



Virginia Cybersecurity Planning Committee (VCPC)

October 21, 2026 – 10:00 a.m.
VITA, Virtual

Agenda

Agenda item	Speaker(s)
Call to order and welcome	Tim Wyatt Vice Chair
Rollcall	Staff
Review of agenda	Staff
Approval of minutes	Staff

Presentations and discussion

Phase 2 Updates	Janet Logan
Phase 3 Follow-Up	Mary Fain
Budget	Mary Fain
Public comment	
Other business	Staff

Adjourn



Virginia Cybersecurity Planning Committee
July 15, 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 10:06am. 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
Robbie Coates, Director, Grant Management and Recovery, 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
Brandon Smith, Chief Information Officer, Department of Elections

Members Attending Virtually

Charles DeKeyser, Major, Virginia Army National Guard
Chris Mowry, Chief Information Technology Officer, Virginia State Police
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black

Members Not Present

Uma Marques, Information Technology Director, Roanoke County Government

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
Rebecca Askew, Policy and Governmental Affairs Manager, Virginia IT Agency
Ephfrom Walker, Legal Compliance and Policy Specialist, Virginia IT Agency
Jennifer Guild, Assistant Director of Communications, Virginia IT Agency
Advait Kulkarni, Junior Associate, Virginia IT Agency
Angevin White, Junior Associate, Virginia IT Agency

Review of Agenda

Mr. Kulkarni provided an overview of the agenda.

Approval of Minutes

The May 20 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 May 20 meeting minutes.

Finances

Ms. Fain presented the financial update. There are no significant changes from the last meeting. The remaining allocations were discussed. The committee previously voted to authorize between \$10.6 million (prioritized) up to \$15.8 million. The program is currently at \$8.7 million (estimated) between known licensing costs and projected implementation and maintenance costs. We anticipate needing up to the full \$15 million to complete licensing and contingency for implementation and maintenance for all elements before getting to firewalls. There is an additional \$2 million available for year 3 that is available to be allocated as well as year 4 funds, that do not have a project tied to it yet.

Phase 2 Project Update

Ms. Logan delivered an extensive update on the status of Phase 2 projects. There are currently still three areas in flight: Firewalls, the second round of Endpoint Detection Response (EDR), and the second round of Vulnerability Management. Application activity continues across all three, with firewalls having 66 applications submitted and 26 completed with full materials, vulnerability management with 25 applications, and EDR with 23 applications. The application window runs through July 17, with a commitment to expedite review and connect approved localities to vendors as quickly as possible. Phase 2 deployment and maintenance windows have been formally extended to October 31, with final project closure targeted for November. Asset and data inventory efforts are proceeding in parallel, with substantial progress reported. With asset inventory, a majority of participating localities have achieved greater than or equal to 70% completion. For data inventory, nearly all participating localities are approaching 70% completion. For Secure Remote Network Access (SRNA), the consent agreements received have reached about 65%. Ms. Logan highlighted that detailed planning for asset and data inventories may extend up to six months, depending on complexity across environments. To reduce operational disruptions, Phase 2 deployments are being strategically staggered, ensuring no single locality experiences excessive blackout periods. Chair Watson reported ongoing selection and negotiation for the Locality Security Operations Center (SOC) contract. Until the SOC is fully stood up, CrowdStrike Falcon Complete will serve as an interim monitoring capability for up to one year. This ensures continuity of endpoint threat detection across participating localities. An internal audit concluded in June covering all Phase 2 applications. Each locality received a customized summary assessing accuracy, completeness, and compliance. Staff reviewed 141 application folders, narrowing outstanding issues to fewer than ten as of the meeting date. Chair Watson expressed optimism that Phase 2 would reach full operational closure before year-end, enabling the committee to pivot more fully into Phase 3.

Phase 3 Follow Up

Ms. Fain reviewed the previous information received and discussed from Phase 3 surveys, including the strong response rate from localities, higher education, regional authorities, and tribal entities. The key themes were significant interest in workforce development and patch management. There was a clear preference for on-demand, self-paced training supported by virtual or hybrid modalities. There is a broad need for tool-specific content, alongside general framework and best practice guidance. Respondents also expressed operational constraints, with most organizations requiring 6-12 months of lead time to budget the training. Also, rural and smaller localities face greater staffing limitations, often able to release only one to three people at a time. Drawing from surveys and adult learning research, the committee explored a flexible skills-based model informed by a formal baseline assessment. Central elements include a skills assessment, with those scoring less than 50% confidence being strong candidates for training. Also, modality matching with training formats aligned with locality preference (self-paced, virtual

instruction, regional workshops, hands-on labs, and tool specific models). The use of outcome measurement in the form of the Kirkpatrick evaluation method (reaction, learning, behavior, results) will be supported by post training reassessments. Committee members raised thoughtful questions to be considered. Should certain training areas be mandatory, such as baseline cyber fundamentals? How do we integrate emerging technologies like AI-based security and deepfake identification? Can we ensure that localities receive concise updates, such as one-page survey summaries or program impact sheets? Ms. Fain moved on to Patch Management program design. The survey results revealed inconsistent and frequently ad-hoc patching across Virginia localities. Respondents noted that they needed practical tools to close gaps in patching, clear Standard Operating Procedures (SOPs) to ensure long-term sustainment, and remediation support for initial catch up. The patch management model under consideration contains three areas. For patch management tool deployment, there will be a preference for tools already on statewide contract, cross-platform, and integrated with existing vulnerability management suites. For SOP development assistance, contracted resources will help localities tailor SOPs to their environments. For catch up remediation, supplemental help for entities significantly behind on patch cycles will be provided. Committee members debated the role of risk prioritization, support for end-of-life systems, and balancing centralized procurement with locality flexibility. Chair Watson reopened discussion on funding allocations, reminding the committee that year 3 retains nearly \$10 million for further program development and decisions regarding distribution among training, patch management, firewalls, and emerging needs must be finalized before upcoming budget cycles. Mr. Smith emphasized that any Phase 4 or capstone activities must be completed by July/August 2027 to align with legislative cycles.

Post Federal Grant Planning

Chair Watson noted that federal grant support is expected to conclude in 12-18 months. Early conversations the Joint Committee on Technology and Science (JCOTS) indicate interest in sustaining and expanding successful elements of the program. The Chair asked the committee to begin considering whether current governance should transition toward an ISAC model, how to capture and communicate statewide cybersecurity maturity gains, and what future committees/structures/focus areas should look like beyond 2027.

Public Comment Period

There were no public comments.

Other Business

Chair Watson opened the floor for other business. It was discussed that all committee members' terms expire in October. The Chair and Ms. Gauldin assured the members that it is being worked on and that mechanisms are in place to have the members continue their work on the committee. Chair Watson also encouraged members to follow updates and attend the Information Security Conference (ISC).

Ms. Gauldin discussed travel forms. Chair Watson cancelled the next meeting in August and Ms. Gauldin noted that since the next scheduled meeting on September 16th coincides with COVITS, it will be rescheduled and that information will be sent out at a later time.

Adjourn

Upon a motion by Mr. Kestner and duly seconded by Mr. Adkins, the Committee meeting was adjourned at 11:21am.



State and Local Cybersecurity Grant Program

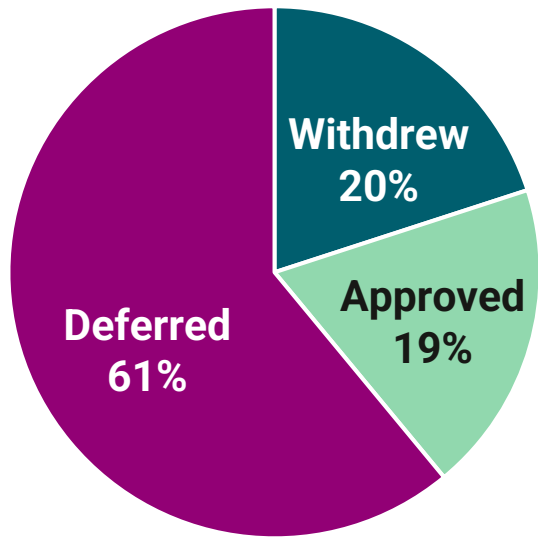
Project update

Oct. 21, 2026

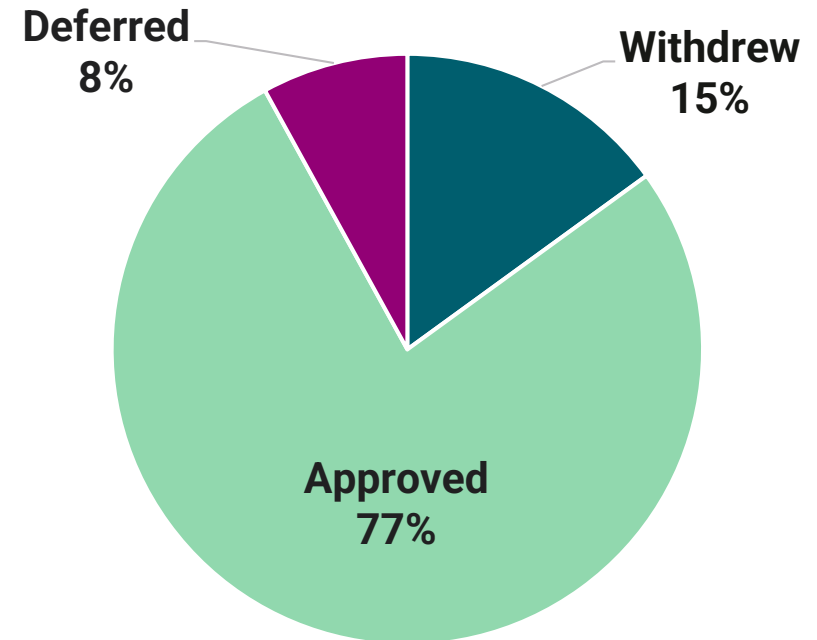
Phase 2 update

Phase 2 application decision outcomes

Firewall - Network



Vulnerability management - Wave 3



Decision criteria

Current capability = 0 - 1

Future capability = 3 - 4

Likelihood of success = High or application review indicated likelihood of success

Phase 2 projected implementation timeline

Project area	October	November	December	January	February	March	April	May	June	July	August
VM*	Waves 4-6 award/deployment/maintenance								Close		
Asset inventory	Detailed planning			Deployment/configuration (six tools)					Maintenance	Close	
Data inventory	Detailed planning			Deployment/configuration (four tools)					Maintenance	Close	
SNRA**	Detailed planning			Deployment/configuration (two tools)					Maintenance	Close	
Firewalls	Award notification		Distribution		Close						

*Vulnerability Management

**Secure Remote Network Access

Locality Security Operations Center (SOC) update

- **Final statement of work (SOW) negotiations underway with preferred vendor**
- **CrowdStrike Falcon Complete serves as 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**

Application period is targeted for late Q4 2006/early Q1 2027. All application announcements will be published via VDEM's listserv. To join the listserv, visit [Virginia Department of Emergency Management \(govdelivery.com\)](http://govdelivery.com), enter your email address and then select the "State and Local Cybersecurity Grants Program" from the list (near the bottom).

Phase 3

Tabletop exercise program proposal

Tabletop exercise program overview

1 Participants

- Local governments, school divisions, higher education, regional authorities and tribal entities
- IT lead and an executive decision maker (administrator, manager, superintendent or equivalent)

2 Program content

- 1. Pre-read | All, about 20 min online**
One-pager on the scenario and roles
- 2. Core scenario | Executives and IT leads, 90 min live**
10-min peer story from a Virginia leader, three 20-min decision rounds, 20-min debrief
- 3. IT working session | IT staff only, about 3 hours**
Turn pain points into needs, rank to a final top three to five with cost bands and funding paths, practice the pitch with the take-back guide and a peer
- 4. Follow-up meeting | IT lead and executive, 30 min**
Within two weeks, the IT lead presents the top 3-5 needs in leadership terms, executive responds, both set a date for a budget conversation

3 Program outputs

- Prioritized needs worksheet
- Leadership take-back guide
- Statewide roll-up for the committee and legislative discussions

Goal: IT participants return home with a ranked list of funding needs and a way to explain it that a board, council or superintendent can act on

Delivery format options

	Statewide in person	Regional in person	Regional virtual
Setup	One event on one date in a central location Large room, tables by entity, a facilitator for every few tables	One session per VDEM region, same agenda at each	Live regional sessions with breakout rooms by entity type
Pros	One design and delivery One dataset to summarize Legislative visibility	Shorter travel Regional peer networks Local relevance	No travel time or cost Shortest ask of executives Easy make-up sessions
Cons	Longest travel for distant regions Day+ away from office, depending on distance Big room limits discussion	Multiple venues and logistics Day away from office Regional size variance	Weaker peer connection Easier to skip or multitask
Main cost drivers	Large venue and AV Travel and lodging - highest Facilitators for one big room	Multiple venues Travel - moderate Multiple facilitation teams	Platform 4-6 facilitators per session No travel or venues

Tabletop exercise timeline vs. state/local budget timelines

	Oct. 2026 to Jan. 2027	Feb. to May 2027	June to Aug. 2027	Sept. to Dec. 2027	Jan. to April 2028
Tabletop exercise	Committee decisions; format and ceiling set once interest is known; procurement follows	Design scenario and guide; interest registration; confirm format and invitations	Pilot session in June, then remaining sessions by mid-August	Packets within 30 days of each session; statewide roll-up by Sept. 30	Follow-up at 90 days: which needs reached a budget request
Local budgets	FY28 requests begin to form	Peak season. Department estimates due by April 1; adoption by July 1	FY28 begins July 1	FY29 requests form. Take-back packets arrive	FY29 peak season
State budgets	Session convenes Jan. 13, 2027	School funding estimates due 15 days after adjournment	Interim	Roll-up informs planning for the 2028 session	Session convenes Jan. 12, 2028

The background is a solid teal color. It is decorated with several light green geometric shapes, including horizontal bars and trapezoids, some of which are positioned at the top and bottom edges, creating a modern, abstract design.

Training and patch management application and criteria proposal

Phase 3 proposed programs

Training

- Skills-based training built from a baseline assessment
- Self-paced and virtual formats, favored in the survey
- Reassessment afterward measures change

Patch management

- Patch tool on a statewide contract
- Help writing patching procedures
- Catch-up remediation for entities that are behind

Proposed application and approval criteria

Single application to cover both programs, submission deadline Dec. 31.

Program	Organization criteria	Participant criteria
Training	• Qualified entity • Current capability score of 0 or 1 for goal/objective 5.1.4 • Projected future capability score of 3 or 4, with high likelihood of success	Confident in fewer than 50% of skills
Patch management	• Qualified entity • Current capability score of 0 or 1 for goal/objective 3.9 • Projected future capability score of 3 or 4, with high likelihood of success • Compatible vulnerability management tool already in place (required for tool deployment)	Not applicable

The background is a solid dark teal color. It features several abstract geometric shapes in a lighter teal and light green color. These shapes include horizontal bars of varying lengths and widths, some with diagonal cuts, and triangular shapes pointing in different directions. The shapes are layered, creating a sense of depth and movement. The word "Budget" is centered in the upper half of the image.

Budget

Statewide (15%) allocations by grant year

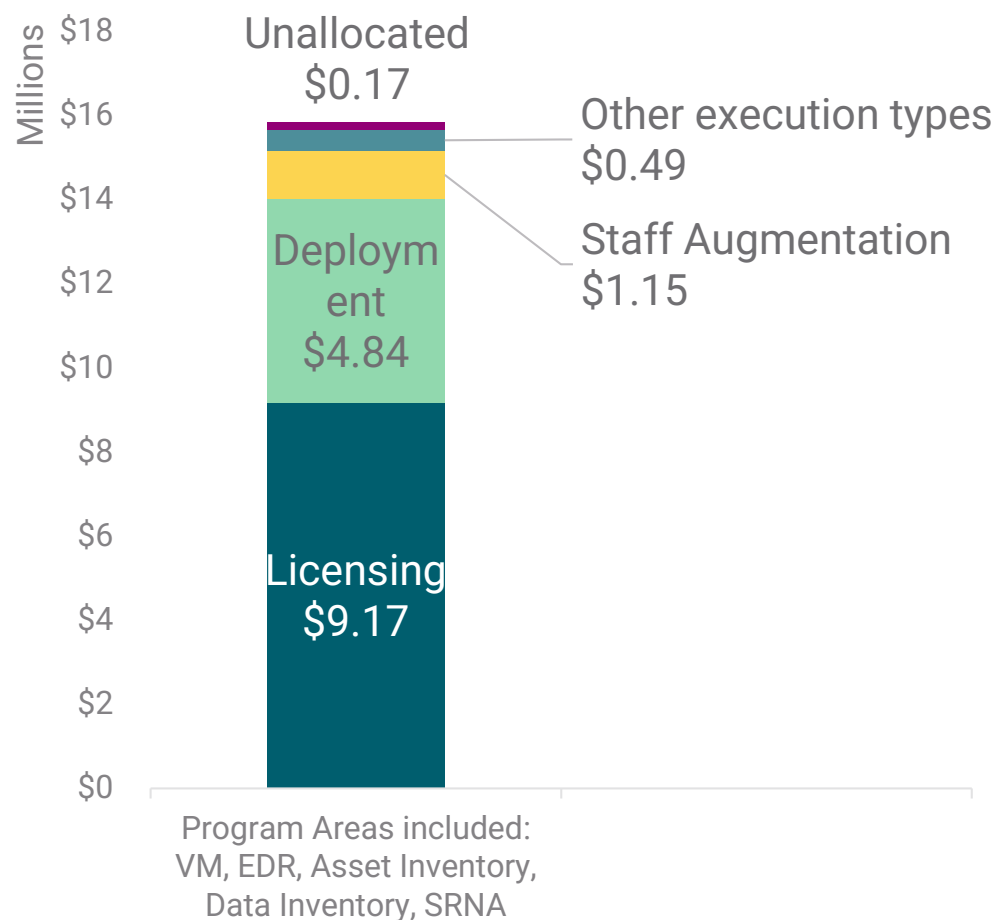
Grant year	Statewide budget	Locality SOC/ statewide ISAC	VCPC	Project support	Available
2022	\$715,238	\$702,963	\$12,275	\$0	\$0
2023	\$1,633,636	\$1,123,636	\$0	\$510,000	\$0
2024	\$1,403,315	\$1,039,065	\$5,000	\$359,250	\$0
2025	\$535,763	\$535,763	\$0	\$0	\$0
Total	\$4,287,952	\$3,401,427	\$17,275	\$869,250	\$0

Local funds by grant year

Grant year	Local (80%)	Allocated: assessments and phase 2	To be allocated
2022	\$3,814,602	\$3,814,602	\$0
2023	\$8,712,723	\$8,712,723	\$0
2024	\$7,484,344	\$5,110,300	\$2,374,044
2025	\$2,857,402	\$0	\$2,857,402
Total	\$22,869,071	\$17,637,625	\$5,231,446

Phase 2 allocation and firewall demand

Phase 2 authorization: up to \$15,829,505



Firewall demand

Network firewalls

10 localities, \$919,904 requested

Web application firewalls (WAF)

13 organizations, pricing pending

Funds available for Phase 3

Available now \$5,231,446

Plus unallocated Phase 2 \$170,514

If forecast holds \$5,401,960

Less network firewalls \$919,904

Remaining \$4,482,056

Options for moving forward

1 Open applications, then allocate

- Approve Phase 3 application process today; window open through Dec. 31
- Phase 3 allocations in January based on application volumes

2 Allocate today

- Vote a split among training, patch, firewalls and tabletop today
- Fastest start

3 Defer to Dec. 16

- Staff finalizes Phase 3 application (patching and training)
- Applications open after Dec. 16

Options 1 and 3 hold decisions on the tabletop exercise and firewalls until Phase 3 application volumes are known

The background is a solid teal color. It features several light green geometric shapes, including horizontal bars and trapezoids, some of which are partially cut off by the edges of the frame. These shapes are arranged in a way that suggests movement or a layered structure.

Decisions and Next Steps

Options for next steps

1 Open applications, then allocate

- Approve Phase 3 application process today; window open through Dec. 31
- Phase 3 allocations in January based on application volumes

2 Allocate today

- Vote a split among training, patch, firewalls and tabletop today
- Fastest start

3 Defer to Dec. 16

- Staff finalizes Phase 3 application (patching and training)
- Applications open after Dec. 16

Options 1 and 3 hold decisions on the tabletop exercise and firewalls until Phase 3 application volumes are known

Recommendations

1 Recommendations for today's meeting

- Pursue option 1: Open the Phase 3 application window through Dec. 31, 2026
- Pursue the tabletop exercise as Phase 4
- Discuss the state fund plans (locality SOC and project support); the committee decides whether to make a motion today

2 Recommendations for future meetings

- Phase 3, tabletop exercise allocations
- Firewall funding decision
- State fund plans for years 3 and 4, if not decided today

Next steps

Oct. 21

- Committee decisions today
- Phase 3 application window opens by Nov. 15

Dec. 16

- Interim update: applications received to date
- Information only, no decision requested

Dec. 31

- Phase 3 application window closes

January 2027

- Meeting date to be set
- Staff report results and recommend allocations
- Committee sets Phase 3 allocations
- Committee decides on firewall allocations
- Committee decides on tabletop allocation

Appendix

Proposed application questions: common

Every applicant answers these, whichever program it selects

1. Entity name and type
2. Primary and secondary points of contact
3. Authorized official who can sign the commitment
4. Prior participation: Capability Assessment project and each Phase 2 focus area
5. Which programs is the entity applying for: training, patch management or both?
6. Is any part of this already funded in the entity's budget?
7. Will the entity complete the limited assessment for the objectives tied to the selected programs (5.1.4 for training, 3.9 for patch management), with supporting evidence, even if it took part in the Capability Assessment Project, and agree to a reassessment afterward?

Proposed application questions: training

Applicants selecting training answer these in addition to the common questions

1. Current state capability level (0 to 4) for objective 5.1.4, with supporting evidence, and the projected future capability
2. Which content areas: baseline cyber fundamentals, frameworks and best practices, tool-specific content, AI-based security and deepfake identification, other
3. Rank preferred formats: self-paced on demand, virtual instructor-led, hybrid, in-person instructor-led (regional or on-site), hands-on labs, tool-specific modules
5. How many staff by role, how many can be released at once and for how many weeks each
6. Which Phase 2 tools does the entity want training on?
7. Has staff already been trained on those tools?
8. Number of participants
9. Baseline skills self-assessment for each potential participant (18 baseline skills, each rated confident, somewhat or not yet)
10. What could block participation?

Proposed application questions: patch management

Applicants selecting patch management answer these in addition to the common questions

1. Current state capability level (0 to 4) for objective 3.9, with supporting evidence, and the projected future capability
2. Which support: tool deployment, SOP development help, catch-up remediation
3. How does the entity patch today, and is there a written procedure?
4. Environment size and mix: workstations, servers, network devices; Windows, macOS, Linux, other
5. Which patch and vulnerability management tools are in use, and did the entity receive a Phase 2 vulnerability management tool?
6. How many systems run unsupported operating systems or software, and is replacement planned?
7. Roughly what share of systems are behind on critical and high-severity patches?
8. Can the entity rank patches by risk, such as internet-facing or critical systems?
9. Who patches today, and how many staff hours a week?
10. Would the entity accept a centrally procured tool?
11. Which SOPs are needed: schedule, testing and rollback, emergency patching, exceptions and end-of-life handling, reporting (shown if SOP help is chosen)
12. Can a contractor access systems for remediation, and what change windows apply? (shown if remediation is chosen)
13. What could block participation?

Virginia State and Local Cybersecurity Grant Program roadmap

