Virginia Cybersecurity Planning Committee
August 21th- 10am
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Approval of Electronic Participation Policy	Staff
Financial Update	Mary Fain
Update on Assessments Project	Mary Fain
Preparing for Project Submissions	Discussion, led by Chair
Public Comment Period	
Other Business	Staff
Adjourn	

Virginia Cybersecurity Planning Committee
May 15, 2024 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,
Richmond, VA, 23225

Committee contact address: cybercommittee@vita.virginia.gov

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:00 am. Mr. Watson welcomed the new members: Ken Pfeil, who is replacing Aliscia Andrews in the seat for the Office of the Governor; Glendon Schmitz, who is replacing Stephanie Williams-Hayes in the seat for public health; and Lisa Walbert, who is replacing Eric Gowins in the seat for public safety; and Brandon Smith, who is filling the vacant seat for elections.

Presiding:

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

Members Present In-Person:

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

Derek M. Kestner, Information Security Officer, Supreme Court of Virginia

Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems

Brandon Smith, Chief Information Officer, Department of Elections

Glendon Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services

Members Participating Remotely:

Michael Dent, Chief Information Security Officer, Fairfax County Department of Information Technology

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black.

Ken Pfeil, Chief Data Officer, Commonwealth of Virginia

Ms. Waller an Mr. Dent participated from home because her principal residence is more than 60 miles from the meeting location. Mr. Pfeil participated remotely for personal reasons.

Members Not Present:

Adrian Compton, Tribal Administrator, Monacan Indian Nation

Robbie Coates, Director, Grant Management and Recovery, VDEM

Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security

Staff Present:

Erica Bland, Info and Technology Manager, Virginia IT Agency

Joshua Heslinga, Director of Legal & Legislative Services, Virginia IT Agency

Patrick Disney, Coordinator Legal & Legislative Services, Virginia IT Agency

Mylam Ly, Legal Compliance & Policy Specialist, Virginia IT Agency

Sam Taylor, PR & Marketing Specialist, Virginia IT Agency

Review of Agenda:

Mr. Disney provided an overview of the agenda and corresponding items in the digital meeting packets.

Approval of Minutes:

The March 26th meeting minutes were displayed. Upon a motion by Mr. Williams and duly seconded by Ms. Carnohan, the committee unanimously voted to adopt the March 26th meeting minutes.

Update on Applications and Assessments

Ms. Fain gave an update on the communications plan results related to the assessments project, including the channels used (VaLGITE and other partners, VDEM listserv, VITA social media posts, and Q&A sessions). The listserv open rate exceeded the 30-40% benchmark. The click rate also performed well, above the 2% benchmark. Social media engagement was between 8-16%, also above the 2-4% benchmark.

Ms. Fain also discussed applicant characteristics. Total qualified applicants reached 172, including 72 local governments, 69 public school districts, 22 authorities, colleges, tribal governments, regional governments, and regional schools. The geographic reach was wide-ranging across the state with 85% of counties having an application submitted. Authorities added even more applications, increasing to 91% of the state, only 12 counties were not represented. Local government and public school districts made up of majority of urban/rural entities.

Update on Pending Procurements

Mr. Watson described that the next step is completing discussion and selection of suppliers for all assessments. Suppliers have not been selected as of the meeting, but there will be enough to cover all applicants. In discussion, Committee members felt it was a good idea to provide guidance for how assessment project vendors aren't automatically allowed to continue business with entities and to provide explicit direction on follow ups to suppliers. The intent is that the Virginia Cybersecurity Planning Committee will be the point of contact for follow-up work related to the grant program. The data from assessments and an approach for further awards is expected to be ready for consideration by early fall. Should be ready to open for more applications (for the technology needs / implementation piece) in early fall, which will avoid a long delay from results. The goal would then be a close date before the end of the year, with further awards proceeding next spring. It is expected that the Committee will next reconvene in the June/July timeframe.

Mr. Watson also provided an update on the intent to use the state portion of the grant money to stand up SOC services, with a contract and such services becoming available in the fall.

Public Comment Period:

There were no public commenters.

Other Business:

Mr. Watson opened the floor for other business. Mr. Watson made sure that the new members had received enough information regarding the cyber security plan and that there would be additional information coming. Mr. Disney reminded members to complete their travel forms and that the next meeting is scheduled for June 23rd.

Adjourn

Upon a motion by Mr. DeKeyser and seconded by Ms. Carnohan, the committee unanimously voted to adjourn the meeting at 10:48 am.

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 IT AGENCY

State and Local Cybersecurity Grant Program

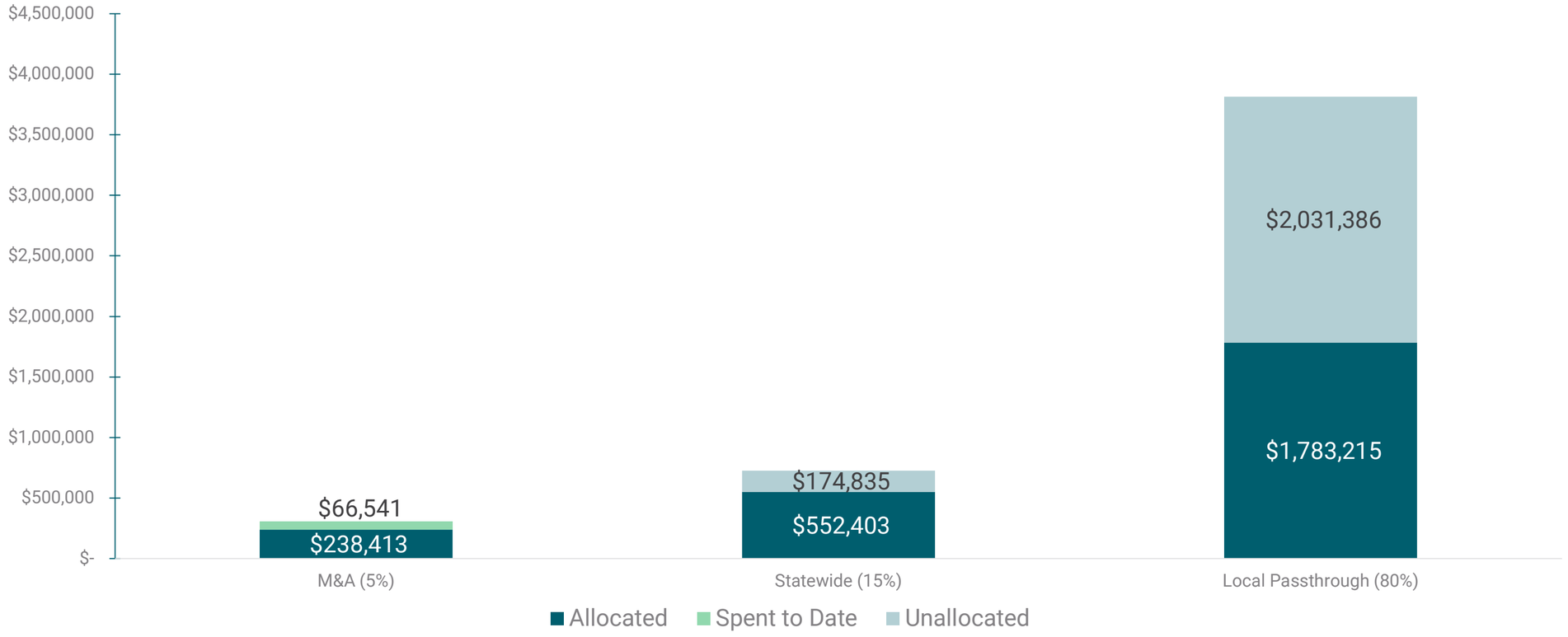
Cybersecurity Plan Capability Assessment Project Update

As of Aug. 16, 2024

Financial Update

Program Year 1 (2022) Financial Update

Period of Performance End: Nov. 30, 2026



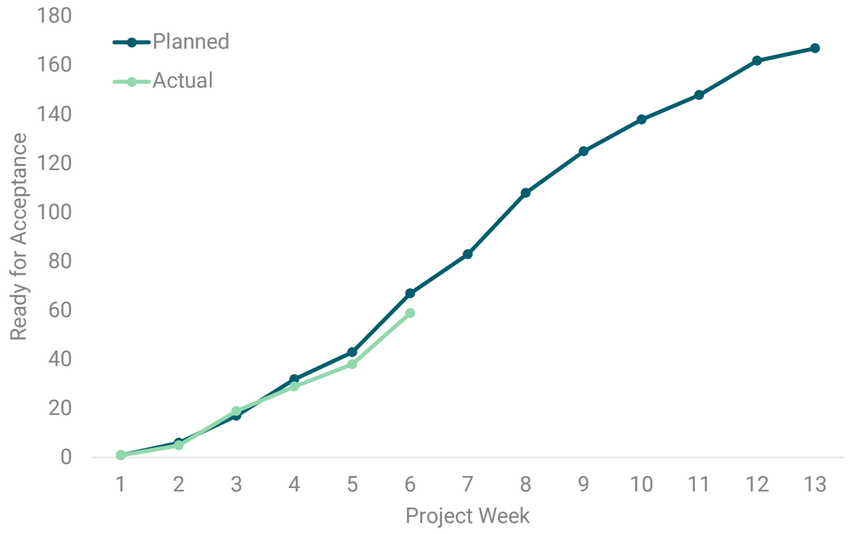
Assessment Project Update

Cybersecurity Plan Capability Assessment Project

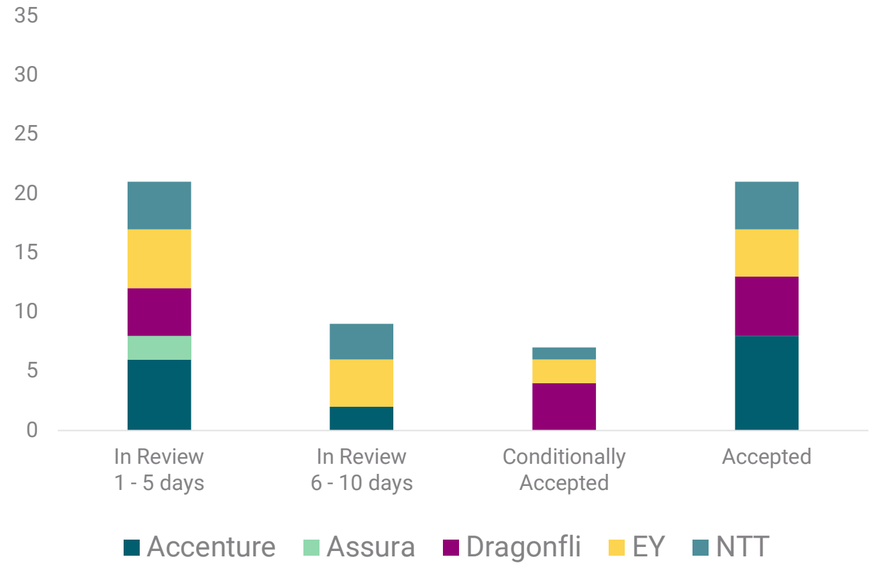
As of Aug. 16, 2024

Current Status	Trending
Green	Green

Assessments ready for deliverable acceptance



Deliverable Acceptance Status

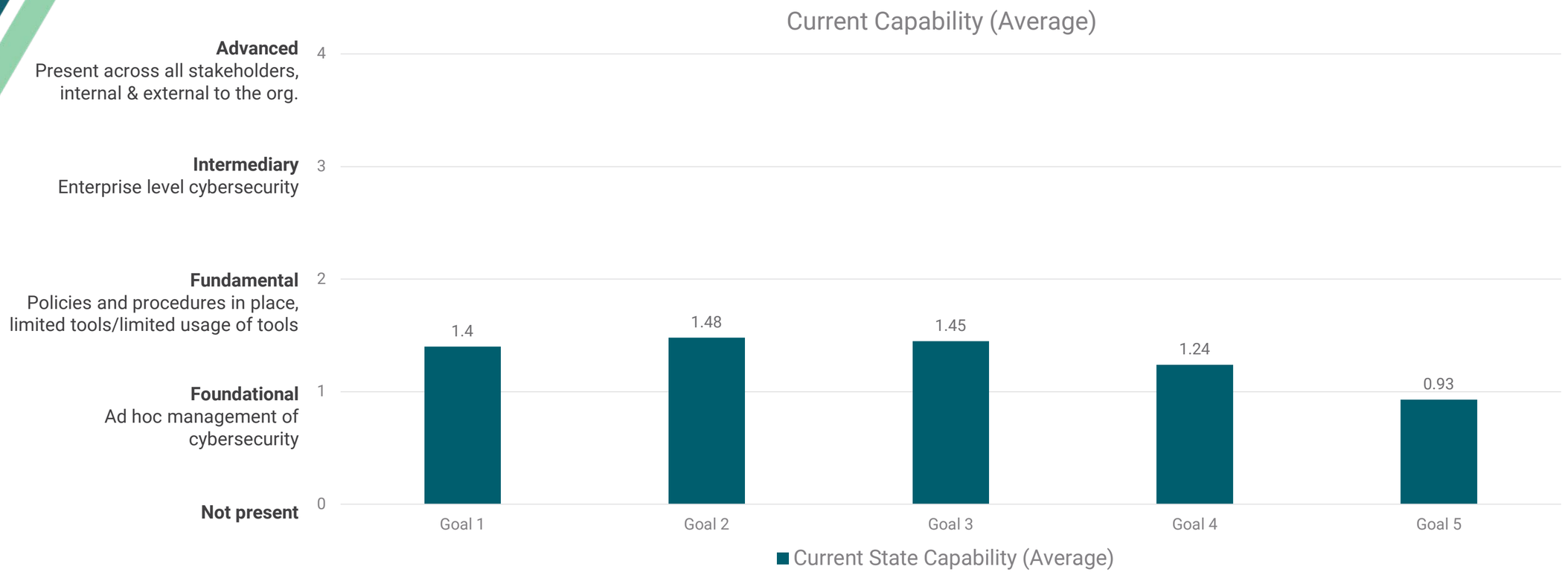


Summary

- 93% of localities are scheduled for assessments, up from 91% in prior week
- As of Aug. 16: Received 54 completed assessments for acceptance
  Vendors continue to remain slightly under target, primary cause continues to be delay from localities in providing final approval
- VITA completed review of 32 assessments

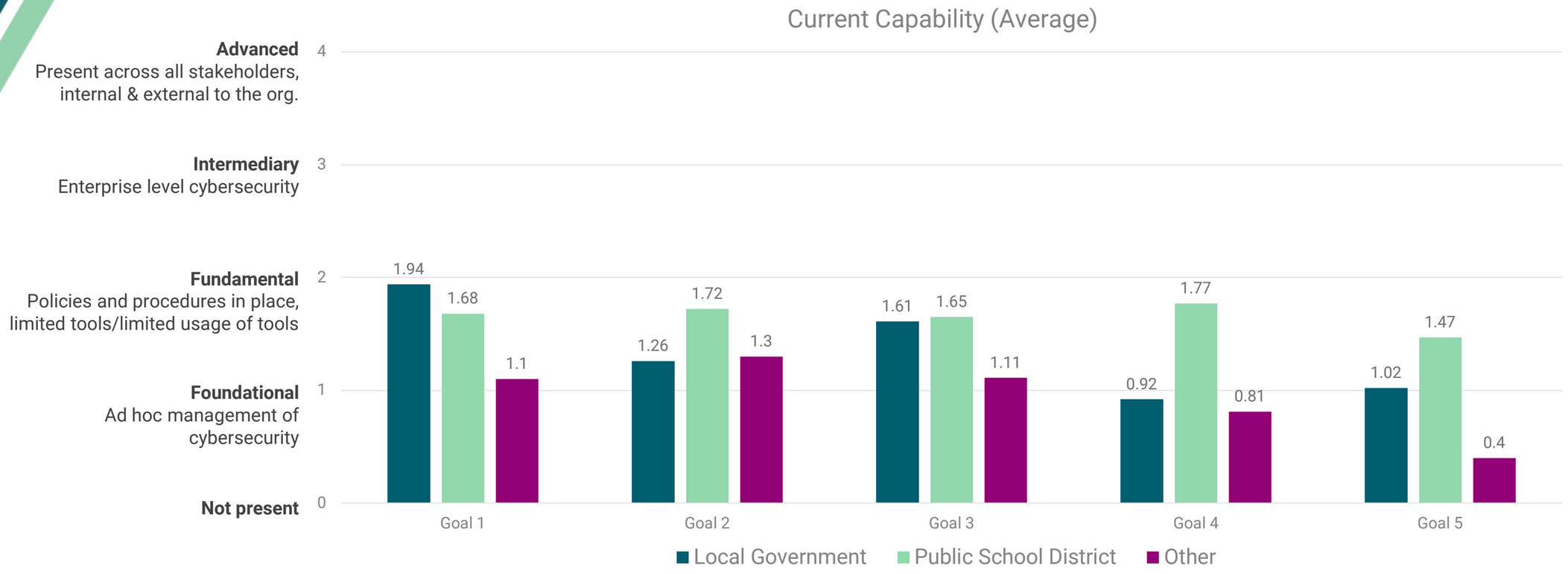
Assessment Findings as of Aug. 16, 2024

Population: 27 accepted assessments



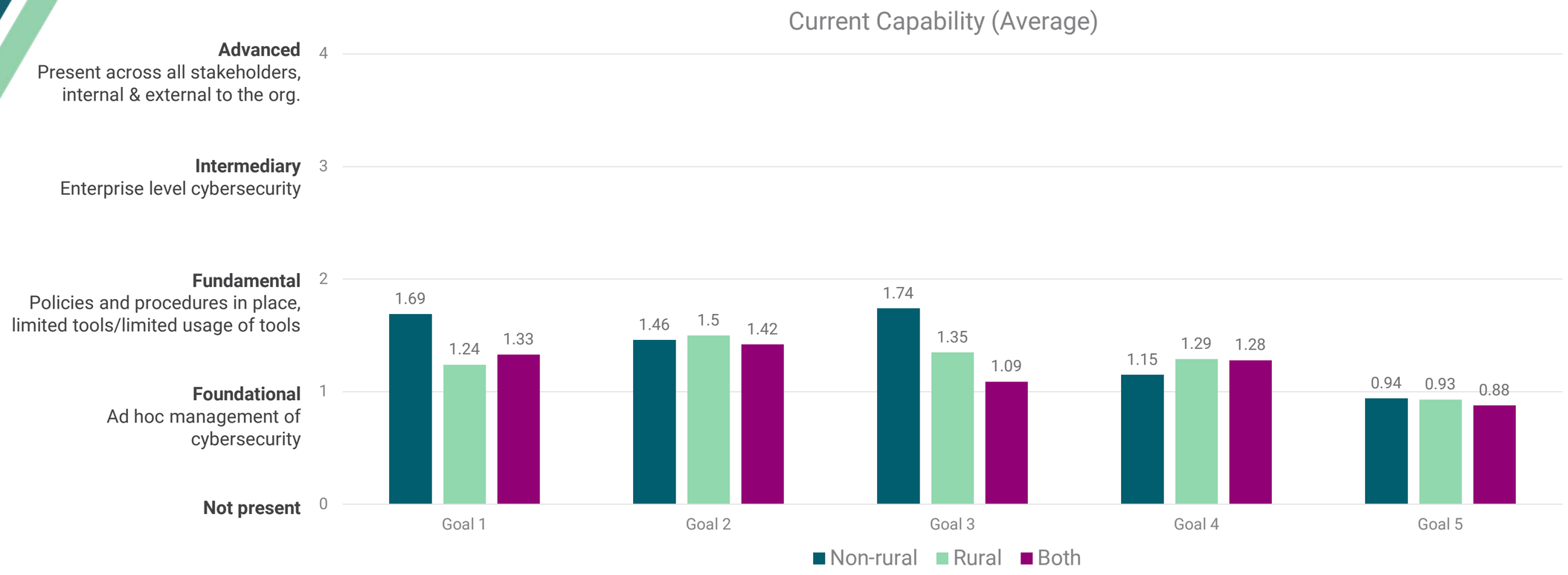
Assessment Findings as of Aug. 16, 2024

Population: 27 accepted assessments



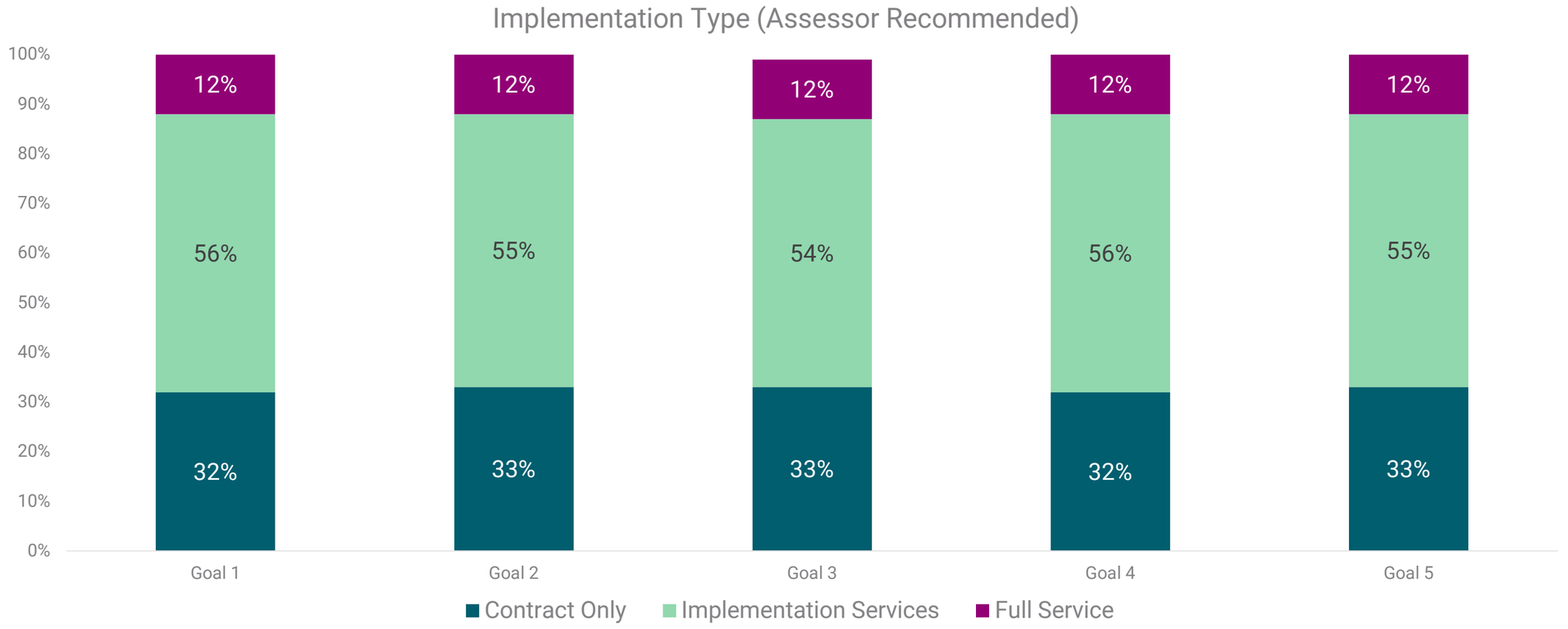
Assessment Findings as of Aug. 16, 2024

Population: 27 accepted assessments



Assessment Findings as of Aug. 16, 2024

Population: 27 accepted assessments



Discussion: Preparing for Project Submissions

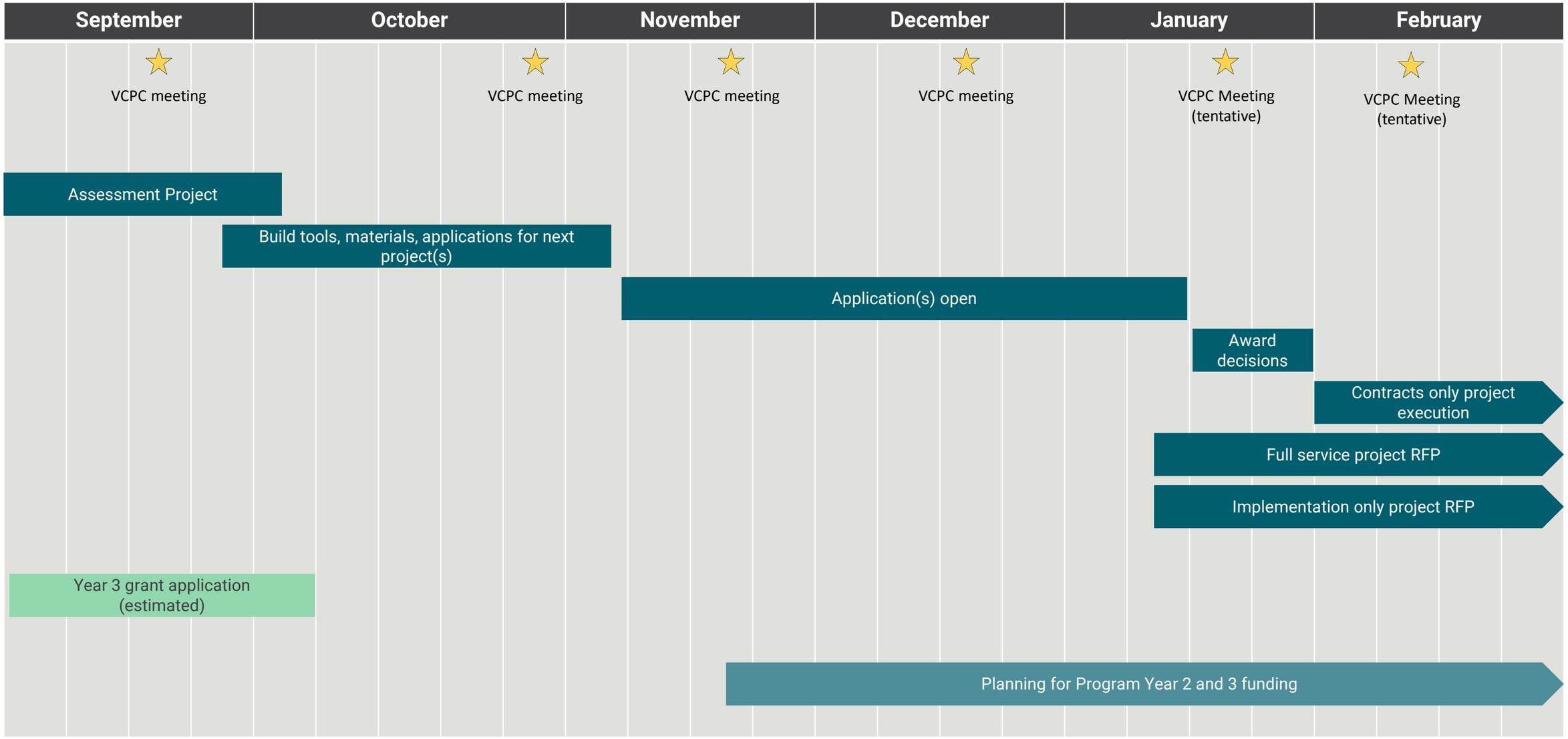
Questions to Answer in Preparation for Project Submissions

- What goals/objectives/sub-objectives will form the basis of our next project(s)?
- How many projects do we move forward with next?
- How much do we anticipate awarding for these projects?
- What criteria should be used for application eligibility?
- What criteria should be used for award decisions?
- Other questions?

What Additional Data, Information Is Needed to Answer Questions

- Assessment findings – what additional data is needed?
- Locality representative input?
- Other information?

Program Timeline


September
October
November
December
January
February
VCPC meeting
VCPC meeting
VCPC meeting
VCPC meeting
VCPC Meeting (tentative)
VCPC Meeting (tentative)
Assessment Project
Build tools, materials, applications for next project(s)
Application(s) open
Award decisions
Contracts only project execution
Full service project RFP
Implementation only project RFP
Year 3 grant application (estimated)
Planning for Program Year 2 and 3 funding

Organization Overview Tab	
Section	**Instructions**
Application Information	Please verify the information provided in the organization's application. Update as needed
Additional Organization Questions	Additional questions to ask the organization prior to starting assessment

All Goal Tabs (1 - 5)	
Column	**Instructions**
Current State Capability Level	Based on your review of the current state of this goal/objective/sub-objective, how would you rate the current state: 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
Current State Technical Analysis	Determine how the current state practice compares to the goal/objective/sub-objective/metric by investigating and documenting answers to questions such as: • What tools are being used today? Or, what tools have been purchased but not yet deployed? • What staff supports this today? • Is there budget associated with this today? • How many licenses are currently purchased? • Is the current state effective in meeting the security objective?
Identified Gaps to Close	Based on the organization, its staff, skills, and capabilities: • What are the gaps that need to be closed between current state and the goal/objective/sub-objective/metrics?
Future State Capability Level	Based on your recommendations of identified gaps to close, what will the organization's rating be after successful 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
Future State Funding Type	Will closing the identified gaps involve new funding for the organization or supplement existing funding? • New Funding • Supplements Existing Funding
Future State Funding Availability	Is funding dedicated to support this in the future? • Exists or will exist • Doesn't exist
Future State Implementation Model – Assessor Recommended	What implementation model do you believe would be best for the organization to use: • Contract only - pre-approved authorized/legal procurement vehicle. The organization is responsible for all aspects of implementation other than establishing the contract. • Implementation Services - Services needed to stand up the technology or processes of the initiative. Once these services are done the organization becomes responsible for running/managing the implementation. • Full Service - The organization needs support to build, implement and run the program objective technology or processes. These services require the least amount of support from the organization.
	What is the organization's preferred model for implementation: • Contract only - pre-approved authorized/legal procurement vehicle. The organization is responsible for all aspects of implementation other than establishing the contract.

Future State Implementation Model – Organization Preference	• Implementation Services - Services needed to stand up the technology or processes of the initiative. Once these services are done the organization becomes responsible for running/managing the implementation. • Full Service - The organization needs support to build, implement and run the program objective technology or processes. These services require the least amount of support from the organization
Future State Implementation and Maintenance Success	In analyzing the organization's ability to implement and maintain based on the implementation model, consider the following questions at a minimum: • What can the organization support for implementation? • Do they have the necessary skills to support the implementation? • Do they have sufficient staff resources available to support an implementation project? • Is there any budget available for implementation? • Does the organization have budget available for ongoing licensing costs? • Budget for other ongoing expenses? • Does the staff have the needed skills to provide ongoing maintenance?
Future State Implementation and Maintenance Success Likeliness	How likely does the organization believe they will be at implementation and maintenance: Low; may not be sufficient resources, skills necessary to implement and/or maintain Medium; at least some resources and/or skills necessary to implement and/or maintain are present High; necessary resources and skills needed for implementation and/or maintenance are available
Assessor Recommended?	Based on the information gathered during the assessment, overall, would you recommend that the organization implement the solution necessary to improve on this goal/objective/sub-objective? No Yes
Organization Interest?	Is the organization interested in moving forward with implementing and maintaining the solution necessary to improve on this goal/objective/sub-objective? No Yes
Other Comments – Assessor	Space for any additional comments by the assessor
Other Comments – Organization	Space for any additional comments by the organization

Application Information	
Organization Name	
Description	
Number of Locations with Technology Assets	
Estimated IT Budget	
Estimated Number of Technology Assets	
Estimated Number of End Users	
Additional Information	

Additional Organization Questions	
What areas/departments are in scope for this assessment?	

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?	Other Comments - Assessor	Other Comments - Organization
1. Inventory and Control of Technology Assets, Software, and Data																	
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 connect 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., healthcare.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 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														

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?	Other Comments - Assessor	Other Comments - Organization
2. Threat Monitoring																	
2.1 Deploy host intrusion detection/prevention and 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 net flow 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 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														
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														

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?	Other Comments - Assessor	Other Comments - Organization
3. Threat Protection and Prevention																	
3.1 Implement and manage firewalls on all end point devices (i.e., user workstations, servers)	N/A	N/A	N/A														
3.2 Implement and manage network firewalls for ingress and egress points	N/A	N/A	N/A														
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																
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														
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																
	3.7.3 Manage or have a third party manage single sign on solutions																
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																
	3.8.3 Maintain or have a third party maintain content/malicious traffic																
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																
	3.9.3 Implement or have a third party implement vulnerability management program and/or software																
	3.9.4 Maintain or have a third party maintain a vulnerability management program																

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?	Other Comments - Assessor	Other Comments - Organization
4. Data Recovery and Continuity																	
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																
	4.2.3 Have a third party maintain a vaulted data recovery solution																
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														

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?	Other Comments - Assessor	Other Comments - Organization
5. Security Assessment																	
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																