Virginia Cybersecurity Planning Committee
June 30, 2023 – 1pm
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Communications Plan	Jason Elmore, VDEM
Virginia Cybersecurity Plan Discussion	Mike Watson
Public Comment Period	
Other Business	Staff
Adjourn	

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
April 12, 2023 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom, Richmond, VA, 23225

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:03am. Mr. Watson welcomed the members.

Presiding:

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

Members Present:

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

Robbie Coates, Director, Grant Management and Recovery, VDEM

Adrian Compton, Tribal Administrator, Monacan Indian Nation

Charles DeKeyser, Major, Virginia Army National Guard

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

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

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

John Harrison, IT Director, Franklin County

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

Benjamin Shumaker, Cyber Security Specialist, King William County Government.

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

Members Participating Remotely:

Aliscia N. Andrews, Deputy Secretary of Homeland Security, Office of the Governor. Ms. Andrews participated from Aldie because her principal residence is more than 60 miles from the meeting location.

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black. Ms. Waller participated from Roanoke because her principal residence is more than 60 miles from the meeting location.

Wesley Williams, Executive Director of Technology, Roanoke City Public Schools. Mr. Williams participated from Roanoke because his principal residence is more than 60 miles from the meeting location.

Members Not Present:

Staff Present:

Amma Appiah Abbey, Legal Compliance & Policy Specialist, Virginia IT Agency

Jason Brown, Chief Administrative Officer, Virginia IT Agency

Stephanie Benson, External Communication & Outreach Manager, Virginia IT Agency

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

Joshua Reynolds, Assistant Attorney General, Office of the Attorney General

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

Trey Stevens, Deputy Chief Information Security Officer, 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 March meeting minutes were displayed on the screen. Upon a motion by Mr. Shumaker and duly seconded by Mr. Kestner, the committee unanimously voted to adopt the March meeting minutes.

Consolidated Draft Cybersecurity Plan

Mr. Watson went over the components of the cybersecurity plan and reviewed the sub-objectives and metrics. There was discussion on the addition of Virtual Private Network (VPN) and data encryption (3.3.2) to the plan. The group viewed the entire plan template including a letter from the VCPC, plan elements, and subcategories. There was a discussion on leveraging CISA services and solutions, including use of .gov and making that a requirement for email addresses, and assessments. There was a request from Mr. Compton to add a clause to the plan defining tribes as federally and state recognized tribes for the application. This addition would ensure that the plan is inclusive of all recognized tribes. The group also discussed staff augmentation and the incorporation of measurements or dashboards with indicators. They talked about how the Virginia budget will cover the grant's matching component and the staggered four-year grant. Lastly, they discussed maturity models, comparison metrics for similar localities, and developing and maintaining a list of local governing bodies.

Current Contract Options

Mr. Gregory Scearce from Supply Chain Management covered several topics related to IT services and staffing. He discussed the use of commercial off-the-shelf software (COTS) and SaaS solutions vetted through VITA Enterprise Cloud Oversight Services (ECOS), as well as the IT contingent labor contract for staff augmentation and statements of work. The full range of IT services was also discussed, and it was noted that scope statements for suppliers need to be reviewed. Information about public contracts portals and contact information was provided, and the importance of leveraging state contracts was emphasized. Additionally, it was noted that there may be additional requirements in contracts from federal regulations. There was also discussion from the group on what contract vehicles should be encouraged. Lastly, Ms. Scearce provided contact information for VITA Supply Chain Management: scminfo@vita.virginia.gov.

Grant Prerequisites

Grant prerequisites were discussed as part of consolidated draft cybersecurity plan.

Public Comment Period:

There were no public comments.

Other Business:

Mr. Watson opened the floor for other business. Ms. Ly discussed travel forms.

Adjourn

Upon a motion by Mr. Harrison and duly seconded by Ms. Carnohan, the committee unanimously voted to adjourn the meeting 11:53am.

Virginia Cybersecurity Planning Committee Minutes
May 17, 2023 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,
Richmond, VA, 23225

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10am. Mr. Dent welcomed the members.

Presiding:

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

Members Present:

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

Adrian Compton, Tribal Administrator, Monacan Indian Nation

Charles DeKeyser, Major, Virginia Army National Guard

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

John Harrison, IT Director, Franklin County

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

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

Members Participating Remotely:

Aliscia N. Andrews, Deputy Secretary of Homeland Security, Office of the Governor. Deputy Secretary Andrews participated virtually because her principal residence is more than 60 miles from the meeting location.

Members Not Present:

Robbie Coates, Director, Grant Management and Recovery, VDEM

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

Benjamin Shumaker, Cyber Security Specialist, King William County Government.

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

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

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

Staff Present:

Amma Appiah Abbey, Legal Compliance & Policy Specialist, Virginia IT Agency

Stephanie Benson, External Communication & Outreach Manager, Virginia IT Agency

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

Amy Judd, Records Management and Compliance Specialist, Virginia IT Agency

Joshua Reynolds, Assistant Attorney General, Office of the Attorney General

Catherine Lee, VDEM

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

Trey Stevens, Deputy Chief Information Security Officer, Virginia IT Agency

Review of Agenda:

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

Cybersecurity Plan Discussion

The following points were discussed in relation to the cybersecurity plan:

- A 45-day window exists for the state to issue funds once the funding is received.
- 25% of the funds are allocated to rural jurisdictions with a population of fewer than 50,000.
- Whether funds can be used for services such as SOC services and penetration testing.
- Prerequisites or requirements that need to be met when requesting funding.
- Deputy Secretary Andrews discussed efforts being made to address challenges arising from grant language.
- The idea of offering free or minimum services to eliminate the need to pay for prerequisites such as NCSR to promote free services.
- The importance of documenting the services provided.
- Questions were raised regarding the allocation of funding, making the application process as easy as possible, and determining the direction of the plan.
- Two models were discussed: localities or entities submitting for grants and receiving funding for projects, or providing services directly to localities.
- Ms. Carnohan discuss concerns/questions having been expressed by school divisions regarding the timeline and application process.
- Assistance with the application process for smaller jurisdictions.
- Ms. Lee discussed vetting subgrant and subgrant administration as well as approaching deadlines for performance of the grant.
- Questions for the next meeting were requested to be submitted to the Committee's email mailbox, cybercommittee@vita.virginia.gov.
- The timeline for vetting subgrants with pass-through was discussed. Assuming Plan submission approximately late September and a 45-day time period, aiming for early November for vetting, mid-October for allocation and November for allocation Notification. If VDEM is to open the portal, the portal opening process takes 3 -4 months.
- A project breakdown with milestones and dates, as well as a communications plan will be established.

Break

Public Comment Period

There were no public comments.

Future Business

There was a discussion on grant funding breakdown and what happens to unmet allocations.

Other Business

Mr. Dent opened the floor for other business. There was a discussion on how applications would be scored. Ms. Lee briefly described VDEM's past engagement with ODU for other grant programs on establishing methodology and subject matter expert panels. It was reiterated that it was the committee's responsibility to set priorities. Ms. Ly covered travel forms and next meeting date.

Adjourn

Upon a motion by Maj. DeKeyser and duly seconded by and Harrison, the committee unanimously voted to adjourn the meeting 12:08pm.

State and Local Cybersecurity Grant Program (SLCGP) Communications Plan
DRAFT

Background

Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act, which established the State and Local Cybersecurity Grant Program, appropriating $1 billion to be awarded over four years. These entities face unique challenges in defending against cyber threats such as ransomware, as they lack the resources to defend against constantly changing threats. The Department of Homeland Security (DHS), through the Cybersecurity and Infrastructure Security Agency (CISA), is taking steps to help stakeholders across the country understand the severity of their unique local cyber threats and cultivate partnerships to reduce related risks across the SLT enterprise.

This phased communications plan will allow the Commonwealth of Virginia to notify as many eligible entities as possible of the SLCGP and its application process.

Phase I – Establish Inclusive Listserv of Eligible Entities

During this phase, a communication will be sent commonwealth-wide to state agencies and local governments via already existing contact lists with the Virginia Municipal League and the Virginia Association of Counties. The communication will outline the funding opportunity, timing of the application process, but most importantly will direct the entities to sign up to receive further updates concerning the SLCGP process through the Virginia Department of Emergency Management (VDEM) website.

Phase II – Updates and Notifications through established listserv

As updates and additional information about the application process and registration are available, we will utilize the listserv created via Phase I of this plan. This will be an ongoing phase until the application deadline is complete.

Phase III – Notification of Grant Recipients

VDEM and VITA communication teams will work with the committee to draft award notifications, as needed.

Phase IV – Notification to Media

Once the award notifications have been delivered to the recipients, a news release will be sent out notifying the public of the grant awards provided by the SLCGP.

VIRGINIA CYBERSECURITY PLAN

NOTE: This template is provided as an optional tool for eligible entities to use (as needed) to develop their cybersecurity plan. This template includes key requirements of the State and Local Cybersecurity Grant Program. Ultimately, eligible entities are encouraged to develop a plan that reflects their unique situation while meeting program requirements. This includes using existing plans and documents as appropriate.

Replace all grey text, as appropriate, to reflect the eligible entity.

Text highlighted in yellow provides instruction for plan authors and should be deleted before the final draft of the document is complete. *Delete text box before final draft.*

MONTH YEAR

Approved by The Commonwealth of Virginia Cyber Planning Committee on XX/XX/XXXX
Version 1.0

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM VIRGINIA CYBERSECURITY PLANNING COMMITTEE

[Including a letter from the eligible entity's Cybersecurity Planning committee chair and the CIO/CISO/CSO or equivalent demonstrates that the plan has been approved by the appropriate officials]

Greetings,

The Cybersecurity Planning committee for the Commonwealth of Virginia is pleased to present the 2023 Commonwealth of Virginia Cybersecurity Plan. The Cybersecurity Plan represents a continued commitment to improving cybersecurity and supporting a whole of state approach to cybersecurity. This update also meets the requirement of the current U.S. Department of Homeland Security guidelines for the State and Local Cybersecurity Grant Program (SLCGP).

Representatives from the [Entity governing body/represented bodies with the Cybersecurity Planning Committee] collaborated to develop and update the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on inventory and control of technology assets, software and data, threat monitoring, threat protection and prevention, data recovery and continuity and understanding an organization's cybersecurity maturity level. They are designed to support the Commonwealth in planning for effective security technologies and navigating the ever-changing cybersecurity landscape.

As we continue to enhance cybersecurity, we remain dedicated to improving our resilience among disciplines and across jurisdictional boundaries. With help from our partners and cybersecurity practitioners, we will work to achieve the goals set forth in the Cybersecurity Plan and become a model for cyber resilience.

Sincerely,

_____

INSERT APPROPRIATE SIGNATURE BLOCKS
[NAME]
[TITLE]
[ENTITY]

INTRODUCTION

The Cybersecurity Plan is a three-year strategic planning document that contains the following components:

- **Vision and Mission**: Articulates the vision and mission for improving cybersecurity programs over the next three years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and governance mechanisms for cybersecurity within the Commonwealth of Virginia as well as successes, challenges, and priorities for improvement. This also includes a strategy for the cybersecurity program and the organization structure that identifies how the cybersecurity program is supported. In addition, this section includes governance that identifies authorities and requirements of the Commonwealth of Virginia's cybersecurity grant program.
- **How feedback and input from local governments and associations was incorporated.** Describes how inputs from local governments as used in order to reduce overall cybersecurity risk across the eligible entity. This is especially important in order to develop a holistic cybersecurity plan.
- **Cybersecurity Plan Elements:** Outlines technology and operations needed to maintain and enhance resilience across the cybersecurity landscape.
- **Funding:** Describes funding sources and allocations to build cybersecurity capabilities within the Commonwealth of Virginia along with methods and strategies for funding sustainment and enhancement to meet long-term goals.
- **Implementation Plan:** Describes the Commonwealth of Virginia's plan to implement, maintain, and update the Cybersecurity Plan to enable continued evolution of and progress toward the identified goals. The implementation plan must include the resources and timeline where practicable.
- **Metrics:** Describes how the Commonwealth of Virginia will measure the outputs and outcomes of the program across the entity.

Vision and Mission

This section describes the Commonwealth of Virginia Cyber Planning Committee vision and mission for improving cybersecurity:

Vision:

Create a cybersecurity ecosystem supporting a whole of state approach for state and local governments to safeguard critical infrastructure, protect Virginians' data, and ensure the continuity of essential services.

Mission:

To further establish and enhance the cybersecurity capabilities of state and local government and tribal entities in Virginia by providing a framework of technology and services to effectively identify, mitigate, protect, detect, and respond to cyber threats. Through leveraging of shared capabilities, strategic planning and common technology the Commonwealth of Virginia strives to efficiently and effectively protect the confidentiality, integrity, and availability of critical systems, data, and services that benefit Virginians.

Cybersecurity Program Goals and Objectives

Commonwealth of Virginia Cyber Planning Committe Cybersecurity goals and objectives include the following:

Cybersecurity Program	
Program Goal	**Program Objectives**
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)
	1.2 Ensure only authorized assets connect to enterprise systems and are inventoried
	1.3 Upgrade or replace all software no longer receiving security maintenance/support
	1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business
	1.5 Identify all government websites and migrate non .gov sites to .gov domains
	1.6 Establish and maintain inventory of administrator, service and user accounts
2. Threat Monitoring	2.1 Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers
	2.2 Deploy network monitoring, filtering and detection at network egress and ingress points
	2.3 Centralize security event alerting
	2.4 Collect network traffic flow logs
	2.5 Audit log collection for all servers and systems hosting data in accordance with ~~federal~~ ~~enterprise~~ log management standards
	2.6 Web application firewall

Program Goal	Program Objectives
3. Threat Protection and Prevention	3.1 Implement and manage firewalls on all end point devices (i.e. user workstations, servers)
	3.2 Implement and manage network firewalls for ingress and egress points
	3.3 Encrypt sensitive data in transit and on devices hosting sensitive data
	3.4 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access
	3.5 Domain Name System (DNS) Filtering/Firewall
	3.6 Email filtering and protection
	3.7 Centralized authentication and authorization (Single Sign On)
	3.8 Content and malicious traffic filtering through anti-virus and threat detection software
	3.9 Ensure patch management program is implemented and up to date
4. Data Recovery and continuity	4.1 Establish and maintain a data recovery process
	4.2 Establish and maintain an isolated/vaulted instance of recovery data
	4.3 Implement disaster recovery and data recovery testing
	4.4 Implement technology to support continuity of services in the case of a natural disaster or cyber attack
5. Security Assessment	5.1 Identify security gaps associated with program objectives which can be supported by the grant program
	5.2 Perform automated vulnerability scans
	5.3 Network and system architecture diagram and assessment

CYBERSECURITY PLAN ELEMENTS

Manage, Monitor, and Track

The cornerstone of an effective cybersecurity program is to first understand what needs protecting. This plan incorporates support of understanding what software and hardware technology is in use along with making sure to prevent unauthorized technology from being introduced into the environment. To support this objective the following strategic approaches have been identified:

- Conduct an inventory of all technology assets used by the organization. The inventory should include necessary support details such as vendor, model, version, etc. of each asset.
- Implement a system for tracking technology assets throughout their lifecycle from acquisition to disposal.
- Establish policies and procedures for managing the lifecycle of technology assets. These policies should include ensuring the security requirements are maintained throughout the lifecycle of the asset.

- Develop and implement a plan for upgrading or replacing technology no longer supported by security patches or critical updates. This plan should include the full decommissioning of the no longer serviceable technology from the environment.

Monitor, Audit, and Track

After understanding the assets in the environment and what needs to protecting the next step is to see what is happening to those assets. Detection of unauthorized activity is critical to preventing a security incident from crippling an organization's ability to function and preventing data from being misused. Understanding that monitoring and detection is simultaneously some of the costliest parts of a cybersecurity program and one that scales significantly, the use of an COV wide SOC is planned to provide monitor and audit the environment. The VA-ISAC and SOC are planned as the state portion of the SLCGP. Monitoring related data from the tools deployed within this program will help ensure adequate detection is in place. The following strategic approach for subrecipients will help ensure monitoring and auditing is in place:

- Deploy authorized host endpoint detection and response technologies to monitor workstations and servers for suspicious activity.
- Implement network monitoring and filtering technologies such as firewalls, DNS filtering, intrusion monitoring and prevention systems and web application firewalls to detect and prevent malicious traffic.
- Participate in the centralized security log monitoring solution to facilitate threat sharing through the Virginia Information Sharing and Analysis Center (VA-ISAC). The centralized security event alerting system will receive and monitor alerts from the tools implemented using the grant program.
- Implement approved network traffic flow log technology to provide visibility into network traffic patterns and identify potential security threats.
- Implement the infrastructure to collect and forward logging information to security monitoring systems.
- Implement and staff a Commonwealth wide security operations center to provide threat monitoring and intelligence information to all public sector entities who participate.

Enhance Preparedness

Preparation is key to ensuring cybersecurity controls and technology is operating effectively within an organization. Preparedness in this case focuses on where the technology and process interact and work together. Testing an organization's incident response capabilities, continuity and disaster preparedness and information sharing are all critical to effective preparedness. The following strategic approach is used to enhance preparedness:

- Develop a comprehensive cybersecurity incident response plan which incorporates the security representatives and, if applicable, the security operations team or equivalent. In circumstances of organizations with limited security resources these should be testing processes between partners who would be most likely to make the organization aware of a cyber security incident (i.e. Virginia ISAC, Multi State ISAC, law enforcement, etc.) and the organizations used to respond to an incident (i.e. cyber insurance designated services, third party contractors, in house incident response staff, etc.)
- Establish and train the security investigation and incident response team with the duties their responsible for performing when responding to malicious activity. The training of these teams should include the roles responsible for making decisions about when to engage resources as well as how to interface with Virginian's about the impact of a security issue.
- Perform penetration testing or red teaming to test an organization's incident response plans. These tests should be looking to both identify weaknesses in the technology controls implemented and the processes involved in response and detection.

Assessment and Mitigation

The threats to public sector environments continue to grow at a rapid rate. In order to protect Virginian's from the ever evolving cyberattacks organizations must continually monitor for vulnerabilities and attack paths that can lead to a compromise of an environment. Using tools and services to understand the threats as well as find weaknesses in the environment is necessary for an effective cybersecurity program. The following areas of focus can help organizations identify areas for concern and mitigation:

- Conduct regular vulnerability assessments to identify potential weakness and vulnerabilities in information systems, applications and user accounts. The use of approved automated scanning tools and assessment technology should be executed on internal and/or public facing systems and applications in order to understand the risk and vulnerabilities an organization is subject to.
- Deploy approved endpoint protection tools to ensure detection and prevention of malicious activity. The implementation must integrate with identified threat and security sharing services.
- Deploy tools which allow for both containment of malicious activity within the organization's environment and prevention of access to the environment.

Best Practices and Methodologies

As part of continually enhancing cybersecurity programs within organizations it is important to incorporate best practices for cyber hygiene as part of any new implementation. All implementations associated with this plan must incorporate and document how they will meet (if applicable) the following set of requirements:

- Multi-factor authentication usage must be included as part of the implementation and implementation plan.

- All implementations must meet identified logging requirements and must share log data with identified parties.
- For any data that is sensitive or may become sensitive encryption must be implemented. Encryption between any hosts and at a minimum volume level encryption must be incorporated into the implementation and implementation plans.
- Any internet accessible solutions which are no longer receiving support for security requirements must be upgraded. Documentation of these systems and their upgrade requirements must be incorporated into the subrecipient request.
- As part of the completion of an effort the subrecipient must indicate all default passwords have been changed and are meeting specified password complexity requirements.

Additionally efforts to implement any of these best practices as an upgrade to existing solutions will be considered as part of the application.

Safe Online Services

Impersonation of digital services for Virginians continues to increase, leading to more frequent victims of fraud. It has become increasingly difficult to ensure the website a Virginian is interacting with is a verified government website. To combat this issue applicants must establish a website presence using a .gov website address. This site must meet the following requirements:

- Indicating the name and contact information for the organization.
- Include reference for the authorized location of where Virginians should interface with the organization either digitally or physically.

Continuity of Operations

Organizations today rely heavily on their information systems and the data presented from them. When those systems aren't available, most organizations struggle to perform their business objectives. In government organizations, this issue is further challenging because government must function even when nothing else is functioning. Ensuring government systems and data remain available means having a resilient design and a robust recovery method. Enhanced protection of backups is also critical because backups are one of the primary targets of a disruptive cyber attack. The following strategic approach is designed to ensure government is able to operate in the case of a cyber attack or other disruption:

- Implement backup and restoration validations processes and procedures to ensure adequate data recovery
- Establish a secure offline separate backup location (i.e. vaulted backup) to protect against cyber disruptions such as ransomware.
- Implement technology allowing for continuity of services in the case of a disaster scenario

- Identify network continuity requirements and technology in the case of an outage due to disaster or cyberattack
- Leverage the Commonwealth Emergency Operations Plan (cyber annex) in the case of a large scale cyber disasters

Workforce

The cyber workforce is challenging to navigate for two primary reasons. The first is the ability to understand the type of expertise within an organization's environment. Whether the need is more technical in nature (such as supporting firewalls) or more focused on the cyber program (such as an information security officer), identifying the knowledge, skills, and abilities required can be a difficult task. Fortunately, the NIST National Initiative for Cybersecurity Education (NICE) provides a framework for the type of cyber personnel needed. Additionally the framework provides details about the knowledge skills and abilities for each of the role types in the cybersecurity field.

- Applicants must include reference to roles within the NICE framework when describing any personnel support needs in support of the program objectives.
- Applicants must include reference to the roles within the NICE framework when identifying security training for cybersecurity roles

Cyber Threat Indicator Information Sharing

Threat sharing is a key component in preventing malicious activity from becoming widespread. Quickly and effectively share threat information between organizations is critical to a successful, whole-of-state approach to defending our environment. To facilitate this effort, Virginia plans to establish a VA-ISAC for cyber threat sharing and incident coordination between government entities. Key features of a VA-ISAC relevant to this program include:

- The VA-ISAC will provide a shared SOC available for use by state, local, and tribal entities.
- Any subrecipient solutions from this program will be required to share information with the VA-ISAC and the VA-ISAC SOC.
- Subrecipients who receive grant funding must sign up as a member of the VA-ISAC, MS-ISAC and EI-ISAC.
- The VA-ISAC will facilitate sharing for CISA's Cyber Information Sharing and Collaboration Program (CISCP) and MS-ISACs indicator feeds.

Department Agreements

All entities participating in the grant program are required to share their threat indicators and corresponding information from the tools implemented in the environment with the VA-ISAC. The application for the grant program will include an MOU indicating the applicant's agreement to share data.

Leverage CISA Services

Subrecipients are required to obtain services supporting objectives in this plan using approved contracts and service providers. CISA services meeting the objectives are considered an approved service provider. Several of the program objectives include support for implementing CISA services.

Information Technology and Operational Technology Modernization Review

Maintaining a modern information and operational technology environment ensures both current security capabilities and knowledgeable and available resources to effectively manage and protect the technology. Modernization efforts should be evaluated within 5 years of technology implementation in the environment. Certain technologies (such as those in the operational technology area) may have a longer lifespan, but an evaluation should be completed to understand if an update is warranted or not. Additionally, the use of cloud services (such as software-as-a-service [SaaS] and platform-as-a-service [PaaS]) should be leveraged as much as possible to remove the need for large capital investments into an organization. Those organizations leveraging services which have predictable sustainability will help maintain a modern environment.

Cybersecurity Risk and Threat Strategies

The development of this plan is the first step in the process for investment in the whole of state approach. The Virginia Cybersecurity Planning Committee appointees represent different government entities that have a stake in the whole of state approach and cybersecurity strategy. Additionally, the Committee sought experienced and interested advisors, who have provided input and feedback to the Committee about the approach. Current entities and the planned VA-ISAC should be able to provide information to the Committee about the effectiveness of the technology implemented based on data collected.

In addition to coordination, this plan will prioritize capabilities which mitigate the most number of risks and threats for the amount of effort. The program objectives chosen are based on the CIS critical control list. The items within that list are identified as the most effective technologies and business practices for mitigating risk to an organization.

Rural Communities

In order to help rural communities get the most out of this program, the plan has a structured path for identifying the areas for which communities should request support. One of the objectives identified is to perform a review of the technology environment to identify the objectives that would be appropriate and most beneficial for the rural community to pursue. This review will be performed by a third party and will help produce a plan for the organization and what needs should be highlighted when applying to be a subrecipient of identified objectives. This will provide the rural organization with a plan for submitting to all of the remaining grant submission cycles.

FUNDING & SERVICES

This program is designed to provide funding to localities to support their cybersecurity program. The funding is focused on providing technology and services in as cost-effective manner as possible while including the needed expertise at the local level for implementation. The structure is heavily focused on obtaining services, products, and/or licenses, not funding staff at an organization. This approach should prepare organizations to either address the hurdle of the large capital investment needed for implementing cybersecurity tools or provide funding for establishing and maintaining third party cybersecurity services.

This program sets up a structure that integrates the technology and services provided for the state, local, and tribal of this program with a centralized monitoring program at the VA-ISAC. The VA-ISAC will be funded by the state portion of the grant funding to establish both a centralized/regional SOC function and an information sharing function with public sector entities within Virginia.

To ensure funds have the opportunity to be used efficiently as possible and ensure services are provided consistently, the use of approved contractual vehicles is necessary and will be considered as part of the evaluation process. The areas for investments should cite the program objectives established in this plan and what technologies and/or services they will use to meet them.

Distribution to Local Governments

Distribution will use a methodology that prioritizes submissions which support the identified primary initiatives of the grant window. For example if the current grant window primary initiatives are for endpoint protection, environment assessment and enterprise asset inventory submissions supporting those initiatives will be prioritized.

Additionally submissions must include which technology and implementation method the request will leverage. The subrecipient must indicate which of the included list of technologies and/or services they plan to implement and the approach planned based on the provided list of options. In the case the provided technology and/or services for that technology is not considered adequate please propose an alternative along with the reason for not leveraging the included technology. Use of the included options is highly encouraged to secure the most cost effective and efficient approach.

Options for implementation approach will be identified as one of the following:

- Contract Only – A pre-approved authorized/legal procurement vehicle. The organization is responsible for all aspects of the 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 would like support to build, implement and run the program objective technology or processes. These services require the least amount of support from the organization.

Request for proposals will be sent to eligible entities outlining how to apply for the program. In the case an organization doesn't have the resources to determine the right approach or isn't certain of how to best structure the approach they can indicate selection of 5.1 on the request form. This will engage resources to assess the organization's environment, identify gaps in the areas outlined within the program objectives and develop the submission for this grant opportunity.

Each submission will include an MOU indicating the subrecipients acknowledgement of the terms and understanding of participation in the threat sharing between participating entities.

Submissions meeting the rural criteria will be prioritized until the 25% criteria has been reached. There is some concern regarding getting enough rural community submissions in the first set of projects. In the case there aren't enough submissions for the 25% criteria in the grant requests, the 25% amount will be set aside until enough rural communities have been identified.

[PENDING COMMITTEE DISCUSSION]

Use the table in **Appendix B: Project Summary Worksheet** to list items, services, capabilities, or activities you plan to provide to local governments to implement your cybersecurity plan.

By documenting your entity's approach distribute funds, items, services, capabilities, or activities to local governments (including distribution of 25% of cybersecurity grant funding received to rural areas) demonstrates that the plan meets requirement **in the State and Local Cybersecurity Improvement Act: e.2.B.xvi.**]

ASSESS CAPABILITIES

[In accordance with the State and Local Cybersecurity Improvement Act; Describe the strategic approach implemented to assess capabilities for the preceding requirements (cybersecurity plan elements) outlined above. Information can be captured in **Appendix A: Cybersecurity Plan Capabilities Assessment**.]

IMPLEMENTATION PLAN

Organization, Roles and Responsibilities

Virginia has a centralized information security program for state government entities. There is a statute establishing the chief information officer as responsible for maintaining cybersecurity policies and standards for the legislative, judicial and executive branches. In addition, the executive branch's information technology program, which includes information security tools is managed centrally within the state information technology agency. While localities are not governed by state requirements directly, all SLTT organizations are responsible for maintaining security requirements where there are interfaces between government entity systems.

In order to facilitate a centralized connection point between organizations for cybersecurity issues, the state plans to establish an information sharing and analysis center. The role of this organization is to be an entity which can assist in the prevention, detection and response areas for those SLTT organizations that don't have the expertise or resources for a fully staffed information security program. Those organizations taking part in the grant program will be required to share data with the information sharing and analysis center to help advance the state of cybersecurity across the Commonwealth.

Appendix B: Project Summary Worksheet provides a list of cybersecurity projects to complete that tie to each goal and objective of the Cybersecurity Plan.

Resource Overview and Timeline Summary

The cybersecurity plan will be implemented over the next 3 years using a combination of SLTT resources and third party service. Each project has a timeline included and has completion criteria within the grant window.

METRICS

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software) 1.2 Ensure only authorized assets connected to enterprise systems and are inventoried 1.3 Upgrade or replace all software no longer receiving security maintenance/support 1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business 1.5 Identify all government websites and migrate non .gov sites to .gov domains 1.6 Establish and maintain inventory of administrator, service and user accounts	1.1 Implement staff augmentation or third party services to asses 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 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 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 Implement staff augmentation or third party services to asses 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 Implement staff augmentation or third party services to migrate existing	100% of targeted websites	Frequency: Monthly Source: Sites publicly available

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	websites to .gov addresses. This migration must include the primary government website (i.e. localityname.gov)		
	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
2.1 Deploy host intrusion detection/prevention and/or endpoint detection and response for all workstations and servers 2.2 Deploy network traffic collection, filtering and detection at network egress and ingress points 2.3 Centralize security event alerting 2.4 Audit log collection for all servers and systems hosting data in accordance with log management standards 2.5 Web application firewall	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.
	2.2.1 Implement third party services to install netflow monitoring at the egress of where a majority of server traffic	At least 1 device deployed and reporting data	Frequency: Completion of installation and quarterly review of data

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	is traversing or the location that has the most amount of network traffic and will support an approved configuration	Target coverage 90% of assets	
	2.2.2 Implement third party services to deploy and/or manage firewall, IDS/IPS technology at an organizations egress with deep packet inspection, malware detection, application awareness, intrusion detection and intrusion prevention	Devices deployed Reports on threat activity available Target coverage 90%	Frequency: Completion of information and quarterly review of data
	2.3.1 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
	2.4.1 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
	2.5.1 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.

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	Program Sub-Objectives	Associated Metrics	Metric Description (details, source, frequency)
	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.
~~3.1 Implement and manage firewalls on all end point devices (i.e. user workstations, servers)~~	NOTE: Collapsed into 2.1		
~~3.1 Implement and manage network firewalls for ingress and egress points~~	NOTE: Collapsed into 2.2		
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 3.4.2 Implement multifactor authentication for Virginian identifies	Accounts implemented with multifactor Target: 100% Minimum: 90%	Source: Target accounts per system or in the environment Frequency: Monthly
3.5 Domain Name System (DNS) Filtering/Firewall	3.5.1 Implement or have third party services implement and configure hosts to	Hosts leveraging DNS filtering / Total hosts in the environment	Sources: Number of devices in organization inventory

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	utilize approved DNS filtering services	Target: 100% Minimum: 90%	Frequency: Monthly
3.6 Email filtering and protection	3.5.1 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 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	Number of organization users with single sign on Number of Virginians with single sign on	Sources: User access list Frequency: Monthly
3.8 Content and malicious traffic filtering through anti-virus and threat detection software	3.8.1 Obtain licenses for content/malicious traffic filtering 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	Number of hosts with filtering and detection	Sources: asset inventory and protected system list Frequency: Monthly
3.9 Ensure patch management program is implemented and up to date	3.9.1 Have a third party upgrade out of date systems 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	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

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
4.1 Establish and maintain a data recovery process	4.1.1 Develop or have a third party develop a business continuity plan and/or disaster recovery plan that enables the recovery of critical information systems that support business processes for all cloud based and locally stored data.	100% of Critical services will be brought online within 72 hours	Source: Asset inventory Frequency: Once
4.2 Establish and maintain an isolated/vaulted instance of recovery data	4.2.1 Obtain licenses for a vaulted data recovery solutions 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	90% of critical data vaulted	Frequency: Source Source: Total GB of data vaulted out of total GB of critical data
4.3 Implement disaster recovery and data recovery testing	4.3.1 Have a third party test the disaster recovery and/or business continuity plan	Successful recovery within plan established time frame	Frequency: Once Source: Disaster recovery plan information
4.4 Implement technology to support continuity of services in the case of a natural disaster or cyber attack	4.4.1 Obtain or have a third party provide services to maintain communications in the case of a regional disaster within 500 miles	Successful test of continuity services	Frequency: Semi-Annually Source: Recovery plan and certification of completion
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 Mitigation plans can begin within 30 days Training to begin within 90 days of award	Frequency: Quarterly

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	5.1.2 Obtain services to review and evaluate existing risk assessments/mitigation plans for potential options 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 *5.1.5 Obtain security awareness training for end users*		
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 within 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 5.3.2 Obtain staff augmentation or have a third party document the organizations network architecture	Network architecture documentation	Source: Asset inventory and network architecture Frequency: Once All assets and/or asset types must be identifiable on the architecture

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

[By taking the following actions, an entity will demonstrate that their cybersecurity plan incorporates the required assessment relating to the **Cybersecurity Plan Required Elements.** Ensure that the assessment incorporates an **entity-wide** perspective**.** It also links any line items from the **project summary worksheet** that will help to establish, strengthen, or further develop your cybersecurity capabilities**.**

Eligible entities can use the "EVAL" column as a self-assessment tool. Entities with newly initiated programs could use this spreadsheet to track the status of their cybersecurity planning efforts. Similarly, entities with advanced programs could use this worksheet to evaluate their current cybersecurity plan using "Yes, No, Partial, or N/A."]

COMPLETED BY [ENTITY]				FOR ASSESSOR
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of State, Local, and Tribal entities within the Eligible Entity**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts				
2. Monitor, audit, and track network traffic and activity				
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts				
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk				
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)				

a. Implement multi-factor authentication				
b. Implement enhanced logging				
c. Data encryption for data at rest and in transit				
d. End use of unsupported/end of life software and hardware that are accessible from the Internet				
e. Prohibit use of known/fixed/default passwords and credentials				
f. Ensure the ability to reconstitute systems (backups)				
g. Migration to the .gov internet domain				
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain				
7. Ensure continuity of operations including by conducting exercises				
8. 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)				
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks				
10. 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 jurisdiction of the eligible entity				
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department				
12. Leverage cybersecurity services offered by the Department				
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives				
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats				
15. Ensure rural communities have adequate access to, and participation in plan activities				
16. Distribute funds, items, services, capabilities, or activities to local governments				

APPENDIX B: PROJECT SUMMARY WORKSHEET

[The project worksheet should mirror all projects applied for in the Individual Justification (IJ) form.]

Purpose: The **Project Summary Worksheet** is a list of cybersecurity projects that the entity plans to complete to develop or improve any needed cybersecurity capabilities identified in **Appendix A: Sample Cybersecurity Plan Capabilities Assessment**.

[Instructions: Completing the table below, including the following information in each column to expedite review and approval:

- **Column 1**. Project number assigned by the entity
- Column 2. Name the project
- Column 3. Brief (e.g., 1-line) Description of the purpose of the project
- Column 4. The number of the Required Element the project addresses
- Column 5. Estimated project cost
- **Column 6.** Status of project (future, ongoing, complete)
- **Column 7.** Project priority listing (high, medium, low)
- **Column 8.** Project Type (Plan, Organize, Equip, Train, Exercise)]

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type

APPENDIX C: ENTITY METRICS

[Describe the metrics you will use to measure implementation and cybersecurity threat reduction (to be provided in your annual report to CISA), including:

1) progress toward implementing the cybersecurity plan; and
2) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to your information systems.

Consider the following when developing metrics:

- Metrics must be aligned to the Cybersecurity Plan and the established goals and objectives
- Review existing metrics that are already be used across the eligible entity
- The data for each metric must be available and reportable and should not create unnecessary bourdons to collect.

The below table should reflect the goals and objectives the Cybersecurity Planning Committee establishes.

Cybersecurity Plan Metrics			
Program Goal	Program Objectives	Associated Metrics	Metric Description (details, source, frequency)
1.	1.1		
	1.2		
	1.3		
2.	2.1		
3.	3.1		
	3.2		
4.	4.1		
	4.2		
	4.3		
5.	5.1		

APPENDIX D: ACRONYMS

Acronym	Definition

Year 1 Priorities and Guidelines

Introduction

The state and local cybersecurity grant program (SLCGP) is a whole of state approach to providing cybersecurity resources to localities. The program is structured to provide resources to eligible entities to support and/or implement an information security program at a state, local, tribal or territory (SLTT) entity.

Virginia has established a cybersecurity planning committee whose mission is to create and maintain a holistic plan to for supporting cybersecurity programs at SLTT organizations. This plan outlines the primary objectives the planning committee has identified as critical to an organization's cybersecurity program. These instructions include how a SLTT organization can apply for funds to implement and/or support those objectives. Additionally, the instructions outline the requirements an organization must agree to when accepting these funds. The following sections will outline the steps and details for filling out the application and interacting with the grant program. Questions can be sent to cybercommittee@vita.virginia.gov if there are any questions about the program or the application process.

Program Strategy

One of the key capabilities a whole of state approach brings to SLTT entities is the ability to provide threat information between SLTT entities. To facilitate this capability the plan is utilize the state portion of the grant funding to VA-ISAC which will maintain threat information relevant to SLTT organizations and will provide shared security operations center (SOC) and/or SOC related services to SLTT entities. A shared SOC provides an efficient way for SLTT entities to maintain visibility into malicious activity impacting their environment. In order for the SOC to be the most effective for all entities in the grant program SLTT grant recipients must agree to share the data from tools and/or services implemented using the grant program with the VA-ISAC. The memorandum of understanding included with the grant application includes protection for this data from being shared outside of the VA-ISAC.

Each grant update cycle will prioritize program objectives within the plan. This approach will help negotiate the best pricing possible along with ensuring basic levels of security are in place in as many SLTT entities as possible. Including a submission for a non-prioritized objective is still encouraged, however if an organization is deciding between multiple objectives the prioritized objective is the recommended submission.

The following objectives are prioritized for the 2022-2023 submission cycle:

1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software)
1.2 Ensure only authorized assets connect to enterprise systems and are inventoried
1.3 Upgrade or replace all software no longer receiving security maintenance/support
1.5 Identify all government websites and migrate non .gov sites to .gov domains
2.1 Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers

Year 1 Priorities and Guidelines

2.2 Deploy network monitoring, filtering and detection at network egress and ingress points
2.3 Centralize security event alerting
2.4 Collect network traffic flow logs
3.1 Implement and manage firewalls on all end point devices (i.e. user workstations, servers)
3.2 Implement and manage network firewalls for ingress and egress points
3.4 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access
3.5 Domain Name System (DNS) Filtering/Firewall
3.6 Email filtering and protection
3.9 Ensure patch management program is implemented and up to date
5.1 Identify security gaps associated with program objectives which can be supported by the grant program
5.2 Perform automated vulnerability scans
5.3 Network and system architecture diagram and assessment

Steps for Applying to the Grant Program

Step 1 – Identifying the program objectives

The full list of program objectives is available in the Commonwealth of Virginia Cybersecurity Plan. Each grant cycle will focus on a specific set of primary objectives. The current primary objectives are included in this document. While the applying SLTT entity is not required to only apply for the included objectives, priority will be given to applications for the current submission cycle identified objectives.

In the case an organization needs assistance in assessing their needs for one or more of the program objectives, submit an application requesting a resource for objective 5.1 - Identify security gaps associated with program objectives which can be supported by the grant program. The result should be information the organization can use to create additional applications.

Step 2 – Review the technology options and service models

Each program objective will have technology options included with them. These options have corresponding contracts already available for SLTT entities to leverage. Entities can provide alternative contract vehicles as long as adequate justification can be provided for selecting an alternative contract (i.e. pricing for equivalent services or desired services not provided).

In addition to selecting a contract vehicle the type of service model must be selected. The service model options can be selected based on the type of assistance the organization needs. One of the following options must be included with the application:

- Contract Only – A pre-approved authorized/legal procurement vehicle. The organization is responsible for all aspects of the implementation other than establishing the contract.

Year 1 Priorities and Guidelines

- 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 would like third party support to build, implement and run the program objective technology or processes. These services require the least amount of support from the organization.

Step 3 – Complete the Project Description Template

This template outlines the details of the projects that the organization plans to implement. Each project must include basic details about current status and the objectives the project will meet. In addition, the metrics for the measurement for project success based on the metric targets indicated in the plan.

Along with the estimated resources needed for the project an indication of whether funds will be committed to sustain the solution once grant funds have been expended.

Step 4 – Review and sign the MOU with the Submission

This template includes an MOU establishing the relationship between the applicant and the state for providing funds and/or services. Entities may be required to integrate technology and/or services with an identified threat sharing body as a requirement in the project. Projects should include plans to integrate with centralized threat monitoring and management as part of the implementation. The MOU outlines the data sharing parameters that are part of these requirements.

Year 1 Priorities and Guidelines

EXAMPLE

Below are the objectives with suggested technology options and known contract vehicles.

OBJECTIVE: 2.1 Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers

- CrowdStrike Falcon - **ECOS/SHI**

OBJECTIVE: 2.2 Deploy network monitoring, filtering and detection at network egress and ingress points

- Cisco Firepower NGFW (Next-Generation Firewall)
- Palo Alto Networks Next - Generation Firewall- **THUNDERCAT/ SHI**
- Fortinet FortiGate - **SHI** publisher

OBJECTIVE: 2.3 Centralize security event alerting

- Splunk Enterprise Security- THUNDERCAT/SHI/ECOSS
- Microsoft Sentinel
- Google Chronicle

Following presentation of an action item, the Chair will ask for a motion to adopt the action item. Upon receiving a second, the Chair will ask if there is any discussion concerning the motion. At that point, the action item will then be in the proper posture to be discussed and considered by the committee. It will also be in the proper posture at that point for any member to offer amendments to the language.

Each member who wishes to participate in the discussion of any of the action items needs to first be recognized by the Chair prior to speaking. If you wish to be recognized, simply raise your hand. The Chair has discretion as to the purpose for which they wish to recognize a member, and if, in the Chair's opinion, the member's desired purpose is not germane to the current discussion or could cause confusion or interfere with the efficient and orderly operation of the Committee, the Chair may choose to delay recognition of the member until after the current discussion/item, but before the Committee's work/meeting is completed.

If any member wishes to offer an amendment to any action item, the amendment needs to be offered in the form of a motion. In making that motion, the member needs to state to the committee the language change/changes they are proposing to the text. If that motion receives a second from another member, the Committee will discuss and subsequently vote on the motion.

If, upon hearing the proposed PRIMARY amendment, another member desires to further amend that amendment, that member must make a SECONDARY AMENDMENT in the form of a motion, which also must receive a second.

Upon receiving a second, the Committee will discuss, and then vote on the SECONDARY AMENDMENT prior to voting on the PRIMARY amendment. If the amendment(s) is(are) adopted, they will be added to the main motion and the Committee will move on to the next amendment and repeat the process. Please note that a secondary amendment that is worded such that it completely negates the primary amendment's meaning can get confusing, but if it is adopted it would be attached to the main motion/PRIMARY amendment directly.

According to Robert's Rules, there can only be one secondary amendment offered. There can be no "amendment to the amendment to the amendment".

Members may provide VITA with written copies of proposed amendments prior to the meeting, which will be included in committee packets. Members may also bring written copies of proposed amendments with them to the meeting which will be photocopied by VITA staff and distributed to the Committee prior to consideration. If any member wishes to make amendments but has not yet reduced them to writing, VITA will be able to type the proposed amendments into the computer and the proposed language will be displayed on the screen for the Committee's consideration prior to voting on the motion. The Chair will ask VITA staff to read the draft amendment. Once the member is satisfied that the

amendment has been correctly stated, the Chair will ask the member to offer the amendment in the form of a motion.

The Committee must vote on any individual amendments and then the action item as a whole. Votes can be taken via a voice vote with a simultaneous show of hands or a roll call vote. All votes are recorded as part of the official committee meeting minutes.

Robert's Rules provides that any member can make a motion to "call the previous question", or "call for the question". If that motion is seconded, it is not debatable; hence the Committee will end discussion and proceed with a vote on the motion (item for consideration before them). If it is agreed to by a two-thirds majority of the members, discussion of the pending motion (for example, an amendment that is under consideration) will end and the Committee will immediately vote on the motion. If the motion to call the previous question does not receive a two-thirds majority of the votes, the discussion will continue.

Finally, please note that under Robert's Rules, a motion must receive a majority vote among the members present and voting in order to be approved. If a motion receives a tie vote, the motion is rejected and does not pass.

Action	What to Say	Can interrupt speaker?	Need a second?	Can be Debated?	Can be amended?	Votes needed
Introduce main motion	“I move to...”	No	Yes	Yes	Yes	Majority
Amend a motion	“I move to amend the motion by (add) (strike words)…"	No	Yes	Yes	Yes	Majority
End Debate	“I move the previous question”	No	Yes	Yes	No	Majority
Adjourn the meeting	“I move to adjourn the meeting.”	No	Yes	No	No	Majority
Extend the allotted time	“I move to extend the time by XX minutes	No	Yes	No	Yes	2/3 Vote

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee

Charter & Bylaws

vita.virginia.gov

November 7, 2022

ARTICLE I. Applicability.

SECTION 1. General.

The Virginia Cybersecurity Planning Committee was created and has the authority to adopt a charter and bylaws pursuant to the Infrastructure Investment and Jobs Act (IIJA), Pub. L. No. 117-58, § 70612 (2021), and Item 93(F) of Virginia's 2022 Appropriation Act. The provisions of these Charter and Bylaws are applicable to all proceedings of the Virginia Cybersecurity Planning Committee ("VCPC") to the extent that the same are not otherwise governed by legislative or executive requirements. To the extent the provisions and authorizations of these Bylaws conflict with legislative or executive mandates, the latter shall control.

SECTION 2. Authority and Limitations.

VCPC is constituted under the IIJA and Item 93 as a "planning committee." As a "planning committee", VCPC is specifically charged with:

- Assisting with the development, implementation, and revision of the Cybersecurity Plan;
- Approving the Cybersecurity Plan;
- Assisting with the determination of effective funding priorities;
- Coordinating with other committees and like entities with the goal of maximizing coordination and reducing duplication of effort;
- Creating a cohesive planning network that builds and implements cybersecurity preparedness initiatives using FEMA resources, as well as other federal, SLT, private sector, and faith-based community resources;
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Ensuring local government members, including representatives from counties, cities, and towns within the eligible entity provide consent on behalf of all local entities across the eligible entity for services, capabilities, or activities provided by the eligible entity through this program.

The VCPC is not permitted to make decisions relating to information systems owned or operated by, or on behalf of, the state.

ARTICLE II. Members

SECTION 1. Voting Members.

Members shall consist of residents of the Commonwealth appointed by the Governor in accordance with Item 93 for terms of 4 years. At least one half of the representatives of the Cybersecurity Planning Committee must have professional experience relating to cybersecurity or information technology. A vacancy other than by expiration of term shall be filled by the Governor for the unexpired term. Each appointed member has one (1) vote.

Composition of Voting members

Representation	Organization
Eligible Entity	Virginia IT Agency

Eligible Entity	Virginia Department of Emergency Management
Institution of Public Education	Virginia Department of Education
Institution of Public Health	Virginia Department of Health
Elections infrastructure official	Vacant/TBA
Office of Governor	Secretary of Homeland Security
Tribal Representative	Monacan Indian Nation
State National Guard	Virginia National Guard
High-Population Jurisdiction	Fairfax County
Suburban Jurisdiction	Franklin County
Rural Jurisdiction	King William County
Legislature	Department of Legislative Automated Services
Public Safety	Virginia State Police
State judicial entity	Office of the Executive Secretary of the Supreme Court of Virginia
Private Sector	Woods Rogers
Public Schools	Roanoke City Public Schools

SECTION 2. Advisors

At the discretion of the Chair, additional persons representing key stakeholders or subject matters may be designated as advisors to the VCPC. Advisors may be designated for a particular purpose or on an ongoing basis. Advisors may participate in meetings of the VCPC outside of public comment periods but are not voting members of the VCPC.

SECTION 3. Officers

The VCPC shall be chaired by the Chief Information Officer of the Commonwealth (CIO), or the Chief Information Security Officer (CISO) as his designee, in accordance with the IIJA and Item 93. The Chair shall preside at all VCPC meetings. A Vice Chair shall be elected from among the voting members through nomination and formal vote, and the Vice Chair may preside at meetings, call a special meeting, and fulfill other similar administrative duties in the absence or temporary unavailability of the Chair. Additionally, the VCPC shall select a member to serve as chairperson of any subcommittees.

SECTION 4. Representation of VCPC.

When the VCPC is requested to appear before the General Assembly, or legislative or study committees, the planning committee shall be represented by the Chair, or by one or more members duly designated by the Chair and, when practicable, confirmed by the planning committee.

ARTICLE III. Meetings and Public Disclosure.

SECTION 1. Regular Meetings.

Regular meetings of VCPC shall be held on at least a quarterly basis, at such time and place as the VCPC may determine, or as needed as determined by the Chair. No business requiring a vote or final decision of VCPC may be conducted in the absence of a quorum, as defined in Article III,

Section 4.

SECTION 2. Subcommittees and Work Groups.

The Chair may call a special meeting, or create a subcommittee or work group, for a specific purpose or purposes. The notice of a special meeting shall set forth the business to be transacted at such special meeting. If a subcommittee or work group is created and will hold more than a single meeting, that subcommittee or work group shall report on its work at each meeting of the VCPC until its business is concluded.

SECTION 3. Notice of Meeting.

Public notice of meetings shall be provided in accordance with applicable law, including the requirements of the Virginia Freedom of Information Act, Va. Code § 2.2-3700, *et seq* (VFOIA).

SECTION 4. Quorum.

A quorum shall constitute a simple majority of the voting members of the VCPC.

SECTION 5. Conduct of Meetings.

Meetings may take place using electronic communication means to the extent permitted by law. The Virginia Information Technologies Agency (VITA) shall provide staff support, including recording all minutes of the meetings and all resolutions adopted and transactions occurring at each meeting. Should a legislative or executive mandate or these Bylaws not set forth a matter concerning the conduct of meetings of the VCPC, the then current edition of Robert's Rules of Order shall govern. Meetings shall be public, except with respect to closed sessions held in accordance with the law and these Bylaws. Pursuant to Va. Code § 2.2-3710, the VCPC shall not vote by written or secret ballot; voting shall be accomplished by voice vote, show of hands, or roll-call vote.

SECTION 6. Closed Session.

Prior to meeting in a closed session, the VCPC must vote affirmatively to do so and must announce the purpose of the session. This purpose shall consist of one or more of the purposes for which a closed session is permitted in accordance with applicable law, including VFOIA. Minutes may be taken during a closed session but are not required. If taken, such minutes shall not be subject to mandatory public disclosure.

SECTION 7. Official Records.

All official records of the planning committee shall be kept on file at VITA and shall be open to inspection in accordance with applicable law. All files shall be kept in accordance with applicable records retention requirements, including the Virginia Public Records Act, Va. Code § 42.1-76, *et seq*. Draft minutes and other meeting records shall be published on VITA's website as soon as practicable. Minutes of a meeting become final after VCPC review and approval, normally through presentation at the next meeting.

ARTICLE IV. Programmatic Priorities

Programmatic priorities will be set by vote of the VCPC, in accordance with the cybersecurity plan. Staff shall document the decisions in the meeting minutes and make them public via VITA's website and, as appropriate, other channels, such as the grants listserv of the Virginia Department

of Emergency Management (VDEM).

ARTICLE V. Financial Decision Making

Financial decisions will be set by vote of the VCPC, in accordance with the priorities set forth in the cybersecurity plan. Staff shall document the decisions in the meeting minutes and post the information on the VITA website.

ARTICLE VI. Amendments to the Charter and Bylaws

The VCPC shall review the Charter and Bylaws and may amend them as necessary. The Charter and Bylaws may be amended at any regular meeting of the VCPC by an affirmative vote of two-thirds of the VCPC membership present and voting.

These Bylaws were adopted by the VCPC, and became effective, on November 7, 2022, and remain in effect until subsequently amended.

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 November 2022, 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 November 2022, such all-virtual public meetings are 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, and may not be held consecutively with another all-virtual public meeting.)

Requests

Requests for remote participation or that VCPC conduct an all-virtual public meeting shall be conveyed to VITA staff who shall then relay such requests to the Chair of the VCPC.

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.

_____

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 subsection B of § 2.2-3708.3 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;
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;
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 (member's disability or medical condition, need to provide medical care for a family member or principal residence distance from the meeting location), 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. While the fact that a disability or medical condition prevents the member's physical attendance must be recorded in the minutes, it is not required to 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

The provisions under Virginia Code § 2.2-3708.3(C) and 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 25 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 subsection D of § 2.2-3708.3, 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

2023 Meeting Dates

April 12, 10a-12pm, Wednesday
May 17, 10a-12pm, Wednesday
June 14, 10-12pm, Wednesday
July 19, 10am-12pm, Wednesday
August 16, 10am-12pm, Wednesday
September 20, 10am-12pm, Wednesday
October 11, 10-12pm, Wednesday
November 15, 10am- 12pm, Wednesday
December 13, 10am-12pm, Wednesday