Virginia Cybersecurity Planning Committee
March 26, 2024 – 1pm
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of January Minutes & Amend December Minutes	Staff
Assessment Project Applications	Mary Fain
Next Uses of Grant Funding (beyond the assessment project)	Discussion
Grant Year 3 / Fiscal Year 24 Preview/Update	Robbie Coates
Other Business	Staff
Adjourn	

Virginia Cybersecurity Planning Committee
January 17, 2024 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,
Richmond, VA, 23225

DRAFT MINUTES

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10am. Mr. Watson welcomed the members and introduced Mary Fain as a new project manager for Virginia's participation in the SLCGP. Ms. Williams-Hayes, who has moved to VSP and will be leaving the Committee, was thanked for her service.

Presiding:

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

Members Present:

Diane Carnohan, Chief Information Security Officer, Virginia Department of Education

Robbie Coates, Director, Grant Management and Recovery, VDEM

Charles DeKeyser, Major, Virginia Army National Guard.

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

Maj. Eric W. Gowin, Division Commander- Information Technology Division, Virginia State Police.

Charles Huntley, Director of Technology, County of Essex

Stephanie Williams-Hayes, Chief Information Security Officer, Virginia Department of Health

Members Participating Remotely:

Adrian Compton, Tribal Administrator, Monacan Indian Nation

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

Aliscia N. Andrews, Deputy Secretary of Homeland Security, Office of the Governor

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

Mr. Compton, Mr. Williams, Ms. Andrews and Ms. Waller attended virtually because their primary residence was more than 60 miles away.

Members Not Present:

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

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

Staff Present:

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

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

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

Mary Fain, Project Manager, Virginia IT Agency

Sam Taylor, Public Relations & Marketing Specialist, Virginia IT Agency

Review of Agenda:
Ms. Ly provided an overview of the agenda and corresponding items in the digital meeting packets.

Approval of Minutes:
The December meeting minutes were displayed on the screen. Upon a motion by Mr. Gowin and duly seconded by Ms. Carnohan committee unanimously voted to adopt the meeting minutes.

Statement of Requirements/Assessments
Mr. Watson reviewed the statement of requirements and the next steps. Committee members will have the opportunity to preview information, announcements and other correspondence to forward to their networks. There was a discussion on working with localities to obtain assessments and spending limits. Initial application preference will go to rural localities to ensure VCPC is hitting the 25% of the rural gran requirement. VITA will handle applications with VDEM making it easier for localities in terms of applications, federal grant paperwork. Applications for localities will identify and/or describe the organization and main contact for assessment. Additional requirements will include consent from localities for VITA to spend funds on services on their behalf. Following receiving the applications, an estimate of the number of assessments will assist with finalizing the SOR.

There was a motion by Mr. Huntley to release application for localities to apply for the first project (assessments), seconded by Ms. Carnohan. Following the motion was the roll call vote (11-Y 0-N)

YEAS – Andrews, Carnohan, Coates, Compton, Dekeyser, Doherty, Hayes, Huntley, Waller, Watson, Williams-- 11
NAYS – 0
Abstentions – 0

The motion to release application for localities to apply for the first project (assessments) passed.

There was a second motion by Mr. Coates to authorize VITA and VDEM to complete necessary administrative grant work to proceed with the first project (assessments), seconded by Mr. Dekeyser. Following the motion was the roll call vote (11-Y 0-N)

YEAS – Andrews, Carnohan, Coates, Compton, Dekeyser, Doherty, Hayes, Huntley, Waller, Watson, Williams-- 11
NAYS – 0
Abstentions – 0

The motion to authorize VITA and VDEM to complete necessary administrative grant work to proceed with the first project (assessments) passed.

Legislative Update
Mr. Heslinga reviewed legislation from the 2024 Virginia General Assembly relevant to the VCPC. Bills mentioned or discussed were HB1095 & SB222, HB651, HB666, HB706, SB487, and HB242/SB242.

Public Comment Period:
No public comment.

DRAFT

Other Business:
Mr. Watson opened the floor for other business. Mr. Disney discussed travel documents and the next meeting February 21, at 10am.

Adjourn
Upon a motion by Mr. Gowin and duly seconded by Ms. Carnohan, the committee unanimously voted to adjourn the meeting at 11:04 am.

DRAFT

VIRGINIA IT AGENCY

State and Local Cybersecurity Grant Program

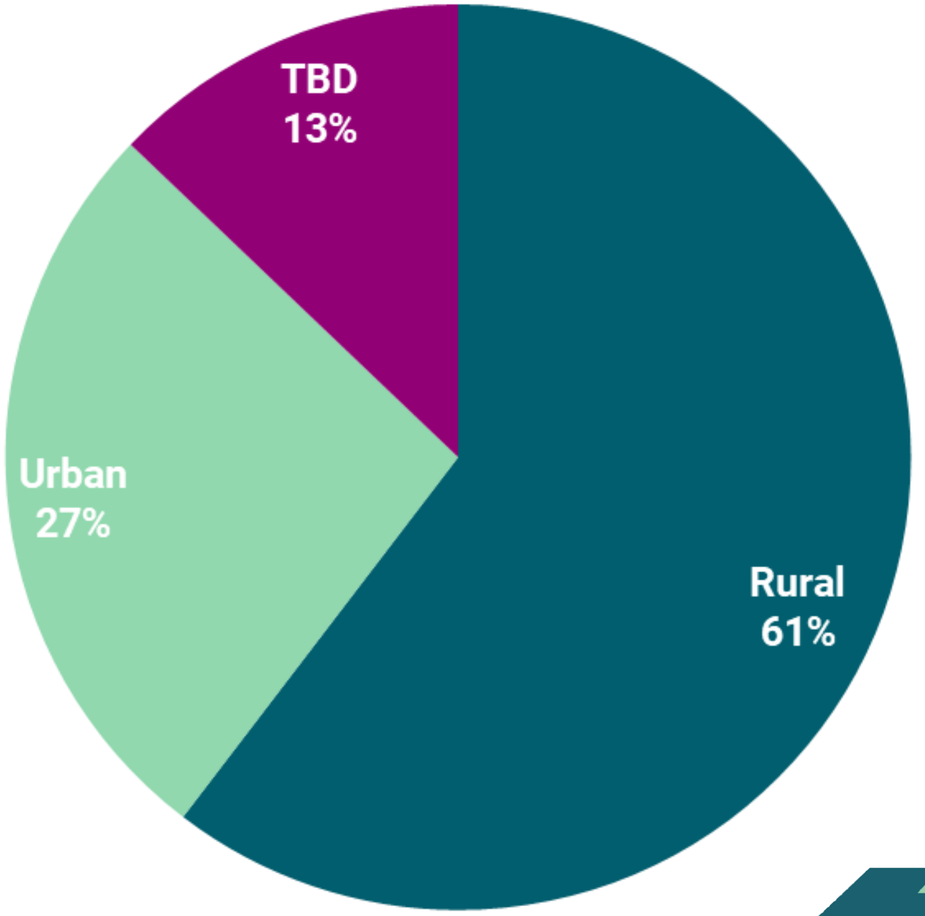
Cybersecurity Plan Capability Assessment Applicant Characteristics

Virginia Cybersecurity Planning Committee
March 26, 2024

Rural Area Pass-Through

As of March 25, 2024

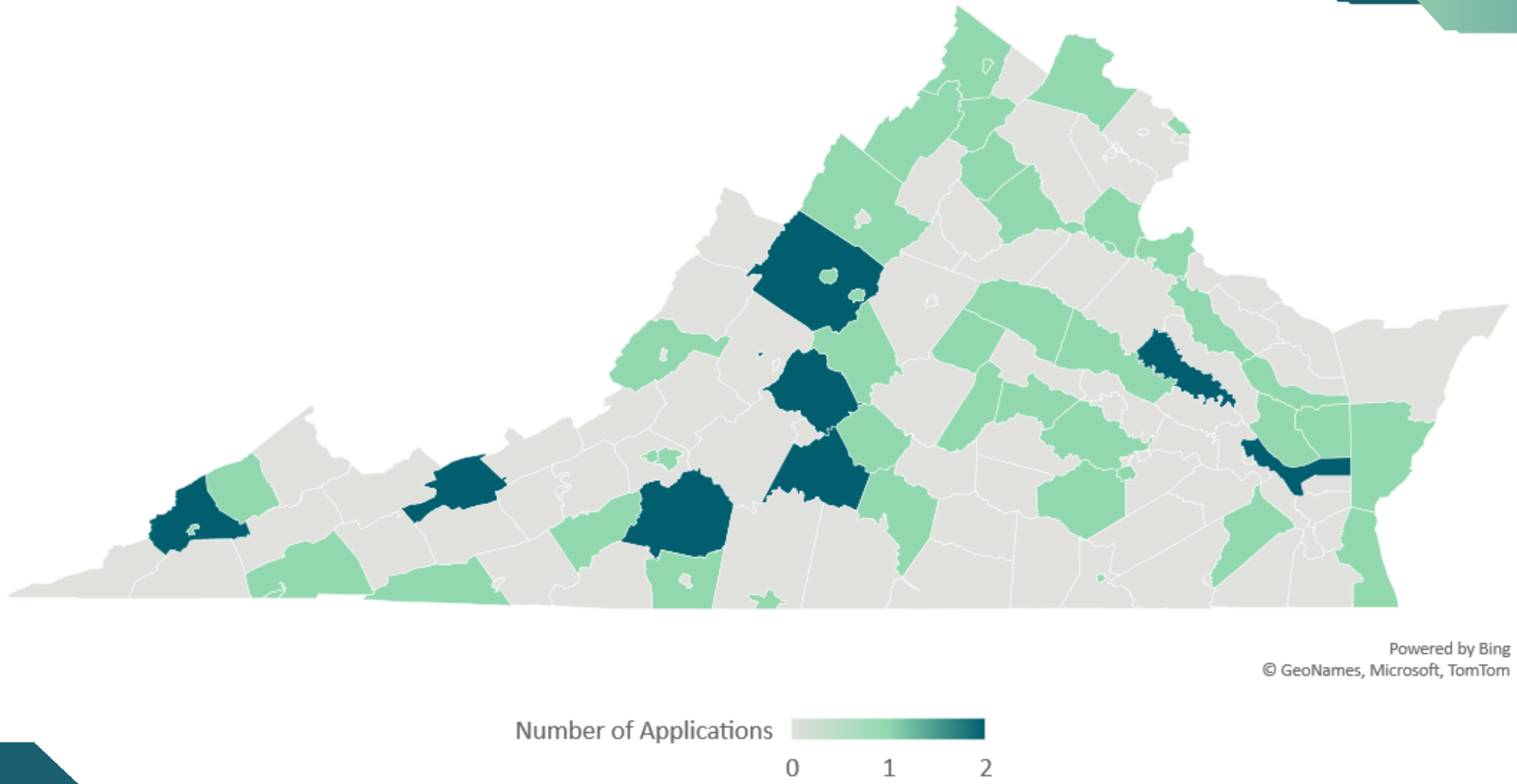
Total Applicants	71
Local Government	25
Public School	25
Local Government/Public School	2
Tribal Government	1
Authority	9



Geographic Reach

Local and Tribal Governments, Public School Applicants

As of March 25, 2024

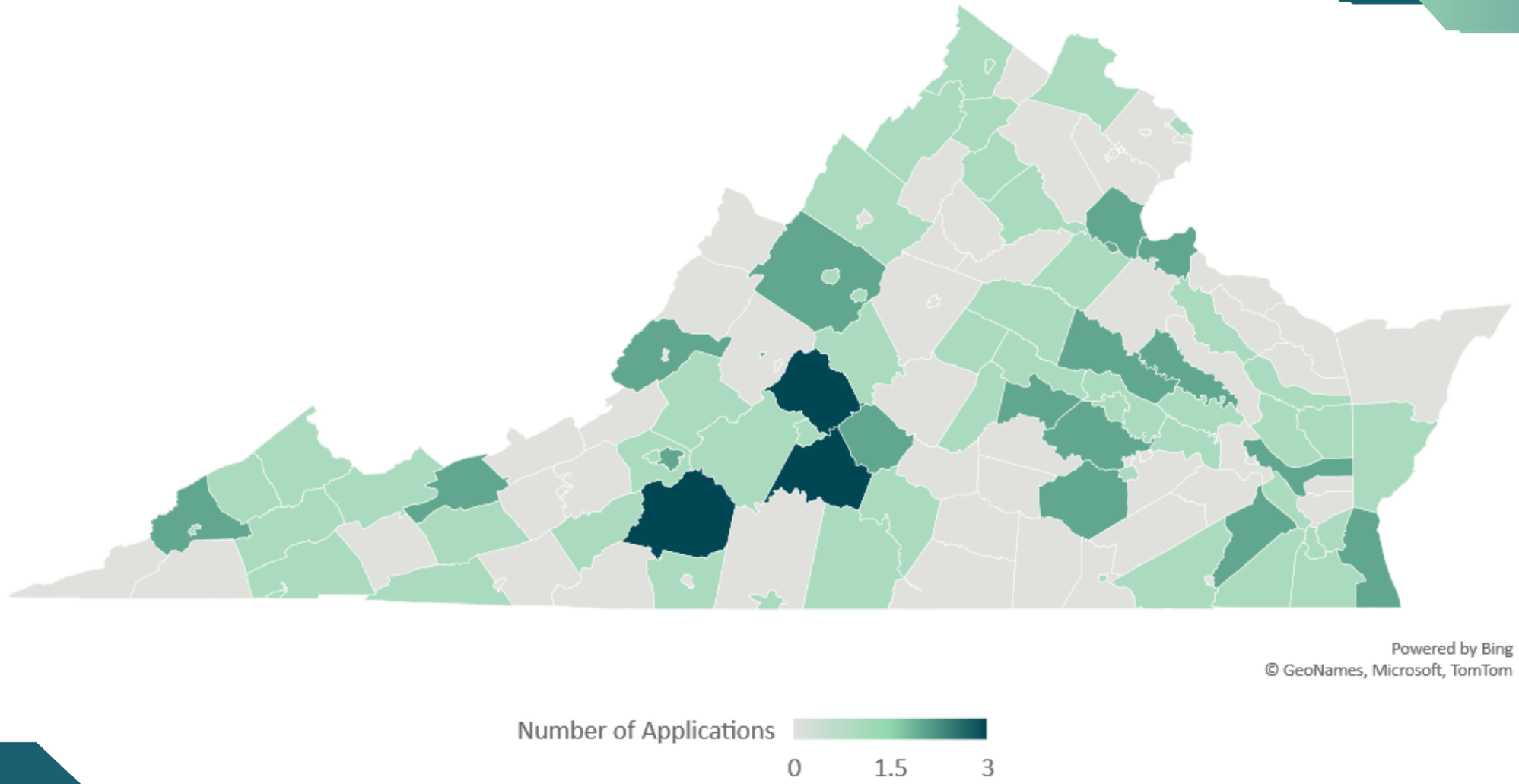


*Does not include cities/counties served by authorities

Geographic Reach

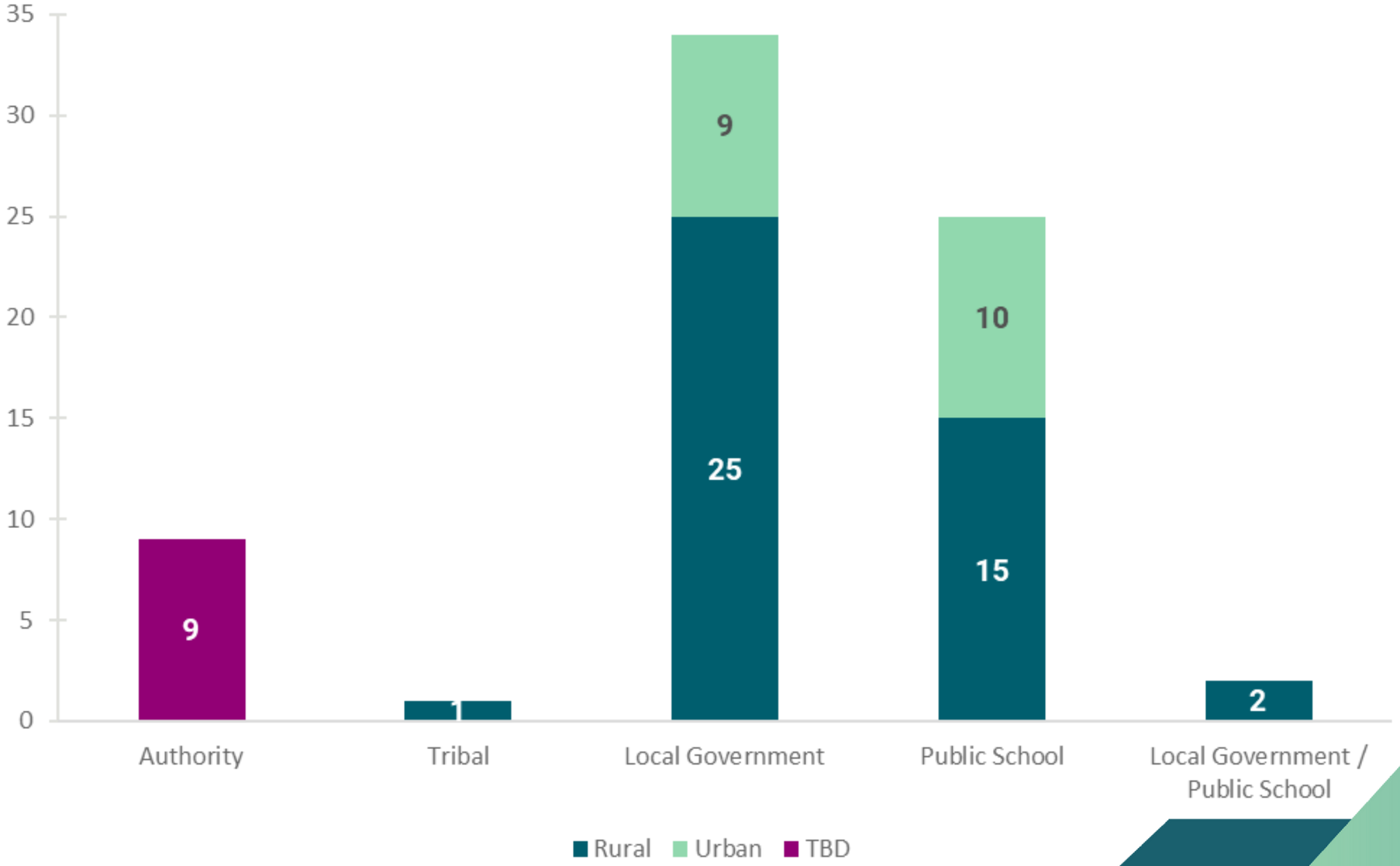
Including Authority Service Areas

As of March 25, 2024



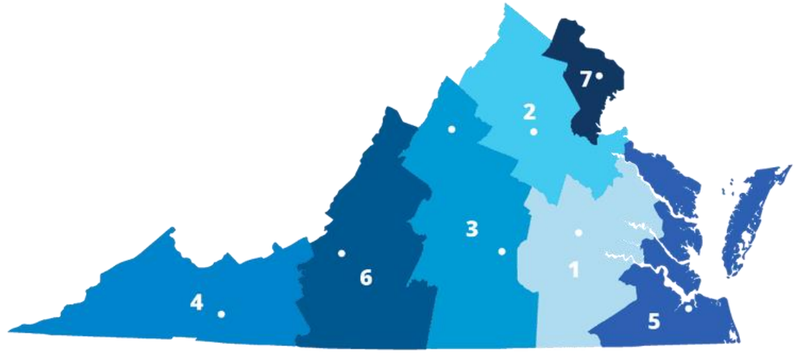
Urban/Rural by Entity Type

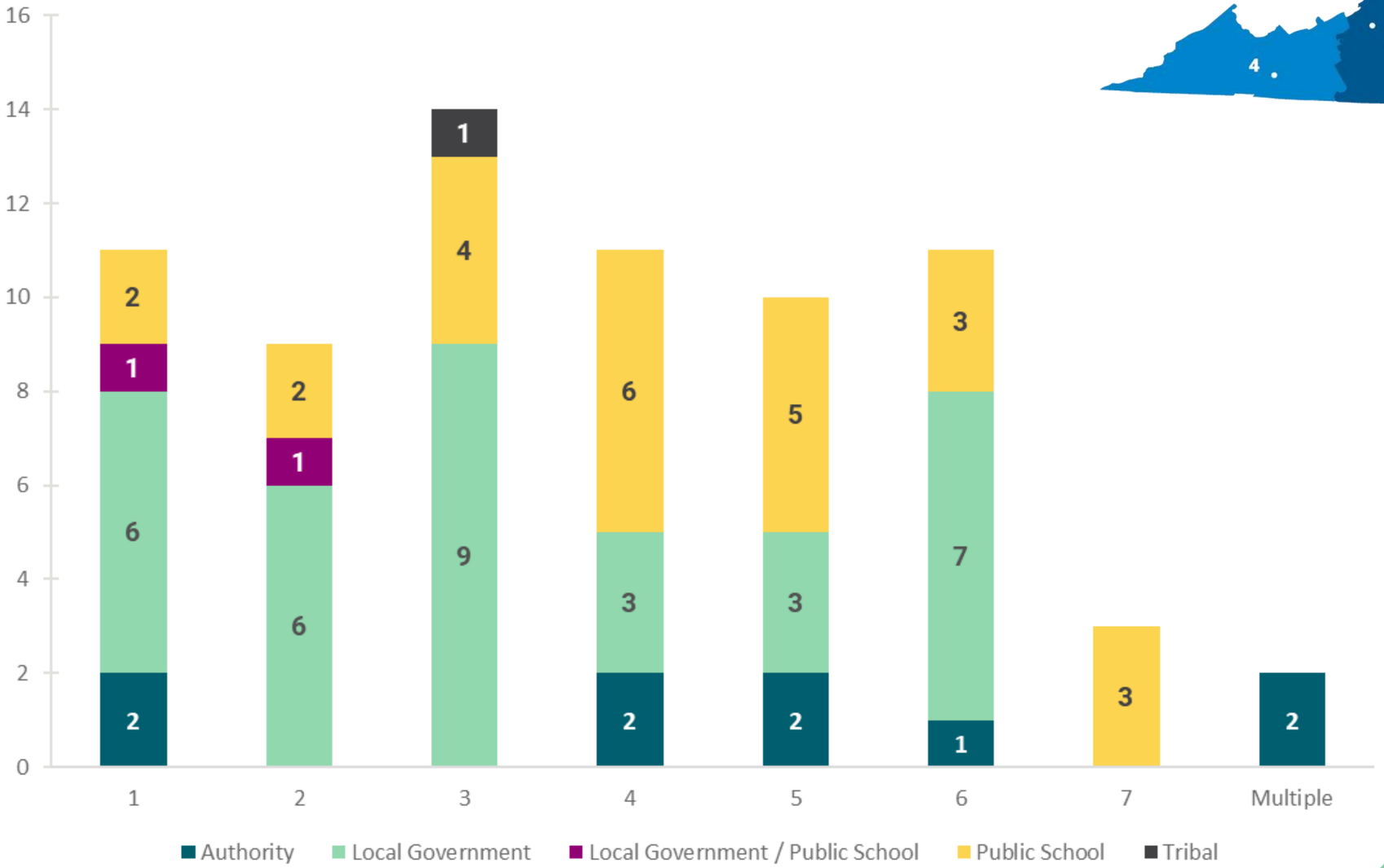
As of March 25, 2024



Entity Type by VDEM Region

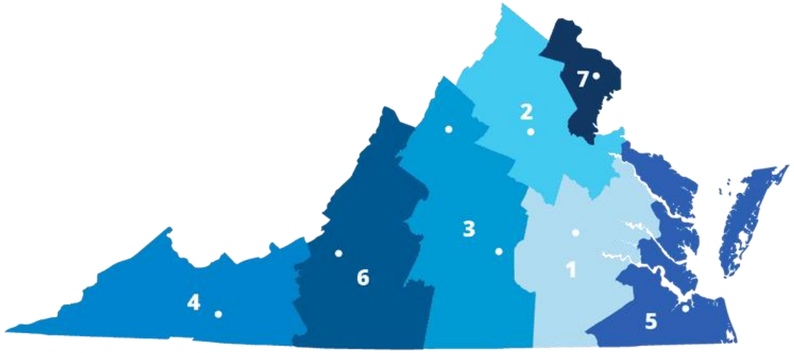
As of March 25, 2024

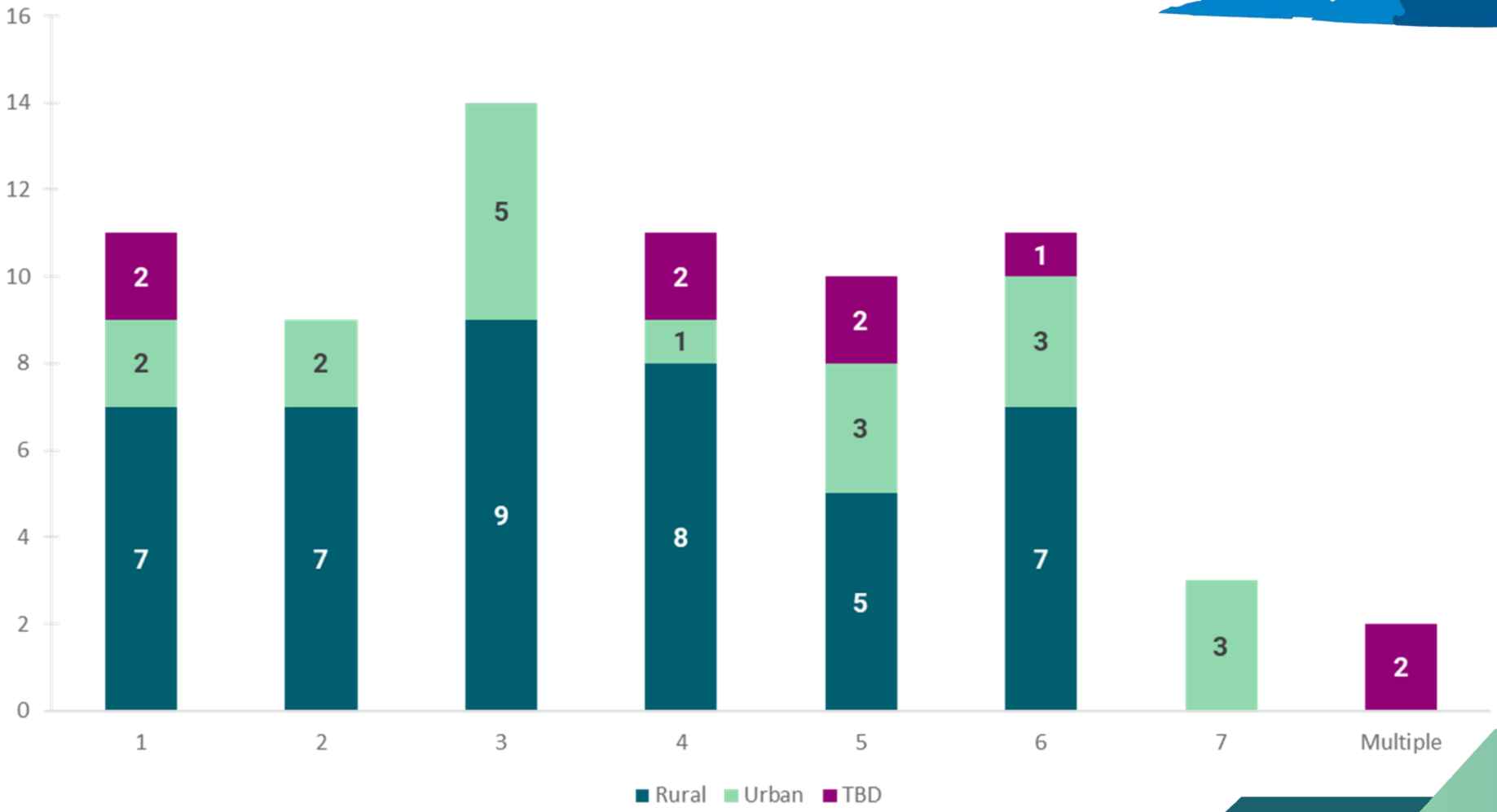




Urban/Rural by VDEM Region

As of March 25, 2024





STATEMENT OF REQUIREMENTS (SOR)

SOR # VITA-240318-01-CAI

VITA State and Local Cybersecurity Grant Program – Cybersecurity Plan Capability Assessment Support

1. **Date:** March 18, 2024

2. **Authorized User**: Virginia Information Technology Agency (VITA)

3. **Authorized User Contact Information:**
Kelley Kapsak, kelley.kapsak@vita.virginia.gov

4. **Solicitation Schedule:**

Event	Date
Release SOR	March 25
Supplier Questions Due to CAI	April 1, 2024
Authorized User Responds to Questions	April 5, 2024
Supplier Response Due	April 19, 2024
Award Decision	May 3, 2024
Estimated Project Start Date	May 13, 2024

PLEASE NOTE: ALL questions related to this SOR should be directed to the CAI Account Manager. Suppliers may NOT contact the Authorized User.

5. **Evaluation and Scoring**

Supplier's Response must be submitted in the specified Statement of Work (SOW) format and will be evaluated for format compliance.

Supplier's Response will be evaluated for technical merit based on its appropriateness to the performance of Authorized User's requirements, its applicability to the environment, and its effective utilization of Supplier and Authorized User resources. The basis and reasonableness of proposed pricing will also be evaluated.

6. **Project/Service:** State & Local Cybersecurity Grant Program Cybersecurity Plan Capability Assessment Support

7. **Specialty Area** (Check one)**:**

- ☐ Application Development
- ☐ Business Continuity Planning
- ☐ Business Intelligence
- ☐ Business Process Reengineering
- ☐ Enterprise Architecture
- ☐ Enterprise Content Management
- ☒ Information Security
- ☐ IT Infrastructure
- ☐ IT Strategic Planning
- ☐ Project Management
- ☐ Public Safety Communications
- ☐ Radio Engineering Services

☐ Back Office Solutions
☐ Geographical Information Systems
☐ IV&V Services

8. Contract Type (Check)**:**

☒ Fixed Price, Deliverable-based

9. Introduction:

Project History
VITA and VDEM are administering Virginia's participation in the State and Local Cybersecurity Grant Program (SLCGP), under which a combination of federal grant money and state-provided matching funds will be used to assist state and local public entities with improving their cybersecurity posture. 80% of the grant fund will be allocated for local public entities and within that 80%, 25% is specifically designated for rural localities (defined by federal law as a population less than 50,000 that has not been designated in the most recent decennial census as an "urbanized area" by the Secretary of Commerce). For further information on the SLCGP generally, see CISA and FEMA's websites:

State and Local Cybersecurity Grant Program | CISA
State and Local Cybersecurity Grant Program | FEMA.gov

For further information on Virginia's participation in the SLCGP, see VITA's website:

Federal Cybersecurity Grants | Virginia IT Agency

The Virginia Cybersecurity Planning Committee has developed a Virginia Cybersecurity Plan, which has been approved by the federal government and is a prerequisite for using SLCGP funding. The Plan contains Virginia's objectives for the program and also identifies a set of priority objectives.

Year one funding is already available to Virginia, and localities will soon be able to seek that funding. With respect to year one funding at least, the intent is to prioritize localities conducting a needs / gap assessment against the program objectives.

The intent of this SOR is to identify and vet suppliers who will be ready to perform a needs / gap assessment of specified locality's environment resulting in an artifact (the Findings and Recommendations Report described below). The produced artifact will be utilized by the Virginia Cybersecurity Planning Committee as a guide and precursor for determining what cyber security services will be implemented in their environment through the SLCGP as further applications for funding are submitted and approved. VITA reserves the right to make multiple awards as a result of this SOR and our expectation is that a total of fifty-three (53) assessments will be completed by one or more suppliers. However this is an estimate, and the actual quantity of assessments awarded may be more or less than those shown.

Authorized User will determine the in-scope localities for assessments before executing any resulting SOW(s).

Business Need
This SOR requires:

- an overall review of a specified locality's current capabilities as compared to the goals and objectives described in the Cybersecurity Plan,
- An assessment of the current state capability level of the organization and,
- Development of recommended security artifacts to support operationalization of the Cybersecurity Plan.

10. Scope of Work:

SOR # VITA-240318-01-CAI
March 18, 2024

This Statement of Requirements (SOR) defines the Cybersecurity Plan Capability Assessment Support required by The Virginia Information Technology Agency (VITA). This SOR requires an overall review of specified locality's current approach for meeting the goals and objectives outlined in the Cybersecurity Plan, as well as development of recommended security artifacts to support operationalization of the Cybersecurity Plan.

The Supplier will review specified locality's current state capability against the following capabilities using a standard list of topics provided by VITA:

- Inventory and control of technology assets, software and data
- Threat monitoring
- Threat protection and prevention
- Data recovery and continuity
- Security assessment

In order to complete the current state assessment, the Supplier will be expected to conduct interviews with the locality's personnel, and request and review a locality's existing documentation and policies that support the Cybersecurity Plan goals and objectives. Supplier is expected to use its security expertise to ask the right questions and follow-ups so as to ensure a useful review. Supplier is *not* being engaged to conduct technical tests of security systems or measures.

After this initial evaluation, the Supplier will generate a Findings and Recommendations Report using a standard template provided by VITA. The draft report is provided as an attachment to this SOR. The report will describe the current state and also recommend actions to improve the locality's capabilities, such as initial development of missing governance artifacts (e.g., Security Management plan, updated policies, updated standards, controls frameworks, capabilities, charters, etc.) as prioritized by senior leadership for this initial phase of this effort. Prioritizations should focus on greatest impact, while keeping in mind feasibility of near-term and program objectives, and may include but are not limited to:

- Manage, monitor, and track information systems, applications, and user accounts;
- Monitor, audit, and track network traffic and activity;
- Enhance the preparation, response, and resiliency of information systems, applications, and user accounts;
- Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk;
- Adopt and use best practices and methodologies to enhance cybersecurity (references NIST);
- Implement multi-factor authentication, implement enhanced logging, data encryption for data at rest and in transit, end use of unsupported/end of life software and hardware that are accessible from the Internet, prohibit use of known/fixed/default passwords and credentials, ensure the ability to reconstitute systems (backups), migration to the .gov internet domain;
- Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain;
- Ensure continuity of operations including by conducting exercises;
- Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity);

- Ensure continuity of communications and data networks in the event of an incident involving communications or data networks;
- Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the specified locality;
- Enhance capabilities to share cyber threat indicators and related information between the eligible locality and the Authorized User;
- Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;
- Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.

Suppliers should provide a **fixed price per assessmen**t in their response. As in-scope localities will be determined prior to SOW execution, Suppliers should also include any assumptions that could impact their price per assessment. The final total price of the SOW(s) will be finalized during Supplier negotiations once the number of in-scope assessments is determined.

11. Period of Performance:

The period of performance for any resulting SOW(s) will be determined based on the number of assessments in scope to the SOW(s) and finalized during supplier negotiations. VITA's initial vision is to have all of the assessments completed within an estimated 12 week timeframe. Suppliers responding to this solicitation should provide estimates for the number of assessments they can complete in a 12 week period and any associated assumptions.

12. Place of Performance (Check one)**:**

☐ Authorized User's Location _____*(City, VA)*

☒ Supplier's Location _____*(City, State)*

☐ Specified Locality and/or Supplier's Location _____*(Explain)*

Suppliers should assume that all the work can be performed remotely when pricing their proposals. However, VITA wants to offer localities the flexibility of requesting onsite visits by the Supplier if needed. In their proposals, responding Suppliers should detail any limitations on travel if requested by a locality. Final determinations about travel and any associated costs will be made during supplier negotiations.

13. Project Staffing:

a. Supplier Personnel

The roles listed in the table below represent the minimum Supplier personnel requirements for this engagement.

Role	Key Personnel (Y/N)	Years of Experience	Certifications	References Required (Y/N)

Security Executive Sponsor and QA	Y	20+ years	N/A	N
Senior Security Lead	Y	15+ years	N/A	N
Junior Security Support	Y	2-5 years	N/A	N

PLEASE NOTE: The use of offshore resources for any SOW is prohibited.

b. Authorized User Staff:

The roles listed in the table below represent Authorized User's staff and the estimated time each will be available to work on the project.

ROLE	DESCRIPTION	% PROJECT AVAILABILITY
VITA Chief Information Security Officer	Project Sponsor work product approval	5%
Various VITA Support Staff	Support discovery, provide expertise on current processes, provide feedback on recommendations and deliverables as appropriate	10%
VITA Project Manager	Primary POC for the project and support project coordination and discovery	85%

14. Milestones and Deliverables:

The minimum required milestones and deliverables and the estimated completion date for each deliverable are listed in the following table.

Milestone Event(s)	Deliverable	Estimated Completion Date
Project Initiation	Project Planning and Kickoff Presentations	May 2024
Acceptance of Final Findings and Recommendations Report	Final Findings and Recommendations Report	TBD
Phase 1 Completion	Completion of Phase 1 Supporting Artifacts per sponsor agreement	TBD

The Supplier should provide all deliverables in hardcopy form and in electronic form, using the following software standards (or lower convertible versions):

Deliverable Type	Format
Spreadsheets	Microsoft Excel

15. Travel Expenses (Check one)**:**

☒ Supplier travel expenses, if required, must be included in the total fixed price of the solution.

Respondents should assume no travel when providing their pricing per assessment. Travel requirements and the associated costs, if any, will be determined during Supplier negotiations.

16. Payment (Check all that apply)**:**

☒ Payment made based on successful completion and acceptance of deliverables

☐ All payments, except final payment, are subject to a *(XX)*% holdback

17. Acceptance Criteria:

The Project Manager will have *(10)* business days from receipt of the deliverable to provide Supplier with the signed acceptance receipt.

Final acceptance of services provided under the SOW will be based upon (Check one):

☐ User Acceptance Test

Acceptance Criteria for this solution will be based on a User Acceptance Test (UAT) designed by Supplier and accepted by Authorized User. The UAT will ensure that all of the functionality required for the solution has been delivered. The Supplier will provide the Authorized User with a detailed test plan and acceptance checklist based on the mutually agreed upon UAT plan. This UAT plan checklist will be incorporated into the SOW.

☒ Final Report

Acceptance criteria for this solution will be based on submission of completed assessments for each interviewed locality.

☐ Other (specify): _____

18. Project Roles and Responsibilities:

Responsibility Matrix	Supplier	Authorized User
Prepare Capability Assessment plan	✓	
Review and Accept Plan		✓
Perform Capability Assessment and Review	✓	

19. Criminal Background Checks and Other Security Requirements (check all that are required):

☒ Standard CAI Required Background Check

☒ Agency Specific Background Check – VITA fingerprinting

20. Performance Bond (Check one)**:**

☐ Required for *(XXX)*% of the SOW value

☒ Not Required

21. Reporting (Check all that are required):

☒ **Weekly Status Update**

The weekly status report, to be submitted by Supplier to Authorized User, should include: accomplishments to date as compared to the project plan; any changes in tasks, resources or schedule with new target dates, if necessary; all open issues or questions regarding the project; action plan for addressing open issues or questions and potential impacts on the project; risk management reporting.

☒ **Other(s)** (Specify): As defined in the Scope of Work and Deliverables sections of this SOR.

22. Federal Funds (Check one):

☒ Project will be funded with federal grant money

☐ No federal funds will be used for this project

23. Training and Documentation:

a. Training:

☐ Required as specified below

☒ Not Required

Training Requirements:
(Specify specific training requirements)

b. Documentation:

☒ Required as specified below

☐ Not Required

Documentation Requirements:
As detailed in Section 10 (Scope of Work) and Section 14 (Milestones and Deliverables) of this SOR

24. Instructions Regarding Freedom of Information Act and Public Availability/Inspection of Records

Authorized User reserves the right to use, copy, and reproduce all submitted documents, data, and other information in any manner Authorized User may deem appropriate in evaluating the fitness of the solution(s) proposed, and in complying with applicable law. All data, materials, and documentation originated and prepared for Authorized User shall be subject to public inspection in accordance with the *Virginia Freedom of Information Act*.

Consistent with the Code of Virginia, Authorized User will, as permitted by law, hold confidential trade secrets or proprietary information that is submitted by a Supplier in connection with the transaction contemplated by this SOR if the Supplier, to Authorized User's satisfaction:

i. **invokes the protections of the Code of Virginia in writing prior to or upon submission of the data or other materials,**
ii. **identifies specifically the data or other materials to be protected, and**

iii. states the reasons why protection is necessary.

FAILURE TO COMPLY WILL RESULT IN THE DATA OR OTHER MATERIALS BEING RELEASED TO SUPPLIERS OR THE PUBLIC AS PROVIDED FOR IN THE VIRGINIA FREEDOM OF INFORMATION ACT.

The Supplier will use this form to identify the information that they deem trade secrets or proprietary information. The designation of an entire proposal or SOR as proprietary or trade secret is not acceptable, and pricing may not be designated as a trade secret or proprietary information.

Supplier Trade Secrets / Proprietary Information Designations Table

SOR/Other Document	Section/Page	Trade Secret / Proprietary Information	Reason

25. Additional Terms and Conditions:

The services to be provided are subject to the following additional provisions:

a. Effective July 1, 2020, the Code of Virginia requires contractors with the Commonwealth who spend significant time working with or in close proximity to state employees to complete sexual harassment training. As a result of the new code, VITA and the Department of Human Resource Management (DHRM) are requiring that all contractors working through the CAI contract complete DHRM's "Preventing Sexual Harassment" training. This training is available as either a short video or a written transcript on the DHRM website: https://www.dhrm.virginia.gov/public-interest/contractor-sexual-harassment-training. The selected Supplier must agree that any assigned resource will complete the training.

b. The selected Supplier must agree that any assigned resource will review and conform to the IT Contingent Labor Program (ITCL) Contractor Code of Conduct. The Code of Conduct can be reviewed on VITA's website at the following link: https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/Contingent-Worker-Code-of-Conduct.pdf

c. FY 2024 DHS Standard Terms and Conditions

26. Scheduled Work Hours:

On an as needed basis, to be coordinated with the Authorized User's Project Sponsor and Project Manager.

27. Facility and equipment to be provided by Authorized User:

The Authorized User may provide furniture and equipment within limited workspace on a temporary basis. Permanent office space, furniture and equipment are the responsibility of the Supplier. If required, while on-site at the project location, the specified locality will provide access to a copier, fax, the agency LAN and the internet (for up to two connections). Specified locality will also provide temporary desk space. The Supplier must provide any cell phones, personal computers or laptops required by the Supplier team. The specified locality's technical staff supporting the specified locality's network must verify that any personal computers or laptops meet minimum-security configuration standards (e.g., current virus protection) before any equipment may be connected to the agency's LAN.

Specified locality will also provide access to all documentation for the referenced projects.

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
	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.

DRAFT

Future State Implementation Model – Assessor Recommended	• 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 Model – Organization Preference	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. • 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

DRAFT

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?	

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis
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 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		
1.3 Upgrade or replace all software no longer receiving security maintenance/support	1.3 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		
1.4 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 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		

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability
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 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				
1.3 Upgrade or replace all software no longer receiving security maintenance/support	1.3 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				
1.4 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 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				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success
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 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			
1.3 Upgrade or replace all software no longer receiving security maintenance/support	1.3 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			
1.4 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 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			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?
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 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			
1.3 Upgrade or replace all software no longer receiving security maintenance/support	1.3 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			
1.4 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 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			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis
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.		

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis
2. Threat Monitoring					
	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.		

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability
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				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability
2. Threat Monitoring							
	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.				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success
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			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success
2. Threat Monitoring						
	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.			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?
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			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?
2. Threat Monitoring						
	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.			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis
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				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability
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						

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success
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					

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?
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					

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis
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		

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Identified Gaps to Close	Future State Capability Level	Future State Funding Type	Future State Maintenance Funding Availability
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				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference	Future State Implementation and Maintenance Success
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			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation and Maintenance Success Likeliness	Assessor Recommended?	Organization Interest?
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			

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Current State Capability Level	Current State Technical Analysis
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				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Identified Gaps to Close	Future State Capability Level	Future State Funding Type
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					

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Maintenance Funding Availability	Future State Implementation Model - Assessor Recommended	Future State Implementation Model - Organization Preference
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					

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Future State Implementation and Maintenance Success	Future State Implementation and Maintenance Success Likeliness
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				

DRAFT

Program Goal and Objectives	Program Sub-Objectives	Associated Metric	Metric Description (details, source, frequency)	Assessor Recommended?	Organization Interest?
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				

DRAFT