planning Committee
May 20, 2026 – 1:00 p.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 1:01 pm. Mr. Watson welcomed the members.

Presiding

Michael Watson, Committee Chair, Chief Information 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
Charles Huntley, Director of Technology, County of Essex
Brandon Smith, Chief Information Officer, Department of Elections
Robbie Coates, Director, Grant Management and Recovery, Virginia Department of Emergency Management
Derek Kestner, Information Security Officer, Supreme Court of Virginia
Chris Mowry, Chief Information Technology Officer, Virginia State Police

Members Attending Virtually

Uma Marques, Information Technology Director, Roanoke County Government

Members Not Present

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems

Staff Present

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
Jaime Hoyle, Director of Legal and Legislative Services, Virginia IT Agency
Ephfrom Walker, Legal Compliance and Policy Specialist, Virginia IT Agency
Jennifer Guild, Assistant Director of Communications, Virginia IT Agency

Review of Agenda

Ms. Gauldin provided an overview of the agenda.

Approval of Minutes

The March 18 meeting minutes were displayed on the screen. Upon a motion by Mr. Wyatt and duly seconded by Mr. Smith, the committee unanimously voted to approve the March 18 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 all fully allocated. For Data inventory and Secure Remote Network Access (SRNA), there is a remaining $3.5 million that will be used for implementation support. Tools have been identified for asset inventory that will allow us to cover the six domains with three tools. There is still outstanding pricing on data inventory and SRNA, specifically for implementation and support resources for those areas. Firewalls will be addressed at the end of the Phase once we have pricing completed for the other areas. Currently, updates are being made to federal documentation so that we can submit the reimbursement requests. There is a backlog from the shutdown, and the process has been lengthened due to validation of numbers and categories.

Phase 2 Project Update

Ms. Logan discussed Phase 2 project status. There are currently four areas still in flight: asset inventory, data inventory, SRNA, and firewalls. There has been an average of about 10 percent in each category that has withdrawn. We will review further information towards the end of the phase for entities that have been deferred. Mr. Smith asked if there is a better picture of firewall requests. The Chair commented that it is between three to five and that it is expensive to ask for both hardware and years of maintenance. Ms. Logan reviewed the current projected timeline for Phase 2. Ms. Logan shared the projected timeline for the remainder of Phase 2. There are currently six program areas in flight. Deployments for Endpoint Detection Management (EDM) and Vulnerability Management (VM) have been completed and are in maintenance phase through July 2026. The detailed planning for Asset Inventory is going to be completed by the end of May 2026 and closed out in March of 2027. We are currently looking at three tools for this area, which are expanding the timeline length. There are currently only two tools in data inventory and that will be closing a little earlier than projected, likely February 2027. Detailed planning for SRNA will be embarking in June 2026. There are a good number of responses and consent agreements from applicants for SRNA, so deployment should begin in the fall of 2026 with close out in early 2027. Data is still being gathered for detailed analysis for Firewall planning. Vulnerability Management and EDR have been closed out, and training has been provided to localities. There are some remaining licenses and those still in need that have already participated in the program will be looked at to receive those licenses. There had initially been seven EDR deployments, but that number is still growing. There will be an update on the Falcon Complete transition at the next meeting. Ms. Marques asked if localities could get more insight into what has been contracted and procured by the state so that localities can start planning. As of right now, they do not have insight into these contracts. Chair Watson agreed that we can start working on that and that the Commonwealth is happy to collaborate to help keep costs down with group pricing. Mr. Smith asked if, as we are completing phases and closing out projects, we are indexing or surveying feedback about how it worked for the vendor and how the localities feel about the product. Ms. Logan assured that we have done that for Phase 1 projects so far and Chair Watson agreed that it would be helpful to make those aggregated results available, but to be aware that prices might increase down the road. Ms. Logan shared that asset inventory and data inventory have entered the detailed planning stage and are moving at a decent pace. Work with the localities began in December but has been challenging due to receiving consent agreements back at a slower pace or not at all. With continuous follow-up required, a cutoff point needs to be determined on when we withdraw localities if we haven't heard back from them. Ms. Marques commented that, in her organization, the point of contact for the project had left their position and the messages had not been forwarded to another contact. She recommended collecting a primary and secondary point of contact so that information is not missed. Chair Watson agreed that it is a good method going forward as well as sending out notes to the remainder of non-responses at the end of June and then closing out if there is no further response. We are currently halfway through consent agreements for SRNA and have gotten a good response rate. Selection and contract negotiation for the grant program locality Security Operations Center (SOC) is currently in progress. In the meantime, Falcon Complete will be in place to bridge the monitoring function

and identify alerts for up to one year. Ms. Carnohan asked if this will be monitored at the state or locality level. Chair Watson stated that it will be both and that Memorandums of Understanding (MOU) are established between VITA and the localities so that local teams can do what they need to.

Phase 3 Survey Results and Follow Up

Ms. Fain reviewed the four possible options for Phase 3 that were presented at the last meeting. During discussion at the last meeting, it was decided that workforce development/training and patch management were the most needed areas to concentrate on during Phase 3. Ms. Fain reviewed the questions that were brought up during the last meeting by the committee members and subsequently addressed in the survey sent out to localities following the meeting. Ms. Fain reviewed the demographics of the survey result respondents. There were over 118 responses, evenly split between localities, higher education, and others (regional entities, tribal governments, etc.). According to statistics, there was a fairly distributed audience, with Northern Virginia being the smallest region of participation. One of the questions on the anonymous survey was the staff size of the IT team. Of those that responded, half of them have five or less employees with about a quarter of respondents with 11 or more. Some of the entities that were screened out as not eligible were nonprofits and vendors. Regarding workforce approach, almost half chose a flexible or tiered model as most beneficial, but they have no clear path to funding for further training. Respondents said that they need at least a six-month lead time to get this training into the budget cycles, but it would probably be closer to 12 months. As for operational impacts, respondents said that it could be challenging but a 1–2-month lead time would help, as well as sending anywhere from 1-3 people to training simultaneously. In response to training areas, there was a strong preference for tool specific training as well as general framework and best practice (NIST, etc.). For training delivery format, the majority of respondents prefer some sort of on demand or self-led training, with instructor led either virtually or in-person following closely behind. Not many respondents were interested in certification prep or long programs (6-month course, etc.). For the question of the ability of the localities to make retention and compensation commitments, it seems feasible according to responses, but it will put a lot of the legwork on the localities and cooperation with their human resources and legal teams since this hasn't been done before. The biggest factor in responses to compensation are the budget constraints that localities face.

Ms. Fain then shared survey results regarding patch management. The survey asked the respondents what their current process is today. Most respondents were in an inconsistent ad-hoc state. The respondents noted that the areas that assistance is needed are in processes and Standard Operating Procedures (SOP), but most respondents need both as well as remediation and process development. The barriers to getting this assistance are mostly tools and resources. The survey asked respondents if they would be interested in participating and the most popular response was that they needed more information, but there is definitely interest. Mr. Smith asked if the respondents that are ready to commit line up with the 17% that have no process at all or ad hoc for patch management. Ms. Fain confirmed that it lined up with regards to patch management but that the numbers for training were all over the place. Chair Watson stated that our next step needs to be outlining what a program would look like and sending out a notice to see if they are ready to engage in these two categories.

Ms. Fain then presented the budget allocations. Year One is fully allocated between M&A, SOC, Phase 2, and assessments. Year Two is fully allocated between the locality SOC and Phase 2. For Year Three, there is a tentative hold for support and SOC, leaving $10 million open to discussion. Chair Watson referenced back to the Phase 3 options slide and asked the committee what they want to do with this money. The question is are the survey results enough to shape what we are doing with the remaining funds, or do we need to shift funding to/from firewalls or expand on what we already have. Mr. Smith asked if we have a number for firewalls and Chair Watson stated that it is whatever we have left because it could eat up the remaining funds. Chair Watson asked if we have enough information to make a plan. It would likely be some sort of computer-based training that would, hopefully, be free. We could approach some of our partners like AWS and MS to help supply low cost or free offerings for localities. For the tool aspect, it would be trickier since we don't know what types of tools to train for. It could be part of the program that we provide generic or open-source training. Major Dekeyser noted that his analysts struggle

to digest operational data from Crowdstrike and it could potentially overwhelm the localities with the amount of information captured. Ms. Carnohan agreed and asked how many localities would be seeing that data. It feels like that might be too detailed and not the training that the localities are looking for. They would get more value out of understanding high-level information and smaller teams don't have the expertise to go that deep. They need to know what they are supposed to be looking at instead of all of it. Ms. Marques stated that the problem isn't the training itself, it's having extra bodies to make the training able to do. The tools are not the problem; people are the biggest problem. She asked if we could use grant funding to hire people and Chair Watson denied that stating that it is part of grant requirements. Ms. Marques followed up asking if the money could go to hiring contractors or consultants and Chair Watson agreed as long as it doesn't supplant funds. Mr. Smith shared that people resources vary per locality and it might be best to give them refreshers on programs they are already using since things change quickly. He also cautioned sending consultants into certain environments as it could become contentious. Ms. Carnohan shared that the Department of Education uses Udeme to find where their skillset is and for training on technical skills on a certain pathway. Chair Watson agreed that we want to give a variety of training opportunities so that we meet several needs, both with topics and skill levels. Chair Watson then asked the committee what tools need to be put in place and what major areas that will be most helpful in being implemented. Mr. Wyatt suggested that it is just a case of making them aware of what they are missing and a centralized way to push out patches. Ms. Marques suggested that the biggest barrier is working with business departments and being unable to move quickly because of approvals. Speaking with these business units and communicating the risk to them that it is worth stopping the service to fix the problem rather than live with the vulnerability. Ms. Carnohan suggested a risk-based approach like explaining what the highest risk is that closes the biggest gap. Chair Watson agreed that we need a risk-based capture. He stated that we will come back with a model representing what was talked about during this meeting and will present it at the next meeting. This will inform what Phase 3 looks like, but we have time to add on if we need to.

Post Federal Grant Planning

Chair Watson discussed that we are approximately 12-18 months from the end of receiving federal grant monies. He asked if there was any interest in continuing what we are doing and how do we do that. He shared that the Joint Commission on Technology and Science (JCOTS) has shown interest in the program and has started conversations on how the program is a success and how it has impacted localities. The next step is seeing how we want to structure the program going forward. The Chair likes the governance model that is currently in place, but it does not have to stay this way. If there are specific things that we want to focus on as a committee, how do we want to go about capturing that and incorporating it into the overall approach. The Chair stated that during the next meeting we will have a larger discussion on how we want to frame the committee moving forward, as well as build out and drum up support. By early 2027, we will need to have an idea of what type of support and structure we want to have going forward.

Public Comment Period

There was one public commenter, Karen Cole from Assura Inc. She shared concerns that she had heard from their clients regarding the locality SOC.

Other Business

Chair Watson opened the floor for other business. The Chair shared the roadmap of where we are going and brought up the possibility of switching from a planning committee to and an ISAC, with the committee members being over the ISAC, since it has a pre-formed structure that we could borrow from. Ms. Carnohan asked if we are looking at a risk-based approach, is there a way that we can showcase the growth from where we started to where we look at the end? The Chair assured that we can look at the

maturity level of each area that was addressed and use that as a way to present to legislators and other stakeholders.

Ms. Gauldin discussed travel forms. Chair Watson cancelled the next meeting in June and Ms. Gauldin noted the next meeting will be July 15th at 10am.

Adjourn

Upon a motion by Mr. Huntley and duly seconded by Mr. Adkins, the Committee meeting was adjourned at 2:45 pm.

VIRGINIA IT AGENCY

State and Local Cybersecurity Grant Program

Cybersecurity Plan Capability Assessment Project Update

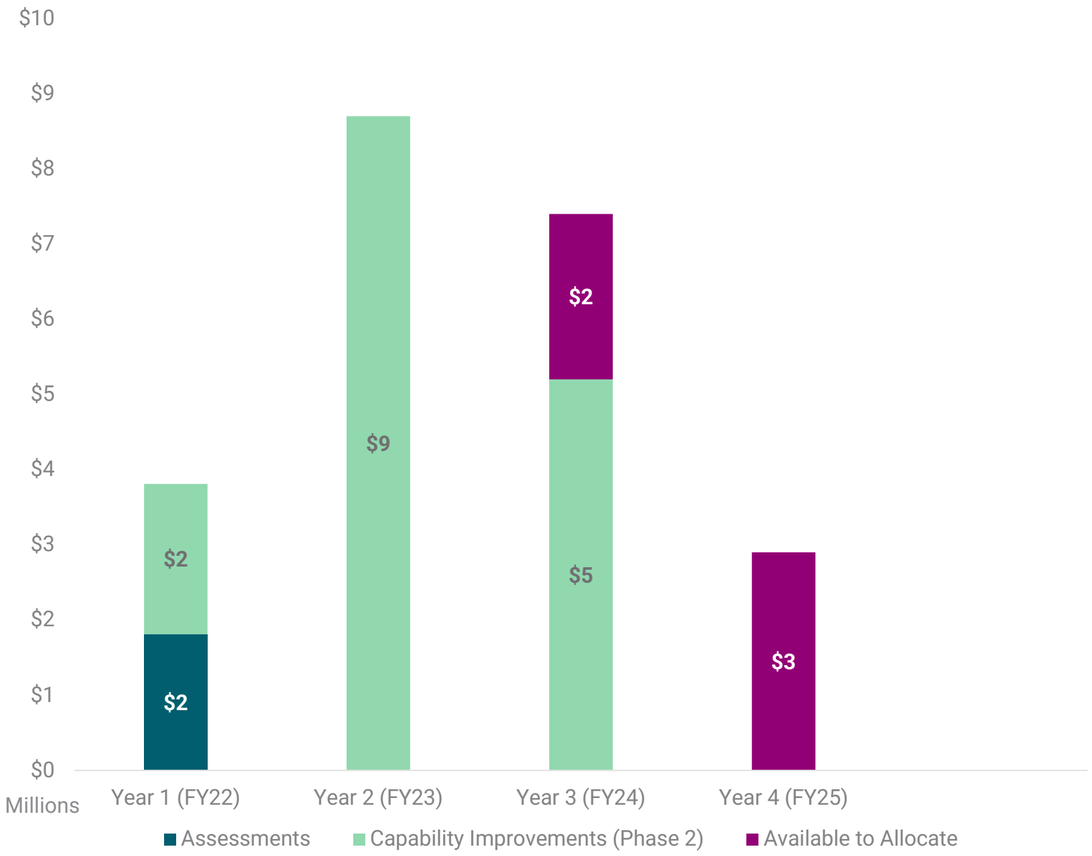
July 15, 2026

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							

Local (80%) Allocations



Project Totals

- Assessments Total - $1.8M
- Capability Improvements - $10.6M - $15.8M

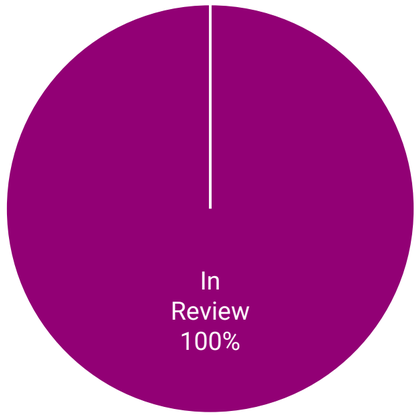
Considerations for Funding Available for Allocation

- **Phase 2 Firewalls**
  - Includes both WAF and physical firewalls
- **Phase 3**
  - Training
  - Patch Management
  - Regional exercises (pen testing and tabletop) with local executive engagement opportunity

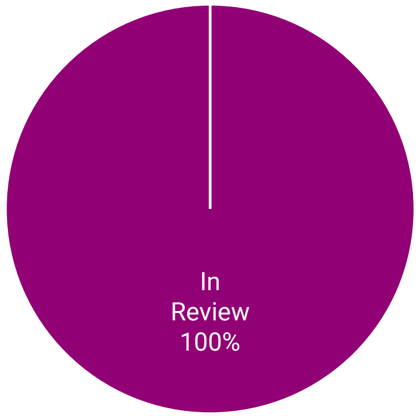
Phase 2 Update

Phase 2 Application Decision Outcomes

Firewall



EDR – Round 2



Vulnerability Management – Round 2

Decision Criteria
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	July	August	September	October	November	December	January	February	March	April	May
EDR	Deployment/Maintenance				Close						
VM	Deployment/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	Evaluation Period	Award Notification									

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%	2/26/2027	
CMDB	33	100%	73%	50%		N/A		45%	2/26/2027	
ITAM	43	100%	72%	50%	N/A	N/A		56%	2/26/2027	
ITSM	36	100%	78%	50%	N/A	N/A		57%	2/26/2027	
Network Monitoring	38	100%	68%	50%	N/A	N/A		55%	2/26/2027	
Software Asset Mgmt	42	100%	76%	50%		N/A	N/A	57%	2/26/2027	

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%	1/29/2027	
Data Loss Prevention	39	100%	69%	30%		N/A		40%	1/29/2027	
Data Loss IR	37	100%	73%	30%	N/A	N/A		51%	1/29/2027	
Device Encryption & Data Protection	36	100%	72%	30%		N/A	N/A	51%	1/29/2027	

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%	64%				N/A	33%	1/29/2027	
Multifactor Authentication	36	100%	70%			N/A	N/A	43%	1/29/2027	

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 continues**

- **CrowdStrike Falcon Complete serves 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 now targeted for Q3 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)

SLCGP Internal Audit

- Internal audit completed for all Phase 2 program area applications
- Review encompassed accuracy, completeness, and compliance across all submissions
- Individualized snapshots of application decisions and statuses were prepared
- Each applicant received their personalized summary for transparency and record-keeping
- Follow-up with organizations as needed in progress

Phase 3 Program Options

Phase 3 Program Design Journey

CURRENT STEP

✓ Conducted initial locality preference survey

✓ Conducted follow-up locality survey

✓ Reviewed training and patch management survey results

4 **Review program design recommendations**

PRIORITY AREAS UNDER COMMITTEE REVIEW

A Workforce Development & Cybersecurity Training

- Highest-impact capability gaps (5.1.1, 5.1.3): +2.47–2.86 improvement potential
- Addresses Survey #1 (NICE skills review) & #2 (personnel training)
- Builds internal capacity, reduces reliance on contracted services

Discussion: Training outcomes

B Patch Management Program

- Freetext cited patch management as a combined priority with pen testing
- Closes the remediation gap in the vulnerability lifecycle — identify, detect, fix
- Sub-objective 3.9.2: 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: risk assessment/mitigation review; freetext cites pen testing, BIA
- Aligns with sub-objectives 1.3 (software lifecycle, +1.96) & 4.3.1 (threat intel, +2.48)

D Incident Response Planning & Resilience Exercises

- Would include SOC onboarding
- Survey #3 (DR plan) & #6 (tabletop exercises) — both top 6 priorities
- Freetext: formalized DR planning, BIA, incident response; aligns with sub-objective 4.1.1 (data recovery, +1.94)

Workforce Development Program Design Considerations

1 Reflects Locality Survey Input

- Delivery: on-demand / self-paced and virtual instructor-led lead all formats; long programs and certification prep rank last.
- Content: tool-specific and framework / best-practice (NIST) preferred.
- Constraints: 1–3 staff released at a time, 1–2 months operational notice, 6–12 month budget lead time.

2 Supports Adult Learning Best Practices

- Adults learn best when training is self-directed, problem-centered, and immediately applicable to their job (Knowles' adult learning principles[1]).
- Skill retention requires practice with feedback and spaced application — not one-time content exposure.
- Relevance is the strongest motivator: learners need to see why each skill matters to their own environment.

3 Measures Outcomes

- Training evaluation practice (Kirkpatrick model) measures four levels: reaction, learning, on-the-job behavior, and organizational results.
- Seat-time and satisfaction measure only the first level. Program recommendation measures learning, behavior, and results.

In Scope: IT Staff

Out of Scope: End-user cybersecurity awareness training

[1] *Knowles, M.S., Holton, E.F., & Swanson, R.A. (2020). The Adult Learner: The Definitive Classic in Adult Education and Human Resource Development (9th ed.). Routledge.*

Program Methodology

1

Assess + Apply

Local entity completes application including:

- Baseline skills self-assessment per staff member
- Modality preferences
- Organization qualification information

2

Approval Criteria

Recommended:

- Organization meets local entity qualification criteria
- Total organization skills assessment at 50% or lower confidence

Build / Buy

Based on gaps identified through approved applications, based on skills gaps and modality preferences of the cohort

3

Assign Learning

Each participant receives a path pairing their “Not Yet” / “Somewhat” skills with stated preferences and release constraints. Locality commits to completing at least one learning path per participant.

4

Complete Training

Participants complete training path based on approved application

5

Re-Assess

Same instrument re-taken at program end, plus one applied-on-the-job indicator per skill. The pre/post shift is the documents outcome(s).

Application Assessment Tool

A skills-based self-rating (Confident / Somewhat / Not Yet) across 18 Baseline and 52 Depth skills from System Administrator, Network Operations, and Technical Support (for breadth/general IT skills) and Defensive Cybersecurity, Incident Response, and Vulnerability Analysis (depth/security specialist), each mapped to NIST NICE Workforce Framework work-role skill statements, supporting SLCGP NOFO Objective 4.2 and the Cybersecurity Plan's workforce element. Would also include skills related to the tools associated with Phase 2.

Training Content Sources to Consider During Build/Buy Phase

A Curated No-Cost Federal Paths (base layer)

- CISA Learning: ~850 hours of NICE-mapped training, free to SLTT staff (replaced FedVTE).
- Learning paths curated by VITA using CISA's Workforce Training Guide and Cyber Career Pathways Tool.
- Modality – virtual, asynchronous

B On-Demand Commercial Catalog

- Commercial e-learning library licensed for all participants — self-paced video courses, built-in skill assessments, NICE-mappable security paths.
- Matches the survey's top delivery preference (on-demand / self-led).
- Modality – virtual, asynchronous

C Virtual Instructor-Led Cohorts

- Scheduled short courses aligned to the NICE Framework, targeted at the highest-frequency gaps across all assessments.
- Cohort format adds peer interaction; virtual delivery fits the 1–3-staff release constraint.
- Modality – virtual, synchronous

D Virtual Hands-On Labs

- Practice in safe, replicated environments — the experiential leg of adult learning, and the bridge from “Somewhat” to “Confident.”
- Modality – virtual, asynchronous

E Regional In-Person Workshops

- One-day, framework-and-practice workshops hosted per VDEM region — short travel, minimal staff release, peer networking.
- Serves the survey's instructor-led / in-person cohort without long programs.
- Modality – in-person, synchronous

F Virtual Tool-Specific Training

- Operator-level “what to look at” essentials on deployed products
- Deployed grant tools prioritized, then top products from the 131 assessments
- Modality – virtual, asynchronous

Training Outcome Measure Following the Kirkpatrick Training Evaluation Model[1]

L1

Course Feedback (where possible)

Short end-of-course feedback, used only to tune the menu and drop underperforming content when possible. Not reported as a program outcome.

L2

Skills Improvement

Pre/post shift on the NICE-aligned self-assessment (Confident / Somewhat / Not Yet), per person and rolled up per locality. Primary measure: reduction in “Not Yet” ratings across the 18 Baseline skills.

L3

Application of Skills

Built into the post-program re-assessment: one applied-on-the-job indicator per skill (“have you used this at work in the past 90 days?”), with an optional supervisor confirmation at the locality level.

L4

Organizational Capability

Capability score movement on workforce development sub-objectives 5.1.1 and 5.1.3

[1] *Kirkpatrick, D.L. & Kirkpatrick, J.D. (2006). Evaluating Training Programs: The Four Levels (3rd ed.). Berrett-Koehler; Kirkpatrick, J.D. & Kirkpatrick, W.K. (2016). Kirkpatrick's Four Levels of Training Evaluation. ATD Press.*

Patch Management Program Design Considerations

1 Tool (Cybersecurity Plan Sub Objective 3.9.2)

- May survey: barriers to patching are “mostly tools and resources”
- Closes the identify → detect → fix loop in the vulnerability lifecycle

2 Process / SOP (Q22 survey category)

- Committee discussion surfaced the need for SOPs to maintain patching once localities complete “catch-up”

3 Catch-Up Remediation

- Committee discussion of the need for resource augmentation to get up to date

Patch Management Program Recommended Components

1 Patch Management Tool (catch-up + ongoing)

- Selection and deployment of patch management tool in local environments
- Locality deployment service to include tool deployment and configuration

2 SOP Development Assistance

- Hands-on (virtual) development of a patch management SOP from the NIST SP 800-40 Rev. 4 framework, localized to the applicant's environment by a contracted resource.
- Award criteria: Local government entity, <=2 on relevant current state capabilities

Patch Management Tool Considerations

Tool Selection Criteria

- Already on an existing VITA / Commonwealth contract vehicle
- Cross-platform OS / application coverage for mixed environments
- Native integration with the vulnerability management platform already in place
- Single vendor, consistent with Phase 2 cost rationale
- Risk-based / AI-assisted prioritization (2026 market baseline)

Applicant Award Criteria

- Local government entity
- Presence of compatible vulnerability management tool
- Current state patch management capability assessment <=2

Patch Management Tool Project Execution Type Sequencing

Open with Full Service + Implementation Only (matches demand pattern)
Hold Contract Only, Additional License, and pass-through in reserve if application volume is not sufficient

Program Methodology

1

Apply

Locality submits one application selecting the tracks it needs and relevant capability assessment(s)

2

Decision

Approved based on criteria in prior slides. Each selected track is approved independently.

Contract

VITA contracts for tools and services based on approved application volume:

- Tool procured through statewide contracts
- SOP partner selection

3

Deploy

Deploy tools, complete SOP engagements, remediations, and execution of penetration testing

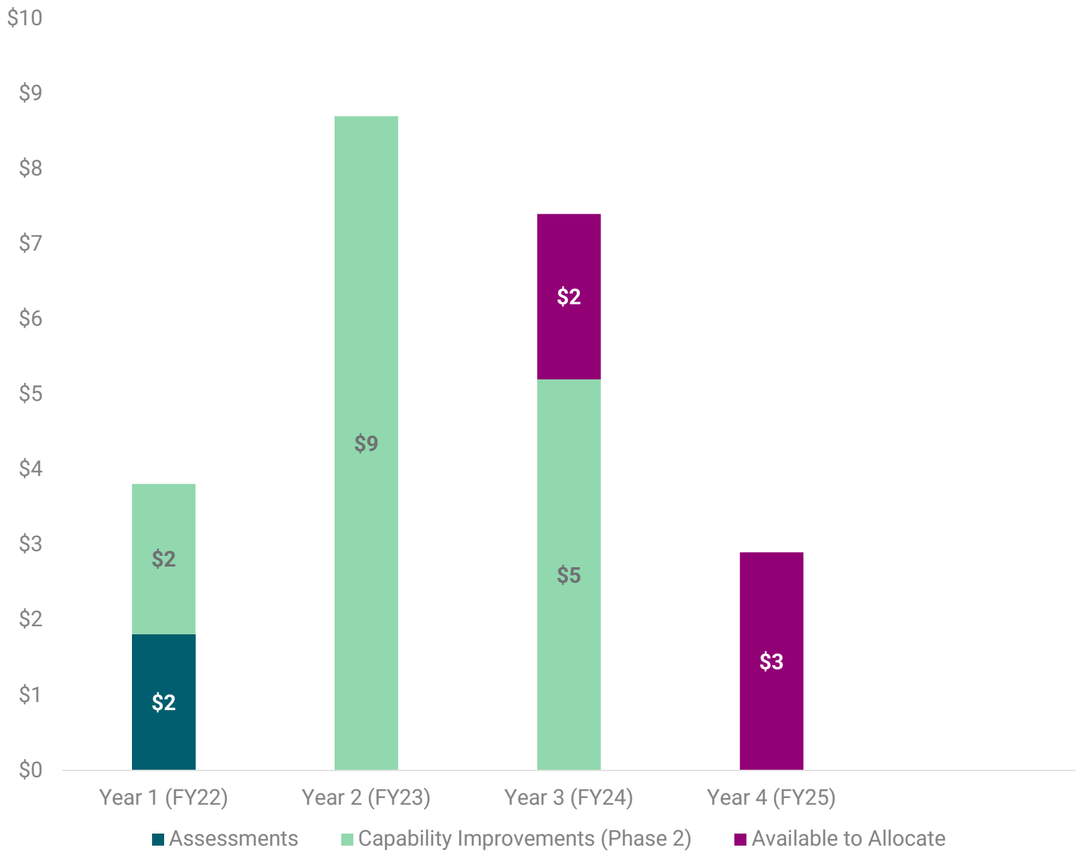
4

Measure

Capability assessment improvements

Phase 3 Funding

Local (80%) Allocations



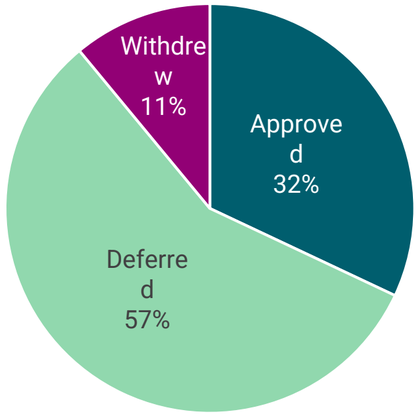
Considerations for Funding Available for Allocation

- **Phase 2 Firewalls**
  - Includes both WAF and physical firewalls
- **Phase 3**
  - Training
  - Patch Management
- **Phase 3/4**
  - Regional exercises (pen testing and tabletop) with local executive engagement opportunity

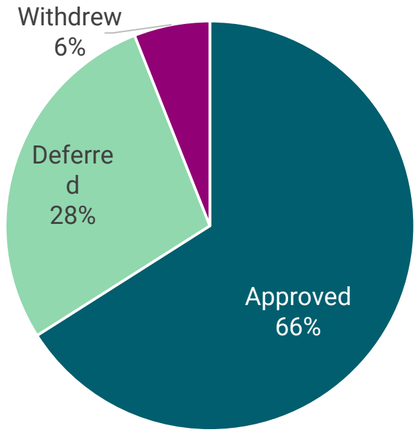
Appendix

Phase 2 Application Decision Outcomes

EDR



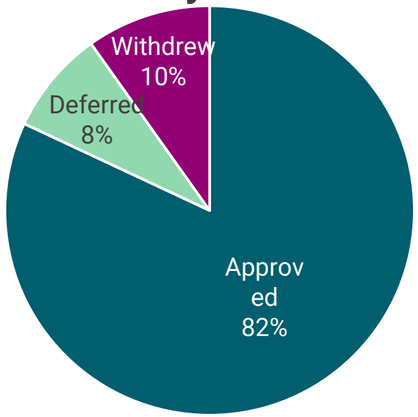
Vulnerability



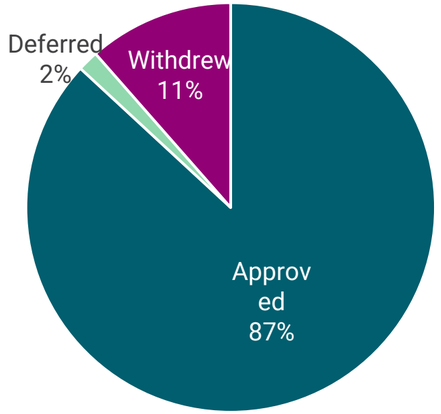
Decision Criteria
Current capability = 0 - 1
Future capability = 3 - 4
Likeliness of Success = High or application review indicated likeliness of success

Phase 2 Application Decision Outcomes

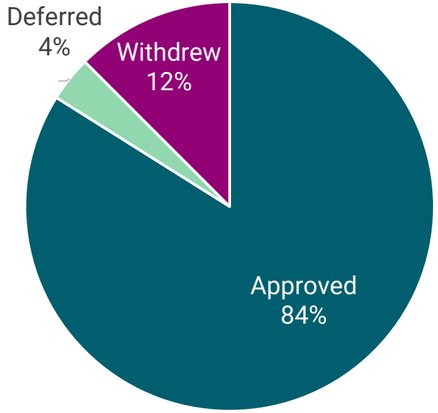
Asset Inventory



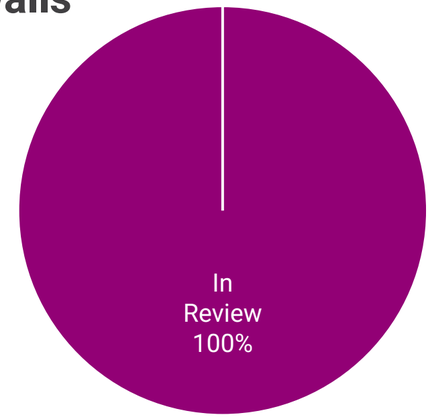
Secure Remote Network Access



Data Inventory

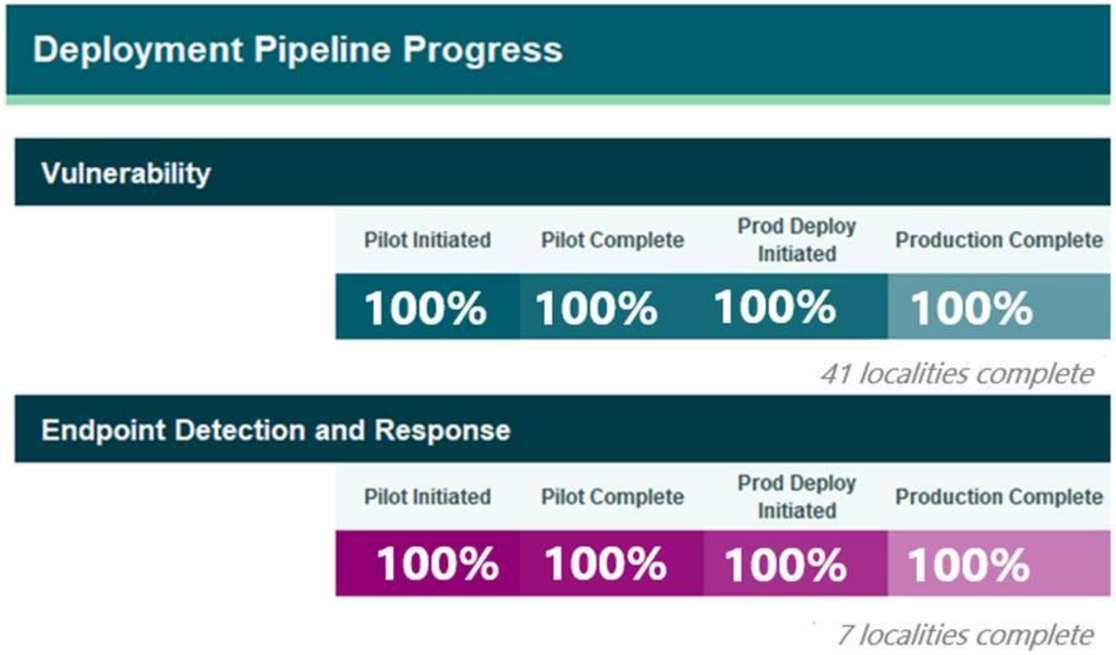


Firewalls



<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



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

VIRGINIA IT AGENCY

Virginia state and local cybersecurity grant program roadmap