Virginia Cybersecurity Planning Committee

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Readoption of Remote Participation Policy	Staff
Approval of Minutes	Staff
Financial Update	Mary Fain & Mr. Watson
Phase 2 Project Status	Mary Fain & Mr. Watson
Project Outcomes & Next Steps	Mary Fain & Mr. Watson
Public Comment Period	
Other Business	Staff
Adjourn	

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

Member Remote Participation

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

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

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

Virtual Meetings

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

Requests

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

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

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

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

_____

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

Additional Explanation of Current Requirements for Remote Participation by Members

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

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

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

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

   or

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

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

Additional Explanation of Current Requirements for Minutes

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

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

Examples of disability or medical condition that prevents physical attendance:

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

Examples of personal matters that may prevent physical attendance:

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

Additional Explanation of Current Requirements for All-Virtual Meetings

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

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

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

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

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

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

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

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

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

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

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

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

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

Approval of Minutes:

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

Finances

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

Phase 2 Updates

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

Public Comment Period:

There were no public comments.

Other Business:

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

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

Adjourn

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

VIRGINIA IT AGENCY

VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT

State and Local Cybersecurity Grant Program

Cybersecurity Plan Capability Assessment Project Update

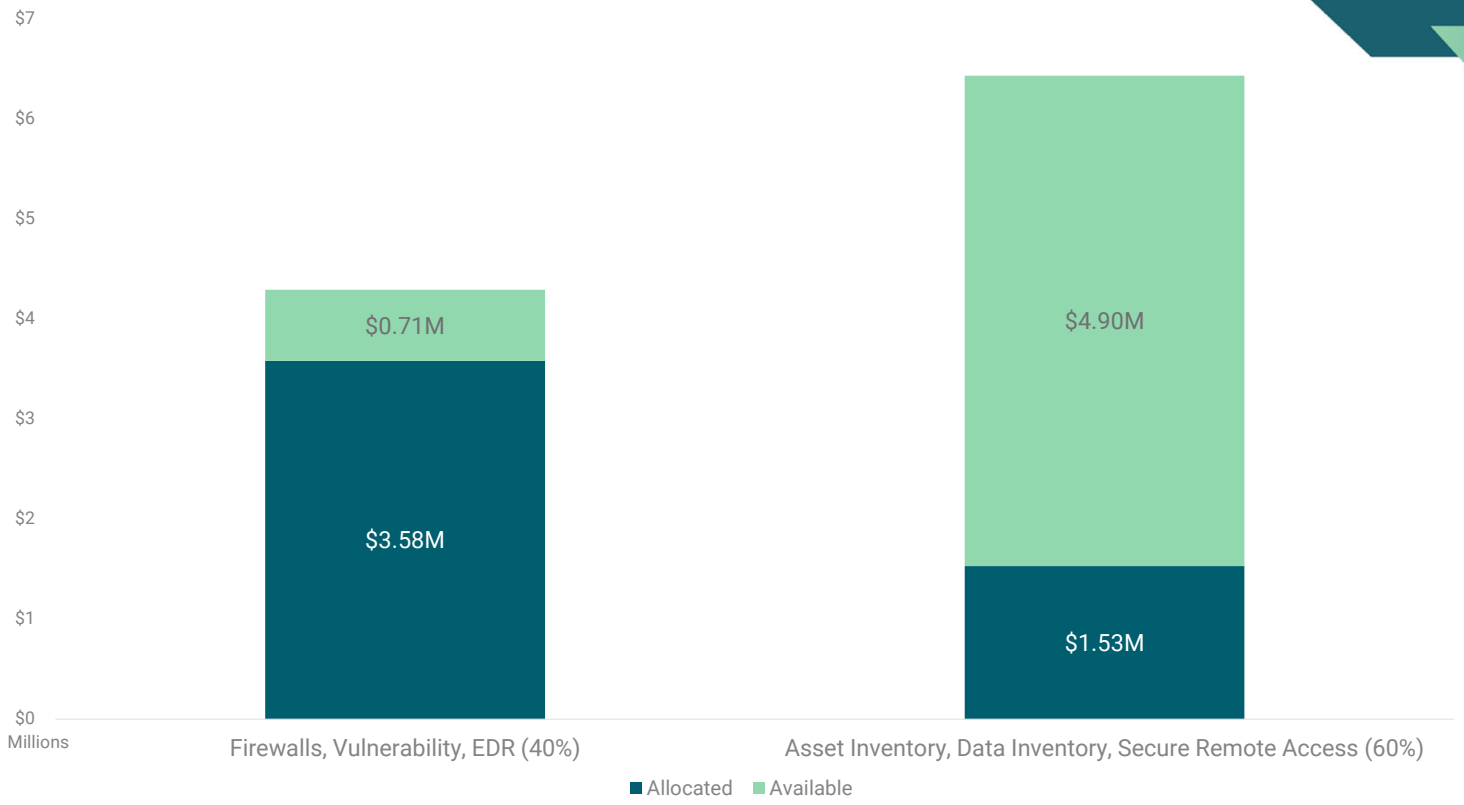
December 11, 2025

Financial Update

Financial Update

Program Year	Total Award	Federal	State Cost Share	Cost Share %	Program Category	Category Amount	Project	Project Budget	Project Budget by State Fiscal Year 2024	2025	2026	2027	2028
1 (FFY 22) Period of Performance: Dec. 1, 2022 - Nov. 30, 2026	$ 4,768,252	$4,291,426	$ 476,826	10%	M&A (5%)	$ 238,413	M&A	$ 238,413	$74,146	$ 164,267			
					Statewide (15%)	$ 715,238	Locality SOC	$ 702,963			$ 351,481	$ 351,482	
							Cybersecurity Plan and Assessments	$ 12,275		$ 7,691	$ 4,584		
					Local (80%)	$ 3,814,602	Cybersecurity Plan and Assessments	$ 58,120		$ 58,120			
							Assessment Project	$ 1,750,001		$1,750,001			
							Phase 2	$ 2,006,480			$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							

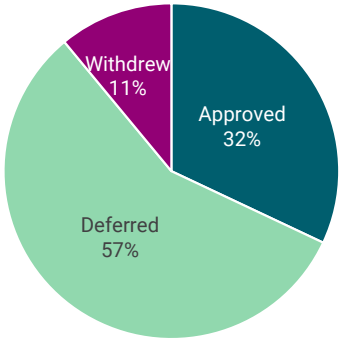
Phase 2 Allocation Tracking



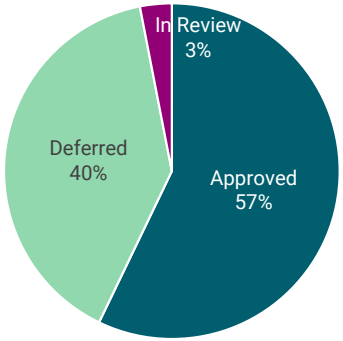
Phase 2 Update

Phase 2 Application Decision Outcomes

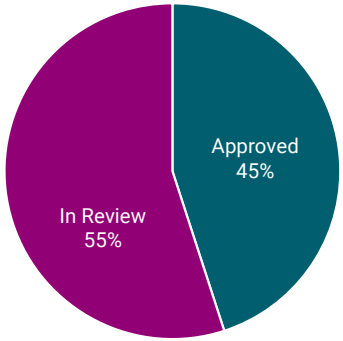
EDR



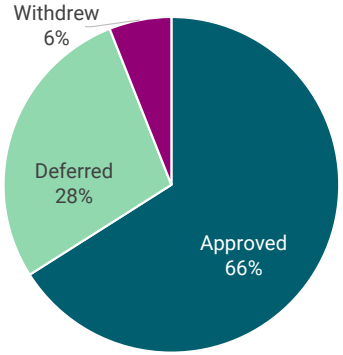
Asset Inventory



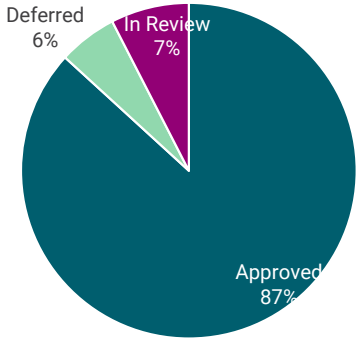
Secure Remote Network Access



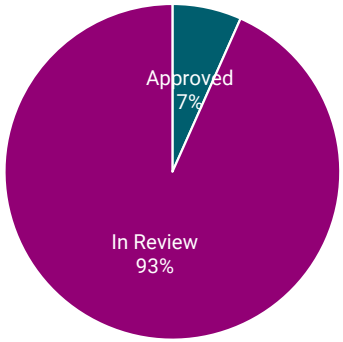
Vulnerability



Data Inventory



Firewalls



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

Status Update: EDR & Vulnerability Management

EDR	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Full Service	11	100%	73%				N/A	35%		3/31/2026	
Implementation	3	100%	67%			N/A		33%		3/31/2026	
Contract Only	2	100%	100%		N/A	N/A		50%		3/31/2026	
Additional licenses	3	100%	100%		N/A	N/A		50%		3/31/2026	
Pass-through project	0	100%	N/A	N/A	N/A	N/A	N/A	100%		3/31/2026	

Vulnerability	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Full Service	35	100%	100%				N/A	40%		3/31/2026	
Implementation	16	100%	75%			N/A		35%		3/31/2026	
Contract Only	2	100%	100%		N/A	N/A		50%		3/31/2026	
Additional licenses	4	100%	100%		N/A	N/A		50%		3/31/2026	
Pass-through project	1	100%	100%			N/A	N/A	50%		3/31/2026	

Significant changes since prior report

None.

Path to Green

Project	Path
N/A	N/A

Status Update : Asset Inventory & Data Inventory

Asset Inventory	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Asset Discovery	40	100%	60%				N/A	32%		3/31/2026	
CMDB	32	100%	84%			N/A		37%		3/31/2026	
ITAM	41	100%	60%		N/A	N/A		40%		3/31/2026	
ITSM	37	100%	62%		N/A	N/A		41%		3/31/2026	
Network Monitoring	40	100%	60%		N/A	N/A		40%		3/31/2026	
Software Asset Mgmt	43	100%	81%			N/A	N/A	45%		3/31/2026	

Data Inventory	Approved Applications	Decision Notification	Signed Consent	Detailed Planning	Deployment/ Execution	Transition - VITA	Transition - Locality	Actual % Complete	Planned % Complete	Planned Completion Date	Status
Data Discovery	43	100%	60%				N/A	32%		3/31/2026	
Data Loss Prevention	44	100%	70%			N/A		34%		3/31/2026	
Data Loss IR	41	100%	61%		N/A	N/A		40%		3/31/2026	
Device Encryption & Data Protection	40	100%	58%			N/A	N/A	40%		3/31/2026	

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

Significant changes since prior report

Initial report

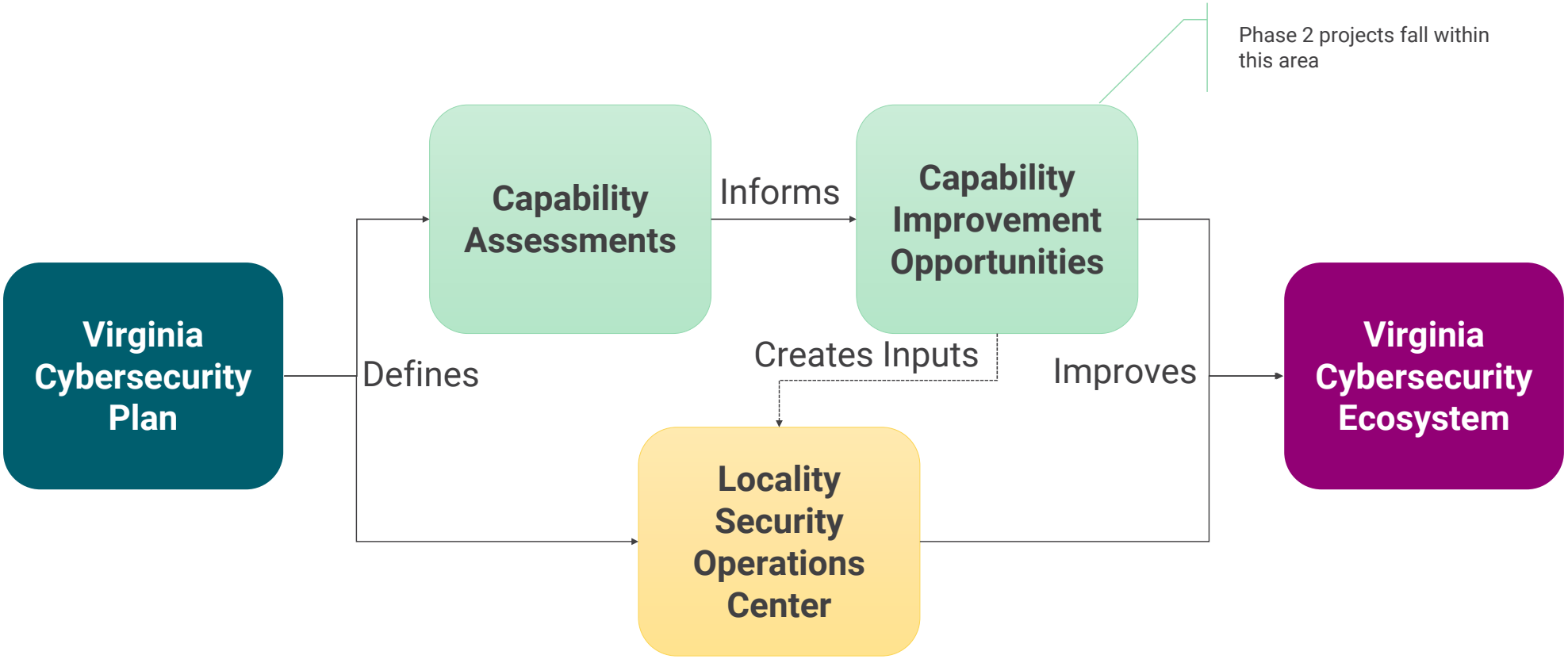
Path to Green

Project	Path
N/A	N/A

Phase 2 Projected Implementation Timeline

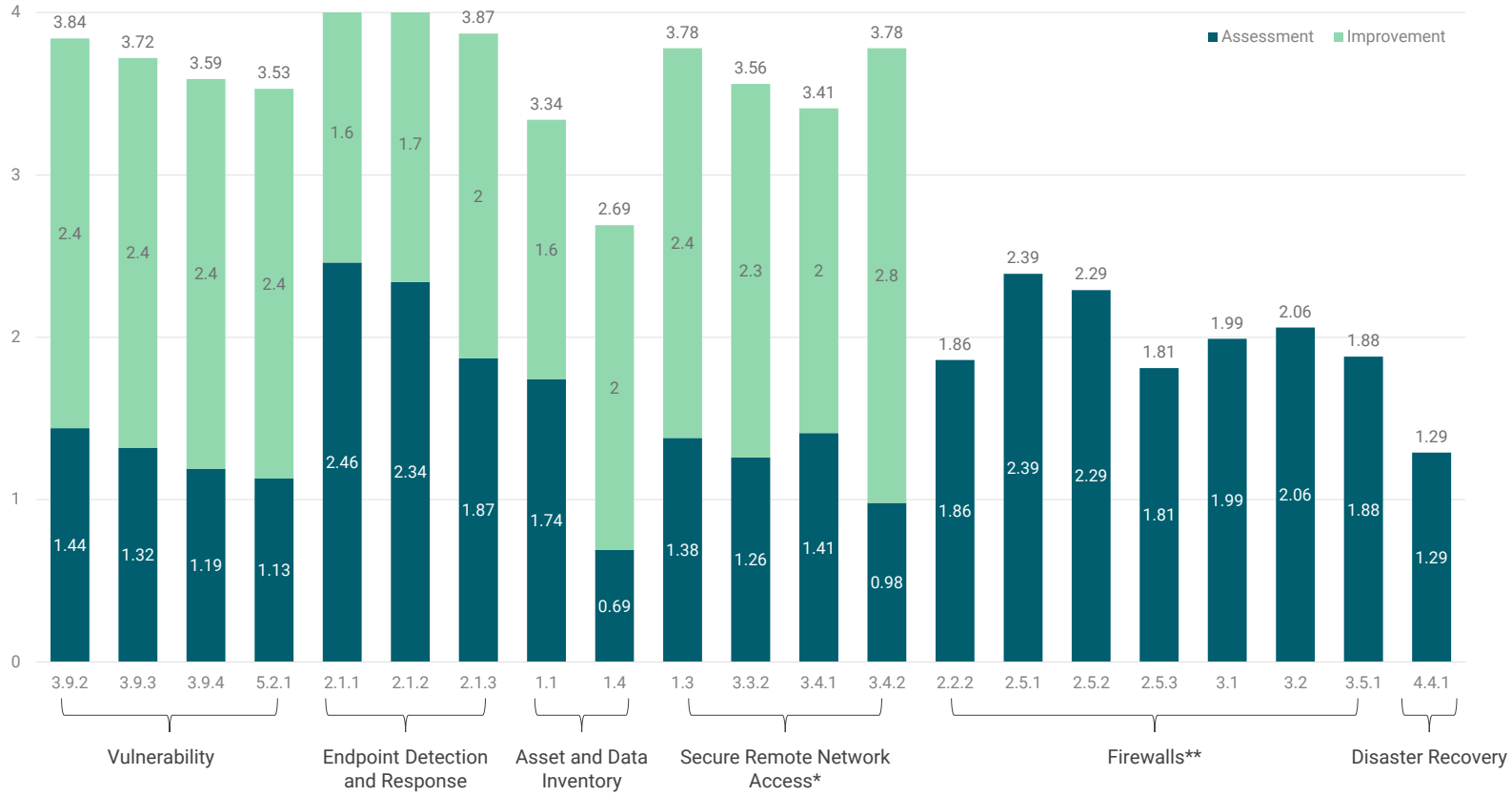
Project Area	November	December	January	February	March	April	May	June	July	August	September
EDR	Detailed Planning		Deployment				Maintenance		Close		
VM	Detailed Planning		Deployment				Maintenance		Close		
Asset Inventory				Detailed Planning	Deployment				Maintenance		Close
Data Inventory				Detailed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

Virginia SLCGP Implementation Roadmap



Phase 2 Projected Outcomes and Next Steps

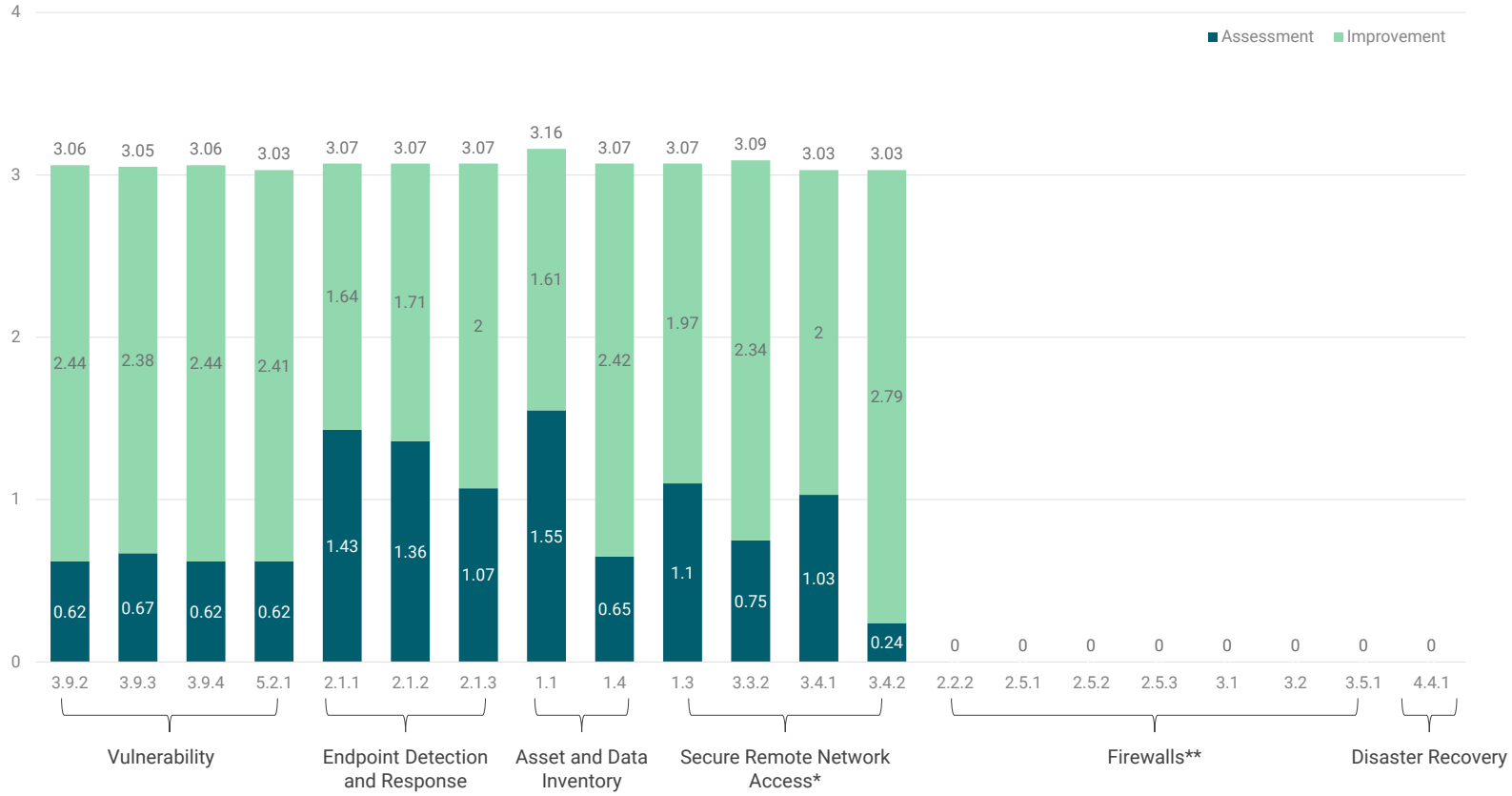
Phase 2 Applicants – Capability Improvement Impacts (all applicants)



0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

*Includes the 45% of reviewed applications
**Impact not calculated due to percentage of applications under review

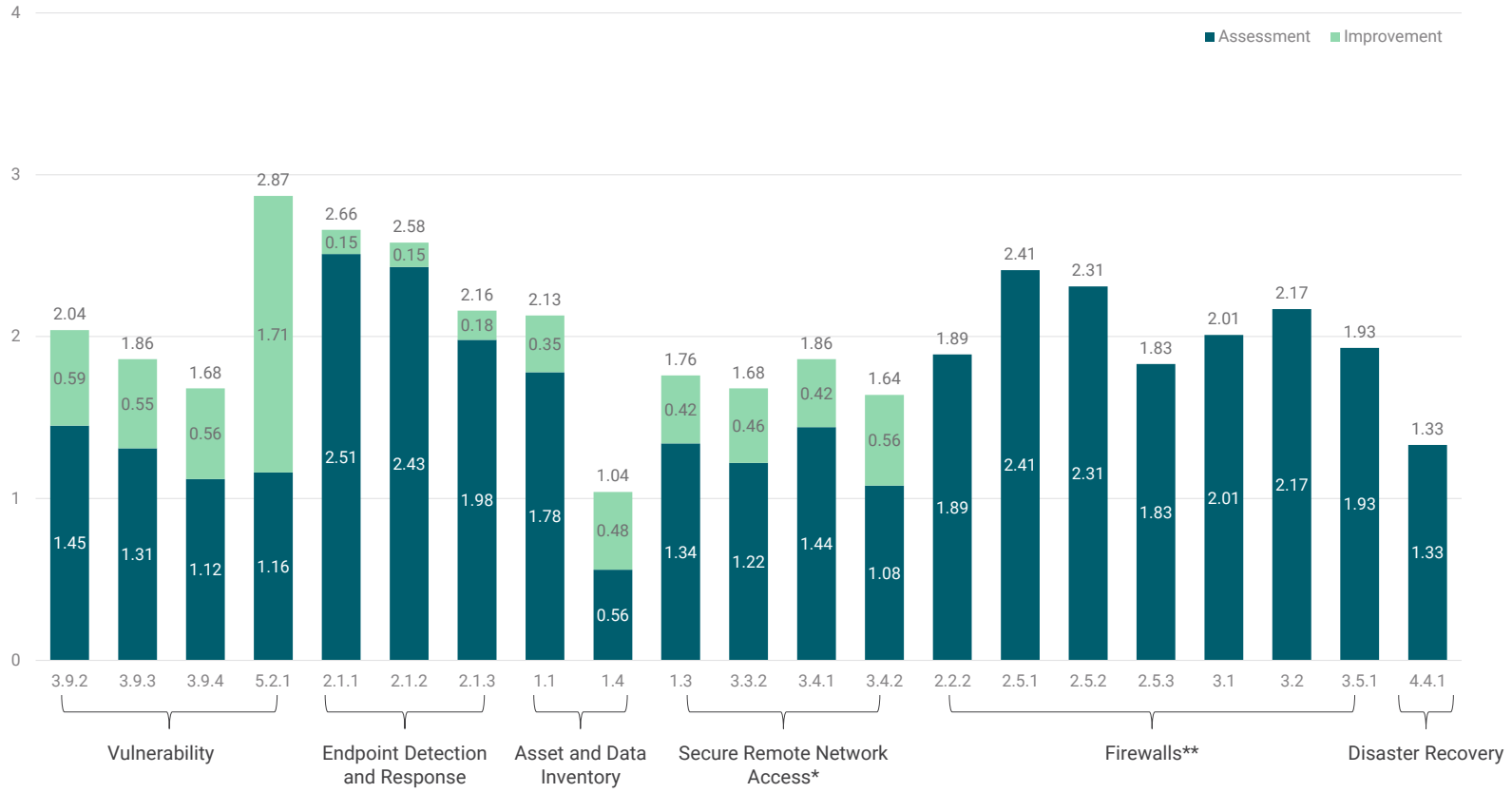
Phase 2 Applicants – Capability Improvement Impacts (approved applicants)



0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

*Includes the 45% of reviewed applications
**Impact not calculated due to percentage of applications under review

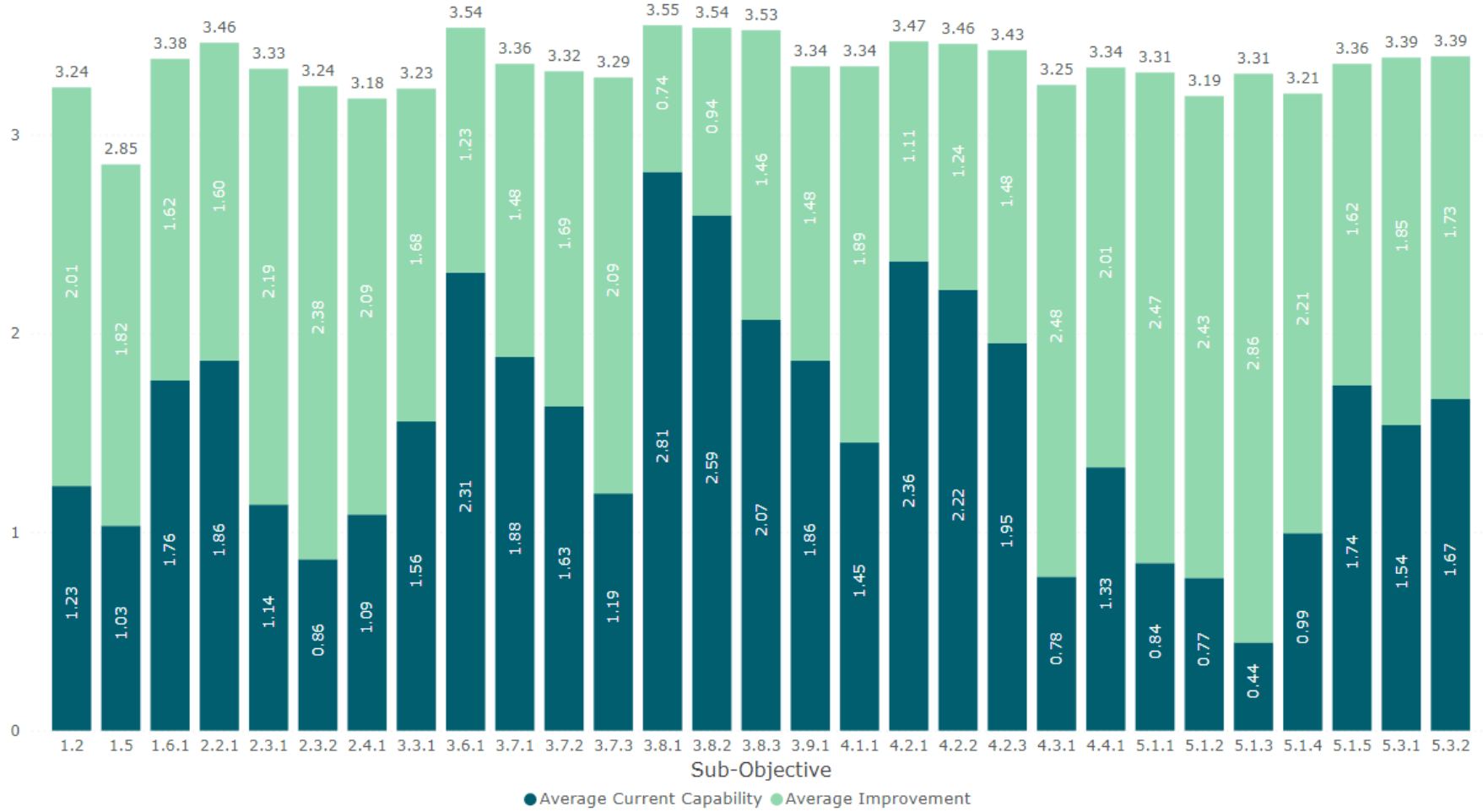
Assessment Population Post Phase 2 Implementation



0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

*Includes the 45% of reviewed applications
**Impact not calculated due to percentage of applications under review

Assessment Population Remaining Sub-Objectives



Appendix

Virginia Cybersecurity Plan – Goals, Objectives and Metrics

Goal 1: Inventory and Control of Technology Assets, Software and Data

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software)	1.1 Implement staff augmentation or third-party services to assess technology inventory	100% of devices and software recorded in inventory – (Total devices and/or software identified) / (Submitter provided initial estimate)	Frequency: Monthly Source: Submitter provided initial estimate NOTE: documentation updating the estimate may be provided at the measurement frequency
1.2 Ensure only authorized assets connected to enterprise systems and are inventoried.	1.2 Implement zero trust network access to provide only authorized systems to connect to the network	100% of authorized devices are using multi factor protected zero trust network access	Frequency: Monthly Source: # of devices connected within the 30 days / # of devices in inventory
1.3 Upgrade or replace all software no longer receiving security maintenance/support.	1.3 Implement staff augmentation or third-party services to assess and/or upgrade software without support for security updates.	100% of targeted devices are updated	Frequency: Monthly Source: # of targets / # of upgrades
1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business.	1.4 Implement staff augmentation or third-party services to assess and inventory data according to inventory requirements	100% of targeted and/or identified data sets inventoried. NOTE: If target unknown begin with estimate	Frequency: Monthly Source: Submitter provided initial estimate or target number NOTE: documentation updating the estimate may be provided at the measurement frequency
1.5 Identify all government websites and migrate non .gov sites to .gov domains.	1.5 Implement staff augmentation or third-party services to migrate existing websites to .gov addresses. This migration must include the primary government website (i.e., localityname.gov)	100% of targeted websites	Frequency: Monthly Source: Sites publicly available
1.6 Establish and maintain inventory of administrator, service, and user accounts	1.6.1 Implement staff augmentation or third-party services to inventory account information	100% of accounts	Frequency: Monthly Source: Accounts reviewed/confirmed within account directory or automated inventory
	1.6.2 Identify software and/or technology to maintain account inventory	100% of accounts	Frequency: Monthly Source: Accounts reviewed/confirmed within account directory or automated inventory

Goal 2: Threat Monitoring

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
2.1 Deploy host intrusion detection/prevention and/or endpoint detection and response for all workstations and servers.	2.1.1 Purchase and/or license preapproved host-based threat protection software	Total number of hosts running the software out of the established target Threat information collected from deployment	Frequency: Monthly Source: Asset Inventory and software deployment totals. 90% of targets Threat data from threat protection software.
	2.1.2 Implement third party services to deploy preapproved host-based threat protection software	Total number of hosts running the software out of the established target Threat information collected from deployment	Frequency: Monthly Source: Asset Inventory and software deployment totals. Threat data from threat protection software.
	2.1.3 Implement third party services to manage and maintain the preapproved host-based threat protection software deployment	Total number of hosts running the software out of the established target Threat information collected from deployment	Frequency: Monthly Source: Asset Inventory and software deployment totals. Threat data from threat protection software.
2.2 Deploy network traffic collection, filtering and detection at network egress and ingress points.	2.2.1 Implement third party services to install netflow monitoring at the egress of where a majority of server traffic is traversing or the location that has the most amount of network traffic and will support an approved configuration	At least 1 device deployed and reporting data. Target coverage 90% of assets	Frequency: Completion of installation and quarterly review of data
	2.2.2 Implement third party services to deploy and/or manage firewall, IDS/IPS technology at an organizations egress with deep packet inspection, malware detection, application awareness, intrusion detection and intrusion prevention	Devices deployed. Reports on threat activity available Target coverage 90%	Frequency: Completion of information and quarterly review of data
2.3 Centralize security event alerting.	2.3.1 Implement and maintain or have third party services implement and maintain security event collection technology to connect to the preapproved security operations center	Devices deployed. Reports on threat activity available	Frequency: Completion of information and quarterly review of data
	2.3.2 Implementation of a Commonwealth security operations center and/or information sharing and analysis center	Devices deployed. Reports on threat activity available	Frequency: Completion of information and quarterly review of data

Goal 2: Threat Monitoring

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
2.4 Audit log collection for all servers and systems hosting data in accordance with log management standards.	2.4.1 Establish data collection points for system audit logs	% of systems reporting logs % of event log sources compliant with standards	Frequency: Monthly Source: Asset inventory and log collection system
2.5 Web application firewall	2.5.1 Purchase and/or license preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.
	2.5.2 Implement third party services to deploy preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.
	2.5.3 Implement third party services to manage and maintain the preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.

Goal 3: Threat Protection and Prevention

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
3.1 Implement and manage firewalls on all end point devices (i.e., user workstations, servers)			
3.2 Implement and manage network firewalls for ingress and egress points			
3.3 Encrypt sensitive data in transit and on devices hosting sensitive data	3.3.1 Obtain certificates to support encrypted transmissions	Number of public-facing hosted systems with approved encryption	Frequency: Monthly Sources: Websites with approved encryption
	3.3.2 Implement and/or manage zero trust network access connectivity (ZTNA VPN)	Number of non-public facing systems potentially accessible	Frequency: Quarterly Sources: Number of devices remotely accessible using multifactor login
3.4 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access	3.4.1 Implement multifactor authentication to systems.	Accounts implemented with multifactor. Target: 100% Minimum: 90%	Source: Target accounts per system or in the environment Frequency: Monthly
	3.4.2 Implement multifactor authentication for Virginian identities	Accounts implemented with multifactor. Target: 100% Minimum: 90%	Source: Target accounts per system or in the environment Frequency: Monthly
3.5 Domain Name System (DNS) Filtering/Firewall	3.5.1 Implement or have third party services implement and configure hosts to utilize approved DNS filtering services	Hosts leveraging DNS filtering / Total hosts in the environment. Target: 100% Minimum: 90%	Sources: Number of devices in organization inventory Frequency: Monthly

Goal 3: Threat Protection and Prevention

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
3.6 Email filtering and protection	3.6.1 Implement or have third party hosts implement email filtering for incoming email services	Filters covering email users. Target: 100% Minimum 95%	Sources: Number of emails in the directory and number of emails protected by the filter Frequency: Monthly
3.7 Centralized authentication and authorization (Single Sign On)	3.7.1 Obtain licenses for single sign on software.	Number of organization users with single sign on Number of Virginians with single sign on	Sources: User access list Frequency: Monthly
	3.7.2 Implement or have third party services implement single sign on	Number of organization users with single sign on Number of Virginians with single sign on	Sources: User access list Frequency: Monthly
	3.7.3 Manage or have a third party manage single sign on solutions	Number of organization users with single sign on Number of Virginians with single sign on	Sources: User access list Frequency: Monthly
3.8 Content and malicious traffic filtering through anti-virus and threat detection software	3.8.1 Obtain licenses for content/malicious traffic filtering	Number of hosts with filtering and detection	Sources: asset inventory and protected system list Frequency: Monthly
	3.8.2 Implement or have third party services implement content/malicious traffic filtering	Number of hosts with filtering and detection	Sources: asset inventory and protected system list Frequency: Monthly
	3.8.3 Maintain or have a third party maintain content/malicious traffic	Number of hosts with filtering and detection	Sources: asset inventory and protected system list Frequency: Monthly
3.9 Ensure patch management program is implemented and up to date	3.9.1 Have a third-party upgrade out of date systems	Hosts scanned within 30 days Hosts updated to supported software within n-1 of most recent release	Source: Vulnerability software and asset inventory Frequency: Monthly
	3.9.2 Obtain licenses for vulnerability management software	Hosts scanned within 30 days Hosts updated to supported software within n-1 of most recent release	Source: Vulnerability software and asset inventory Frequency: Monthly
	3.9.3 Implement or have a third party implement vulnerability management program and/or software	Hosts scanned within 30 days Hosts updated to supported software within n-1 of most recent release	Source: Vulnerability software and asset inventory Frequency: Monthly
	3.9.4 Maintain or have a third party maintain a vulnerability management program	Hosts scanned within 30 days Hosts updated to supported software within n-1 of most recent release	Source: Vulnerability software and asset inventory Frequency: Monthly

Goal 4: Data Recovery and Continuity

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
4.1 Establish and maintain a data recovery process	4.1.1 Develop or have a third party develop a business continuity plan and/or disaster recovery plan that enables the recovery of critical information systems that support business processes for all cloud based and locally stored data.	100% of Critical services will be brought online within 72 hours	Source: Asset inventory Frequency: Once
4.2 Establish and maintain an isolated/vaulted instance of recovery data	4.2.1 Obtain licenses for a vaulted data recovery solutions	90% of critical data vaulted	Frequency: Source Source: Total GB of data vaulted out of total GB of critical data
	4.2.2 Implement or have a third party implement a vaulted data recovery solution for critical backups	90% of critical data vaulted	Frequency: Source Source: Total GB of data vaulted out of total GB of critical data
	4.2.3 Have a third party maintain a vaulted data recovery solution	90% of critical data vaulted	Frequency: Source Source: Total GB of data vaulted out of total GB of critical data
4.3 Implement disaster recovery and data recovery testing	4.3.1 Have a third party test the disaster recovery and/or business continuity plan	Successful recovery within plan established time frame	Frequency: Once Source: Disaster recovery plan information
4.4 Implement technology to support continuity of services in the case of a natural disaster or cyber attack	4.4.1 Obtain or have a third party provide services to maintain communications in the case of a regional disaster within 500 miles	Successful test of continuity services	Frequency: Semi-Annually Source: Recovery plan and certification of completion

Goal 5: Security Assessment

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description (details, source, frequency)**
5.1 Identify security gaps associated with program objectives which can be supported by the grant program	5.1.1 Have staff augmentation provide an assessment or have a third-party assessment of the technology environment for services supported by the grant program	Assessment completion within 120 days	Frequency: Quarterly
	5.1.2 Obtain services to review and evaluate existing risk assessments/mitigation plans for potential options	Mitigation plans can begin within 30 days	Frequency: Quarterly
	5.1.3 Obtain a service or have a third party provide a skills review for necessary cybersecurity skills in the environment based on the NIST NICE framework		
	5.1.4 Obtain security training used to train or educate personnel for careers in cybersecurity	Training to begin within 90 days of award	Frequency: Quarterly
	5.1.5 Obtain security awareness training for end users	Training to begin within 90 days of award	Frequency: Quarterly
5.2 Perform automated vulnerability scans	5.2.1 Obtain third-party services to provide a vulnerability scan and assessment of the environment	Obtain a vulnerability review report within 90 days Mitigations to be done with a target of 30 days of report	Source: Vulnerability assessment Frequency: Monthly
5.3 Network and system architecture diagram and assessment	5.3.1 Obtain software to provide a network map of the environment	Network architecture documentation	Source: Asset inventory and network architecture Frequency: Once All assets and/or asset types must be identifiable on the architecture
	5.3.2 Obtain staff augmentation or have a third-party document the organizations network architecture	Network architecture documentation	Source: Asset inventory and network architecture Frequency: Once All assets and/or asset types must be identifiable on the architecture