

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Financial Update	Mary Fain
Overview of Applications	Mary Fain
Analysis & Recommendations [VOTE]	Mike Watson
Public Comment Period	
Other Business	Staff
Adjourn	



Virginia Cybersecurity Planning Committee
January 23, 2025 – 10:00 a.m.
All Virtual Meeting

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10 am. Mr. Watson welcomed the members to the all virtual meeting. Mr. Watson noted meeting materials were available on the Regulatory Town Hall Website, opportunity for public comment, and audio-visual requirements for members.

Presiding:

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

Members Present:

Troy Atkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe
Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
Robbie Coates, Director, Grant Management and Recovery, VDEM
Adrian Compton, Tribal Administrator, Monacan Indian Nation
Charles DeKeyser, Major, Virginia Army National Guard
Michael Dent, Chief Information Security Officer, Fairfax County Department of Information Technology
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Charles Huntley, Director of Technology, County of Essex
Derek M. Kestner, Information Security Officer, Supreme Court of Virginia
Uma Marques, Information Technology Director, Roanoke County Government
Kenneth Pfeil, Chief Data Officer, Office of Data Governance and Analytics
Glendon Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services
Brandon Smith, Chief Information Officer, Department of Elections
Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security, Office of the Governor
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black
Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Staff Present:

Mary Fain, Project Manager, Virginia IT Agency
Joshua Heslinga, Director of Legal & Legislative Services, Virginia IT Agency
Mylam Ly, Legal Compliance & Policy Specialist, Virginia IT Agency

Review of Agenda:

Ms. Watson provided an overview of the agenda.

Approval of Minutes:

The October meeting minutes were displayed on the screen. Upon a motion by Mr. Schmitz and duly seconded by Mr. Smith, the committee unanimously voted to adopt the October meeting minutes.

Financial Update

Ms. Fain provided a financial update. A few projects have spent funds. The locality SOC is one of these projects and is intended to use federal FY 2022 and FY 2023 funds. VITA has paid for and completed the cybersecurity capability assessments project, which amounted to ~\$1.8 million.

Phase 2 Communication

Ms. Fain provided an update on the Phase 2 Communication plan and reviewed the plan for email, social media (Facebook, LinkedIn and X) and other modes of communication on the phase 2 application cycle. Outreach also includes presentations at the Virginia Local Government IT Executives (VALGITE) February meeting, and three VITA-hosted virtual information sessions. Key messaging included application availability, timeline, project areas, execution options and eligibility requirements. Staff will continue to send messaging on a regular cadence along the timeline aligned with major application milestones.

Annual Review of the Cybersecurity Plan

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

- Updating the members of the committee
- Renumbering and reorganizing sub-objectives which had a typo or were misplaced.
- Adding a project to Appendix B

Upon a motion by Mr. Smith and duly seconded by Mr. Kestner, the committee unanimously voted to adopt the amended cybersecurity plan.

FY24 Application Status Update

Mr. Coates provided an update on the FY24 Application. The application was approved by FEMA with:

- \$6,548,801 – federal share
- \$2,806,629 - cost share
- \$9,355,430 - total

Public Comment Period:

There were no public comments.

Other Business:

Mr. Watson opened the floor for other business. The next VCPC meeting is February 11 at 1pm. There was a brief legislative update. The most relevant legislative item is a proposed budget amendment providing additional funds for the state cost share to offset the cost share gap created because the initial state appropriation of cost share funds occurred before the Notice of Funding Opportunity was released. There are additional potentially-relevant bills, including regarding IT technology and foreign adversaries and IT accessibility. A further legislative update will be presented at a future VCPC meeting once session ends.

Adjourn

Upon a motion by Mr. Dent and duly seconded by Mr. Smith, the committee unanimously voted to adjourn the meeting at 10:35am..



State and Local Cybersecurity Grant Program

Cybersecurity Plan Capability Assessment Project Update

As of March 14, 2025

The background is a solid teal color. It features several light green geometric shapes, including horizontal bars and trapezoidal shapes, some of which are layered or overlapping, creating a modern, abstract design.

Financial Update

Financial Update

Program Year	Total Award	Cost Share %	Program Category	Category Amount	Project	Project Budget	Project Budget by State Fiscal Year					Balance
							2024	2025	2026	2027	2028	
1 (FFY 22) Period of Performance: Dec. 1, 2022 - Nov. 30, 2026	\$ 4,768,252	10%	M&A (5%)	\$ 238,413	M&A*	\$ 238,413	\$ 74,146	\$ 89,316	\$ 74,951			\$ -
			Statewide (15%)	\$ 715,238	Locality SOC	\$ 715,238			\$ 357,619	\$ 357,619		\$ -
			Local (80%)	\$3,814,602	Establish Cybersecurity Plan	\$ 128,740		\$ 42,913	\$ 42,913	\$ 42,913		\$ 84,926
					Assessment Project Phase 2	\$ 1,893,046	\$ 1,808,120					
2 (FFY 23) Period of Performance: Dec. 1, 2023 - Nov. 30, 2027	\$10,890,904	20%	M&A (5%)	\$ 544,545	M&A	\$ 544,545			\$ 181,515	\$ 181,515	\$ 181,515	\$ -
			Statewide (15%)	\$1,633,636	Locality SOC	\$ 1,633,636			\$ 544,545	\$ 544,545	\$ 544,545	\$ -
			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	\$ 6,548,801	30%	M&A (5%)	\$ 327,440	M&A	\$ 544,545						
			Statewide (15%)	\$ 982,320								
			Local (80%)	\$5,239,041								
4 (FFY 25)			<i>Not available to apply</i>									

*State FY25 YTD actual; amount will increase by end of fiscal year

Legend

- Actual
- Planned

The background is a solid teal color with several light green geometric shapes, including horizontal bars and trapezoids, scattered across the page.

Phase 2 Project Applications

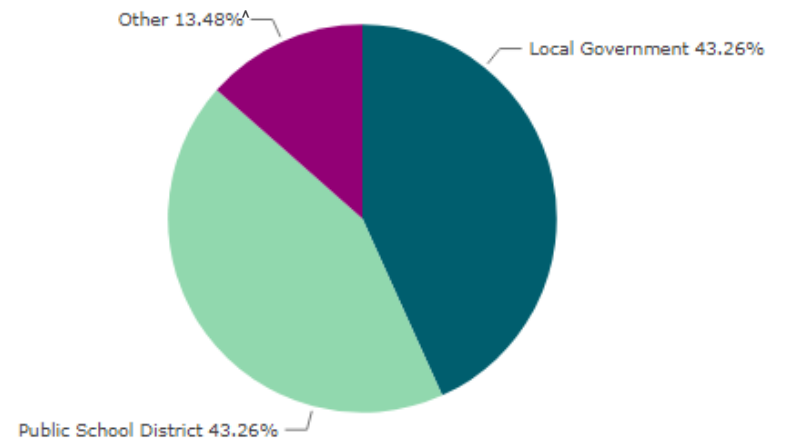
Applicant Overview

Applications were received from 141 qualified organizations across the Commonwealth representing various types of local government

Geographic Reach

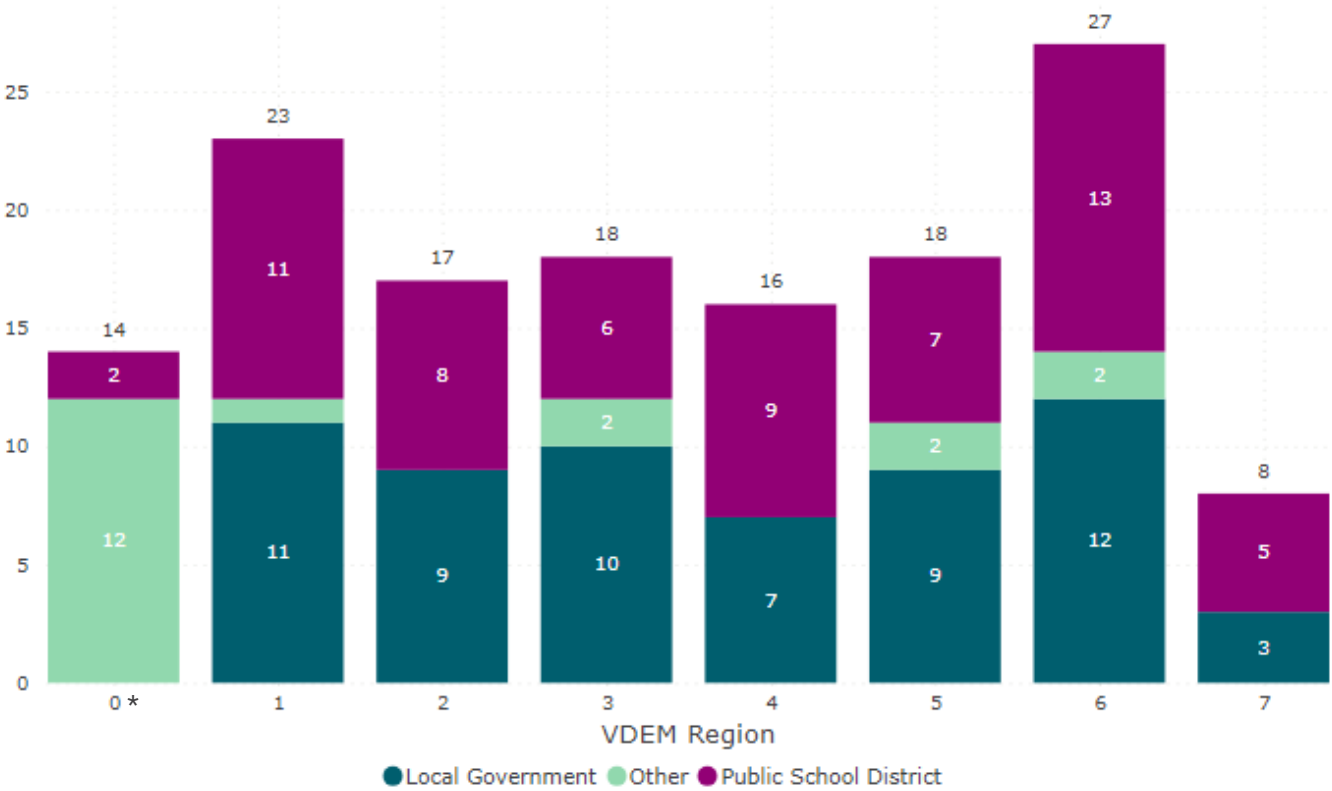
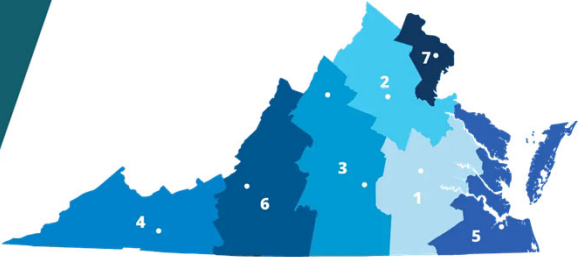


Organization Type



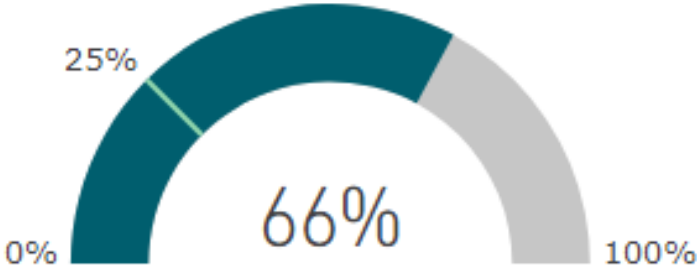
^Includes tribal government, authorities and other local government entities

Applicants by VDEM region

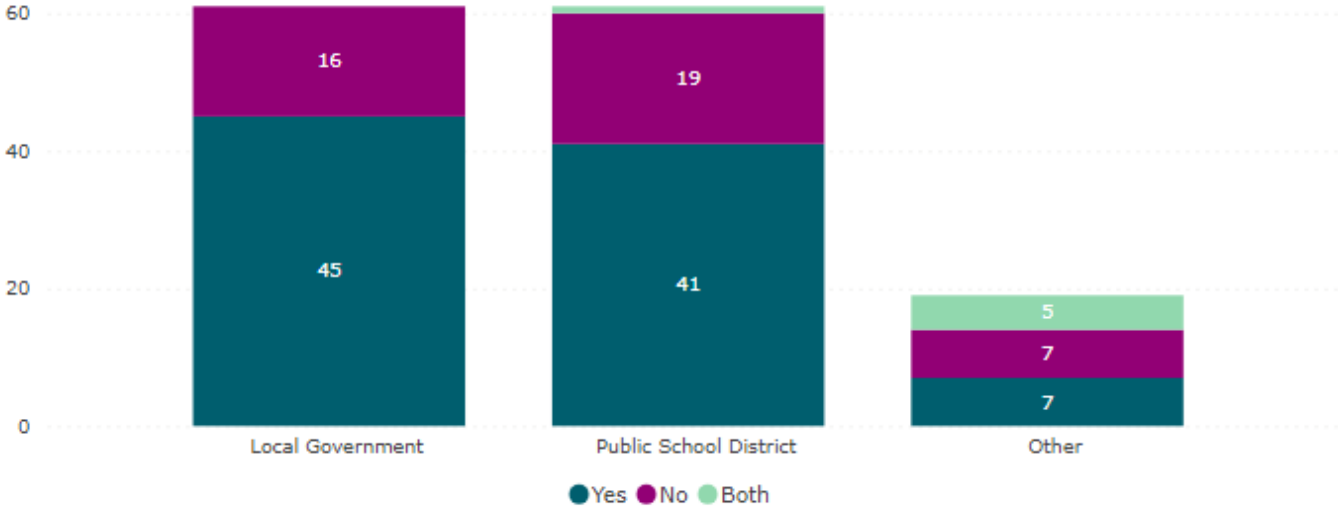


*Region 0 – organization crosses VDEM regions

Number of applicants exceeded 25% rural requirement*



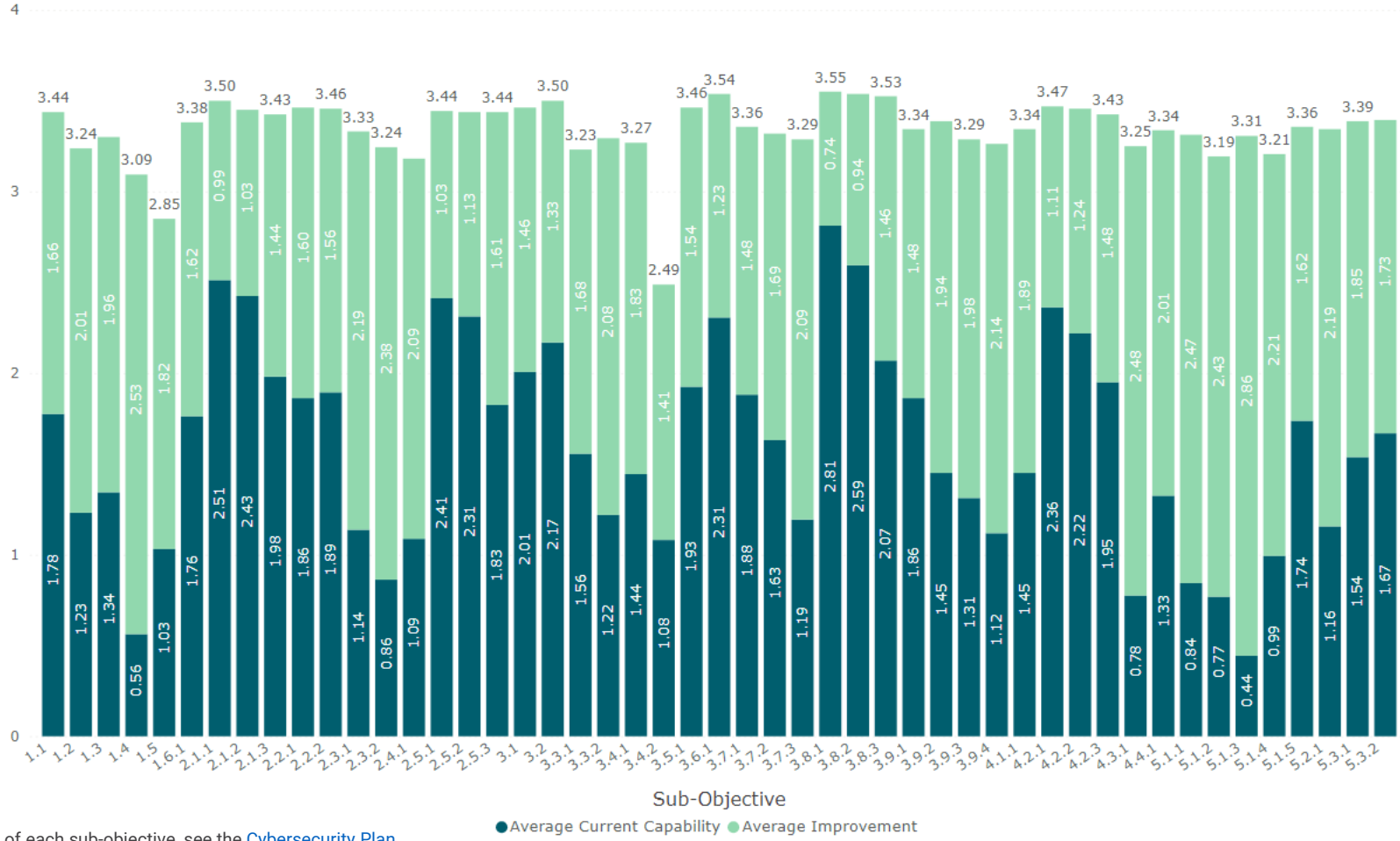
Organization Types by Rural Status



*Based on number of applicants, not on approved funding

Application Data Overview

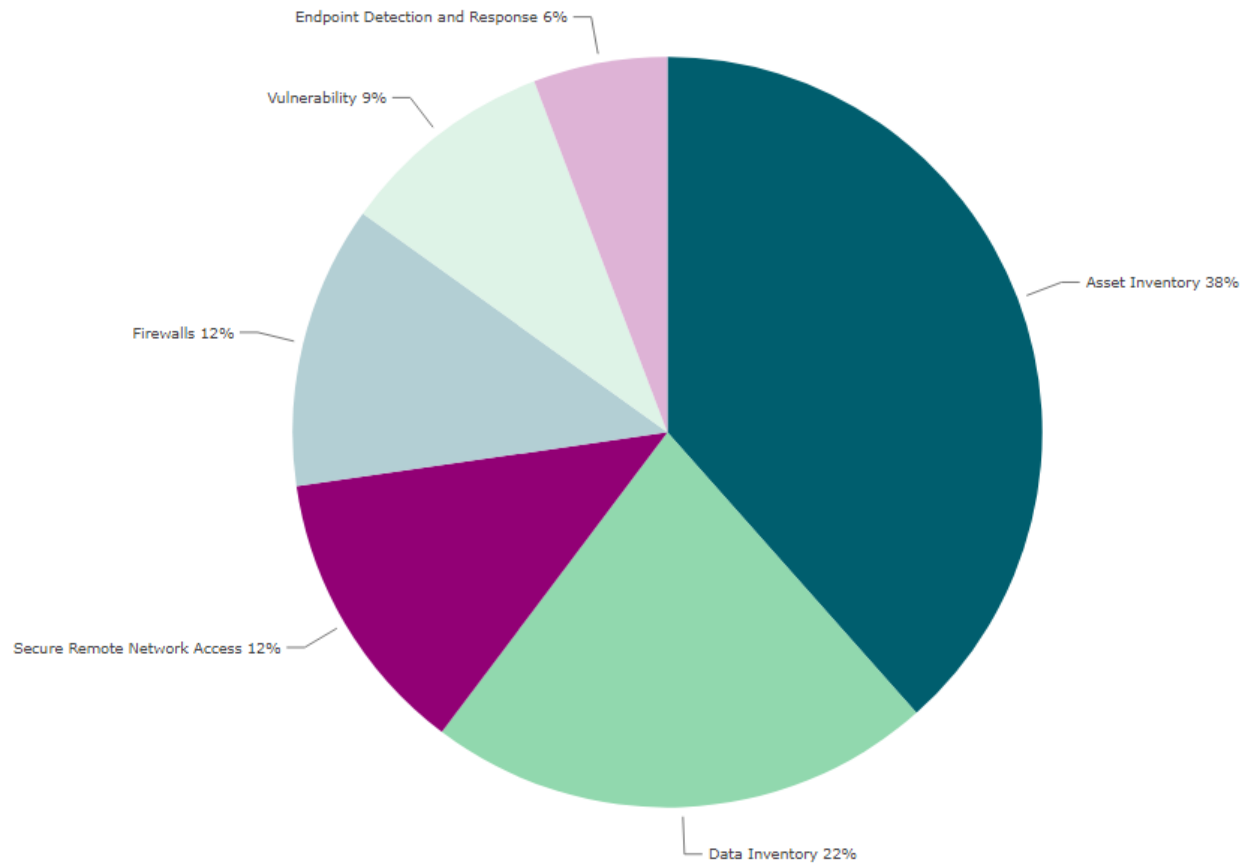
Local Pass-Through Decision Option 3: Blended



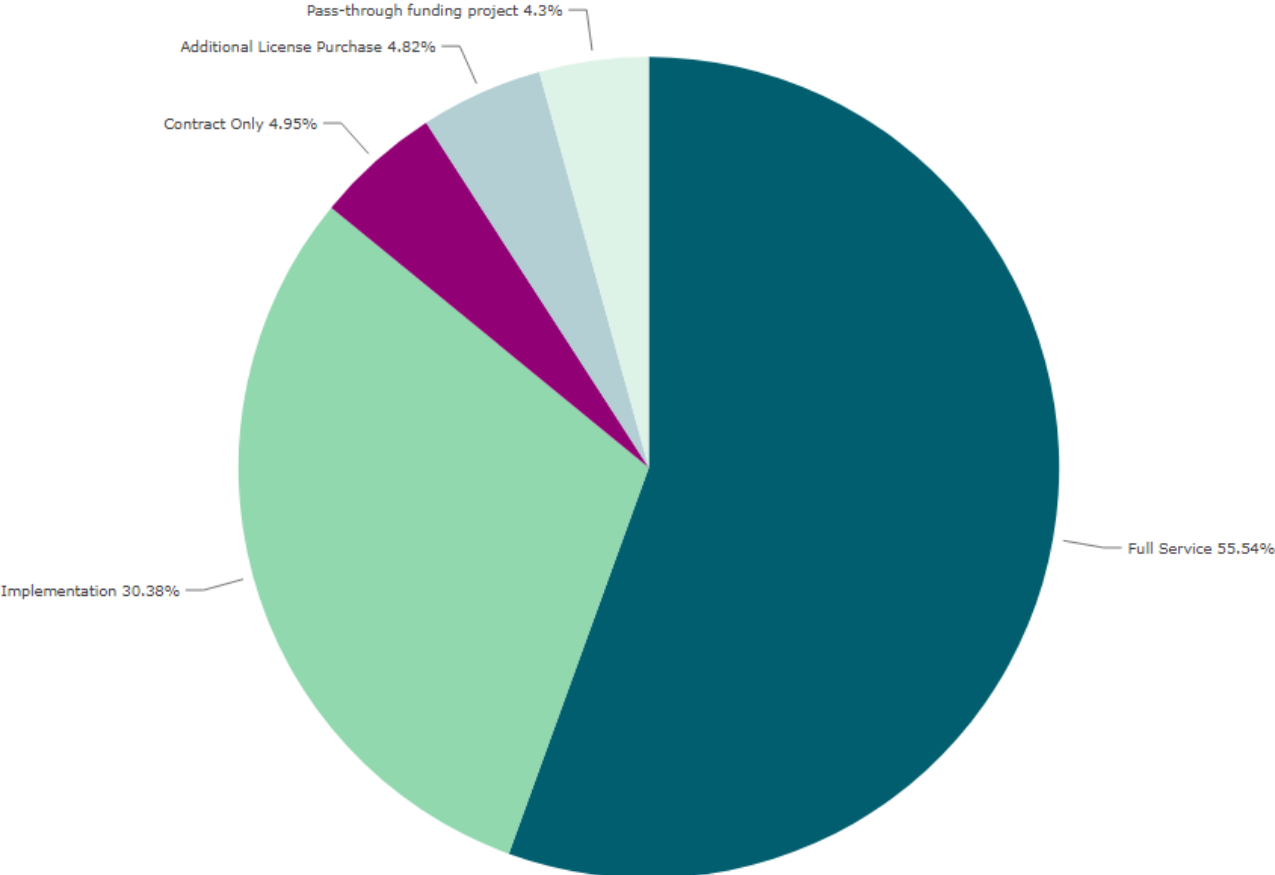
- Recommended Sub-Objectives**
- Vulnerability**
 - 3.9.2
 - 3.9.3
 - 3.9.4
 - 5.2.1
 - Secure Remote Network Access**
 - 1.3
 - 3.3.2
 - 3.4.1
 - 3.4.2
 - Data and Asset Inventory**
 - 1.1
 - 1.4
 - Disaster Recovery**
 - 4.4.1
 - EDR**
 - 2.1 (all sub-objectives)
 - Firewalls**
 - 2.2.2
 - 2.5 (all sub-objectives)
 - 3.1
 - 3.2
 - 3.5.1
- Phase 2 Application Scope

To view details of each sub-objective, see the [Cybersecurity Plan](#)

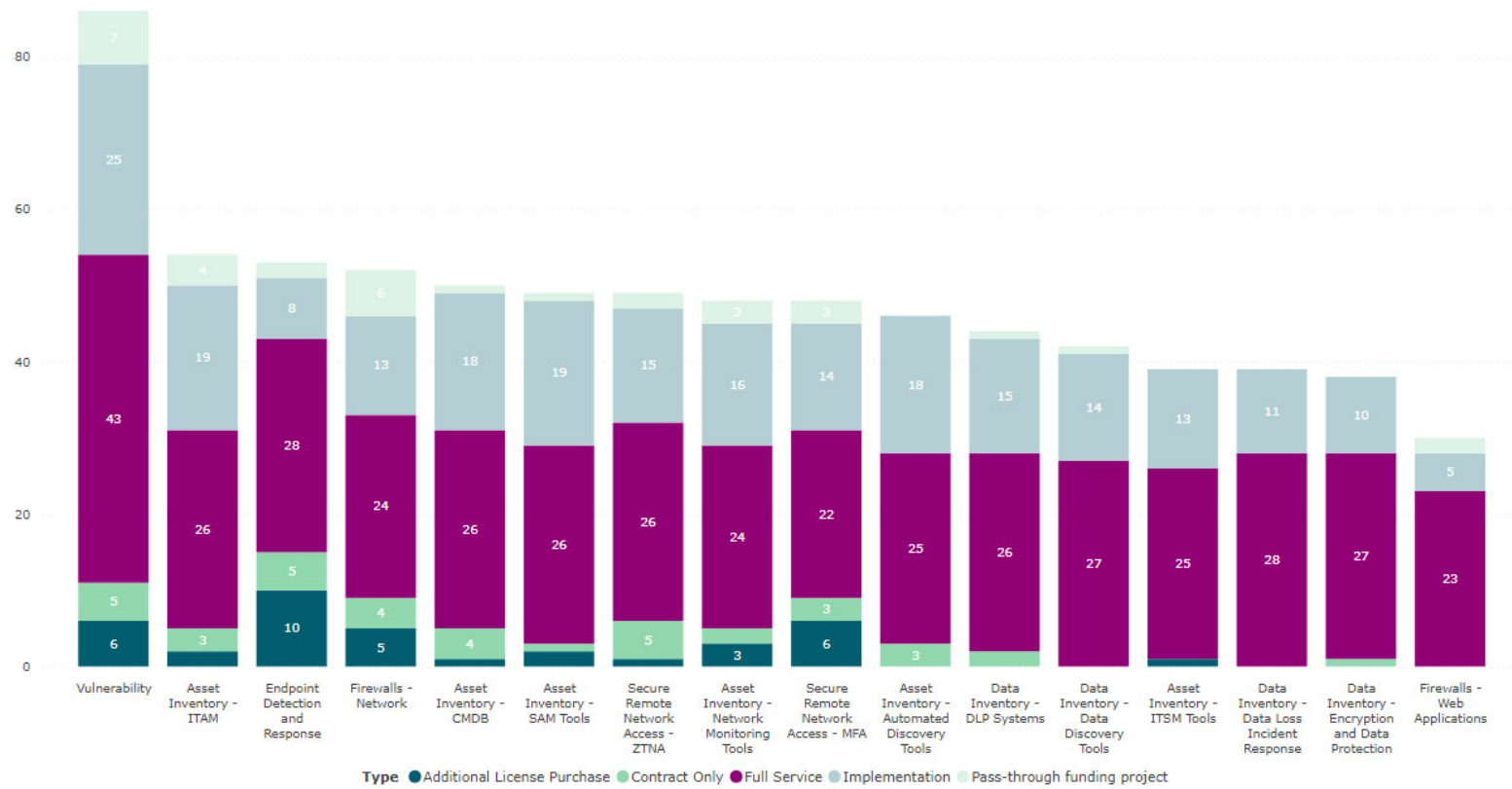
Requested Project Areas



Requested Project Execution Type



Applications by Project Area and Execution Type

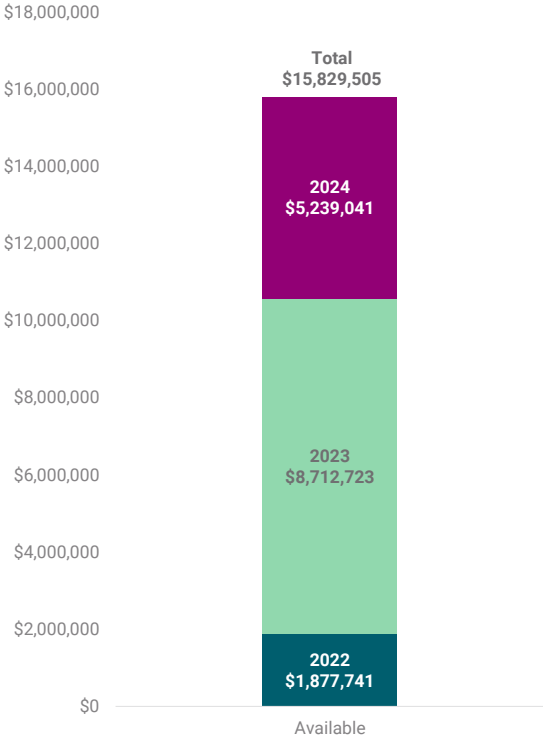


The background is a solid teal color with several light green and teal geometric shapes, including horizontal bars and trapezoids, arranged in a modern, abstract pattern.

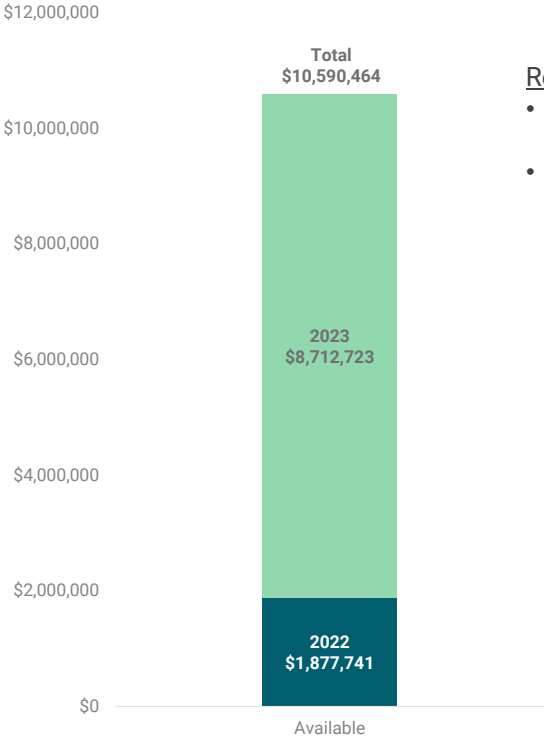
Analysis and Recommendations

Available Funding

Total Potential Funding Amount



Total Recommended Funding Amount



Recommendation

- Prioritize funding from grant years 2022 and 2023
- Target \$10.6M and authorize up to full \$15.8M due to uncertainty at the federal level

Funding Prioritization Recommendation Methodology

Reviewed available data and utilized:

- Organization eligibility per NOFO
- Assessment data
 - Current capability level
 - Future capability level

Capability Level	Definition
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

- Likelihood of success

Likelihood	Definition
High	Necessary resources and skills needed for implementation and/or maintenance are available
Medium	At least some resources and/or skills necessary to implement and/or maintain are present
Low	May not be sufficient resources, skills necessary to implement and/or maintain

Funding Prioritization Options for Project Areas

Project Area	Recommended			
	Option 1 All Applications	Option 2 Current capability = 0 Future capability = 3 - 4 Likelihood of Success = High	Option 3 Current capability = 0 - 1 Future capability = 3 - 4 Likelihood of Success = High	Option 4 Current capability = 0 - 2 Future capability = 3 - 4 Likelihood of Success = High
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%

- Minimum anticipated improvement = +2 per goal/objective
- Focused on organizations with highest likelihood of success

Any option will result in improvements for the Commonwealth

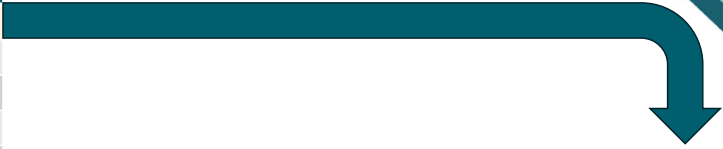
Project Area Funding Prioritization Criteria

Recommendations based on:

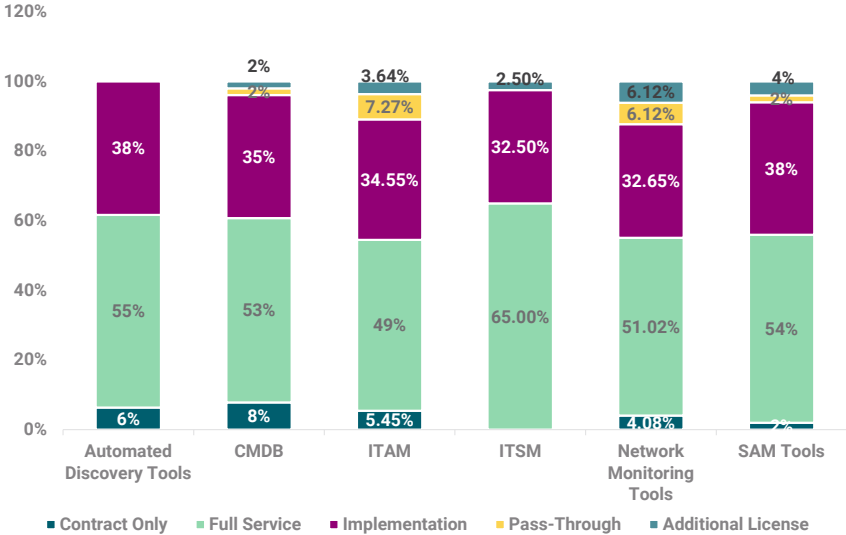
1. Prior qualification requirements
2. Current state capability level
3. Future state capability level
4. Likelihood of success
5. Preliminary review of applications

Asset Inventory Projects Funding Prioritization Recommendation

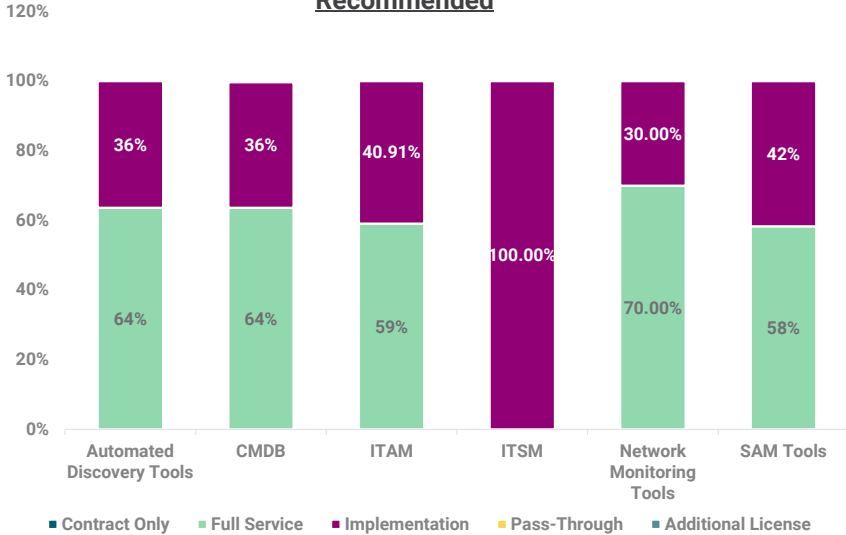
Project Area	Option 1	Option 2	Option 3	Option 4
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%



All Requests



Recommended

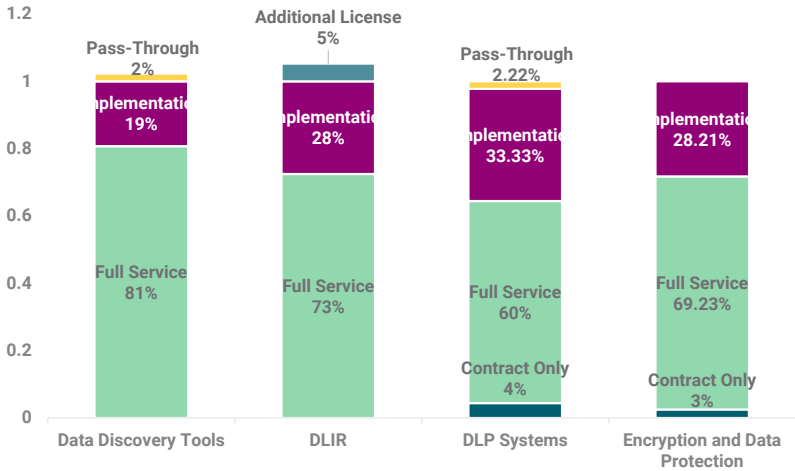


Data Inventory Projects Funding Prioritization Recommendation

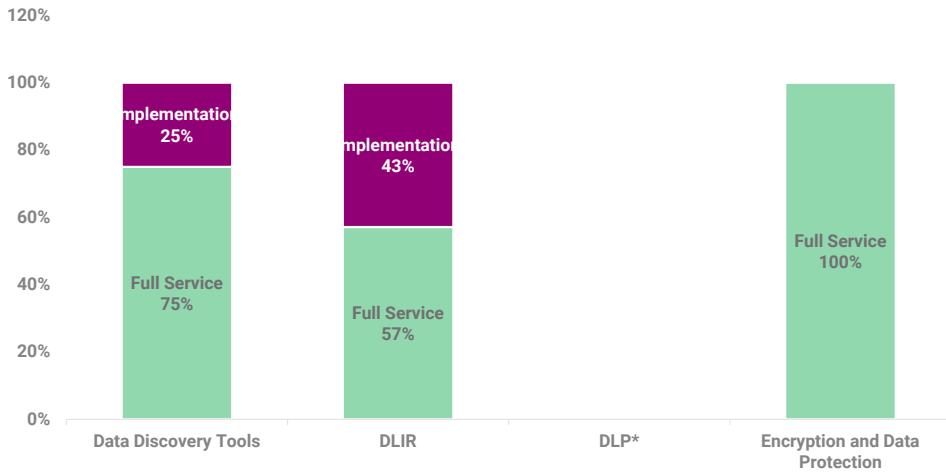
Project Area	Option 1	Option 2	Option 3	Option 4
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%



All Requests



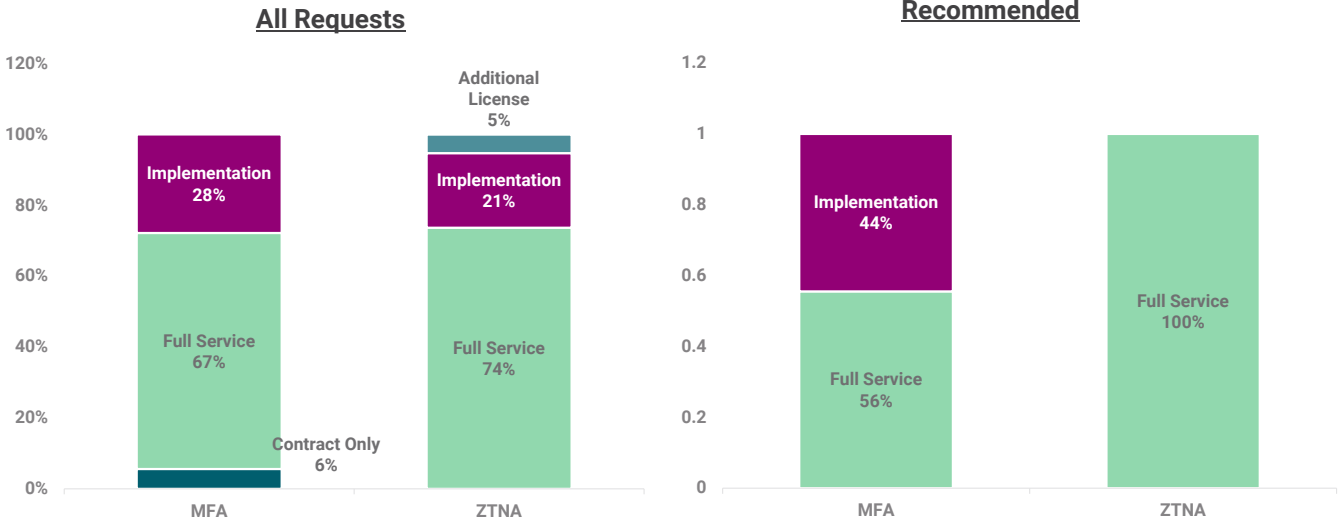
Recommended



*Doesn't exclude those that may be interested in firewall related products that also include DLP services

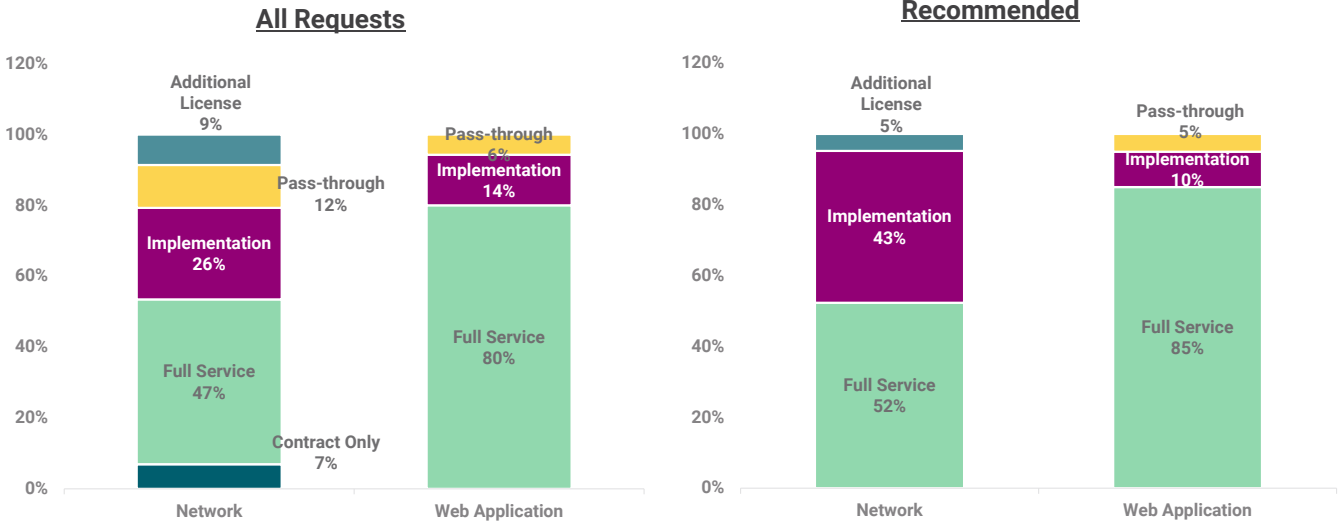
Secure Remote Network Access Projects Funding Prioritization Recommendation

Project Area	Option 1	Option 2	Option 3	Option 4
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%



Firewall Projects Funding Prioritization Recommendation

Project Area	Option 1	Option 2	Option 3	Option 4
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%



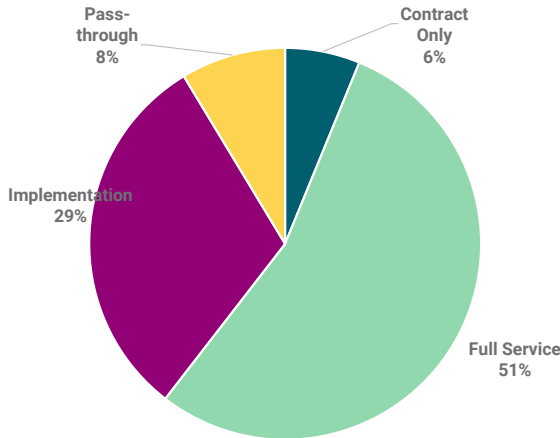
Vulnerability Projects Funding Prioritization Recommendation

FM(0)

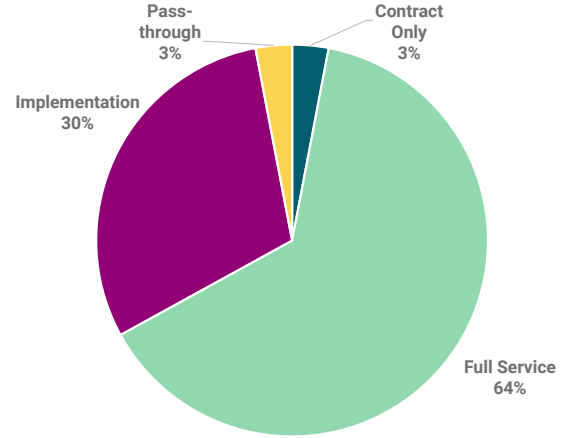
Project Area	Option 1	Option 2	Option 3	Option 4
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%



All Requests



Recommended



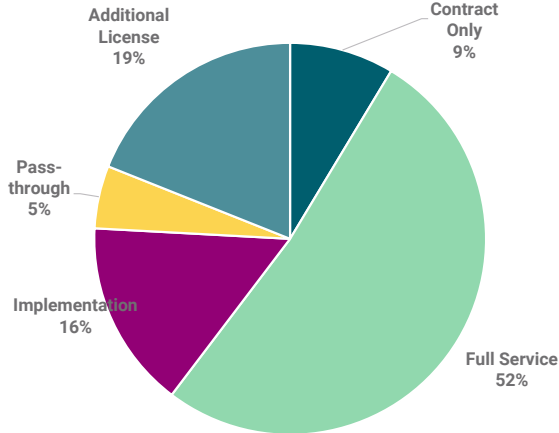
FM(0 Include original vs. recommended
Fain, Mary (VITA), 2025-03-17T19:24:44.944

Endpoint Detection and Response Projects Funding Prioritization Recommendation

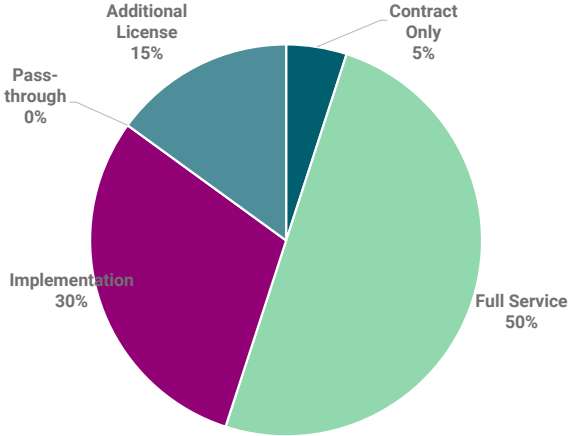
Project Area	Option 1	Option 2	Option 3	Option 4
Asset Inventory	37%	34%	35%	36%
Data Inventory	21%	22%	23%	22%
Secure Remote Network Access	13%	13%	13%	13%
Firewalls	11%	12%	12%	11%
Vulnerability	11%	10%	10%	11%
Endpoint Detection and Response	7%	9%	7%	7%



All Requests

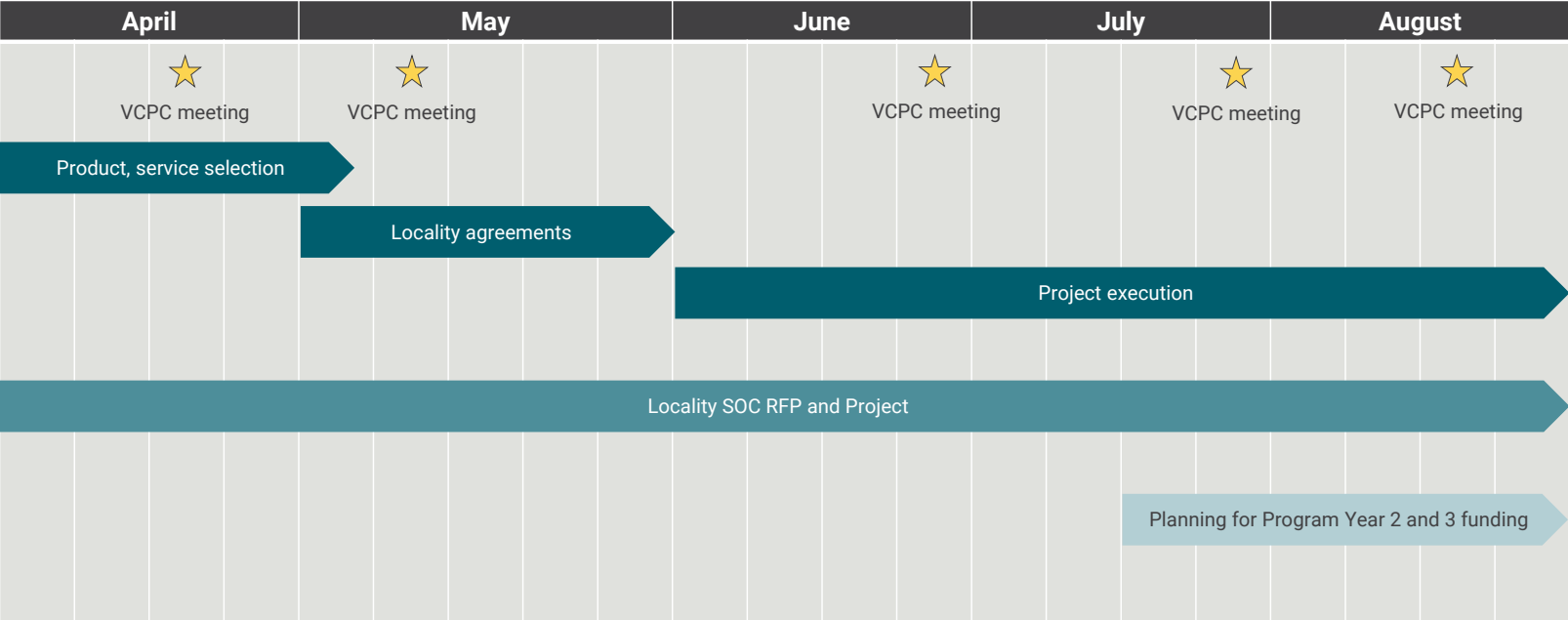


Recommended



Program Timeline

Program Timeline





Virginia Cybersecurity Planning Committee

March 19, 2025 - 10am

VITA, Mary Jackson Boardroom



Motion 1: Overall budget allocation

I move that the VCPC approve the overall budget for Phase 2 as presented, prioritizing \$10.6 million and authorizing up to the full \$15.8 million of funding to Phase 2 Projects.

Motion 2: Percentage allocation to capabilities

I move that the VCPC approve the allocation of funds for Phase 2 Projects across its designated capabilities, with up to 60% allocated across Asset Inventory, Data Inventory, and Secure Remote Access, 40% allocated across Firewalls, Vulnerability and Endpoint Detection and Response, ensuring that total allocations do not exceed the established funding cap for this technology level investment. The project team with the concurrence of the Chair, is authorized to make necessary adjustments within these percentages to optimize resource distribution while maintaining compliance with funding guidelines.