VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
April 12, 2023 – 10am
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Consolidated Draft Cybersecurity Plan	Discussion, led by Chair
Current Contract Options	Supply Chain Management
Grant Prerequisites	Discussion, led by Chair
Public Comment Period	
Other Business	Staff
Adjourn	

Committee Email - cybercommittee@vita.virginia.gov

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
March 15, 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 9:02 am. Mr. Watson welcomed the members.

Presiding:

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

Members Present:

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

Robbie Coates, Director, Grant Management and Recovery, VDEM

Adrian Compton, Tribal Administrator, Monacan Indian Nation

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

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

Capt. 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

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

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

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

Members Participating Remotely:

Charles DeKeyser, Major, Virginia Army National Guard. Major Dekeyser is on temporary duty from his home base for the National Guard.

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

Members Not Present:

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

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

Amy Judd, Records Management and Compliance Specialist, 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 January 13 meeting minutes were displayed on the screen. Upon a motion by Mr. Shumaker and duly seconded by Ms. Williams-Hayes, the committee unanimously voted to adopt the January 13 meeting minutes.

Cybersecurity Plan Development Report

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

Mr. Kestner and Ms. Carnohan presented on this goal and provided an overview of the changes made to the program objectives. They discussed asset inventory control, network security, end-of-life assets, assessment services and password management tools. They also addressed challenges faced by smaller localities without IT groups and suggested additional technical assistance.

Goal 2: Threat Monitoring

Mr. Harrison and Ms. Doherty presented on Goal 2 and described the three tiers of support, gap analysis, managed security services, and vendor agnostic EDR SOC service. They also discussed the importance of setting up a structure for maintaining control and insight of the environment, and an SOC.

Goal 3: Threat Protection and Prevention

Mr. Williams and Mr. Shumaker presented on Goal 3 and suggested adding executive summaries to the goal and objectives to provide examples and clarification, defining sensitive data, encryption, and single sign-on. They also discussed patching, reputation monitoring and change control.

Goal 4: Data Recovery and Continuity

Mr. Compton and Captain Gowin presented on Goal 4 and discussed data recovery, business continuity planning, backup solutions, testing and training.

Goal 5: Security Assessment

Major Dekyser and Ms. Williams-Hayes briefly presented on Goal 5, and it was suggested to add incident response training and risk assessment.

Discussion of Grant Prerequisites

Mr. Watson discussed potential prerequisites for application of the grant. The discussion included: prerequisites with no-cost services, ensuring the services are available, defining which goals are tool-based versus person-based resources, and centralized contracts to lower costs.

Public Comment Period:

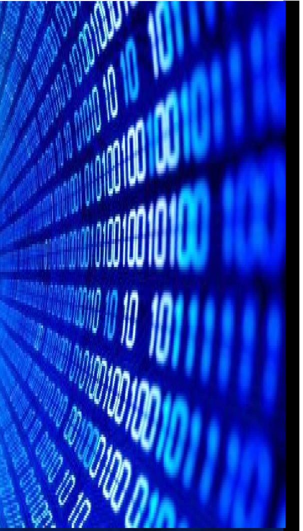
There were no public comments.

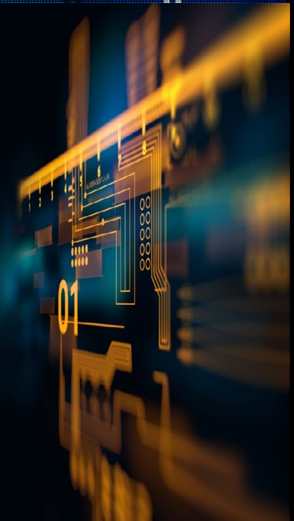
Other Business:

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

Adjourn

Upon a motion by Mr. Kestner and duly seconded by Ms. Carnohan, the committee unanimously voted to adjourn the meeting 12:08pm.





[ENTITY] 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.*

INSERT ENTITY SEAL OR LOGO

MONTH YEAR

Approved by INSERT GOVERNING BODY on INSERT DATE
Version X

[Including this statement regarding the entity's cybersecurity governing body demonstrates that the plan has been approved by an appropriate planning committee]

DRAFT – INTERNAL WORKING DOCUMENT

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM [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 [Entity] am pleased to present to you the 202X [Entity] Cybersecurity Plan. The Cybersecurity Plan represents the [Entity's] continued commitment to improving cybersecurity and supporting our State, as well as cybersecurity practitioners across our local jurisdictions. In addition, this update 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 [[Insert plan priorities]. They are designed to support our entity in planning for new technologies and navigating the ever-changing cybersecurity landscape. They also incorporate the SLCGP required plan elements.

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

Sincerely,

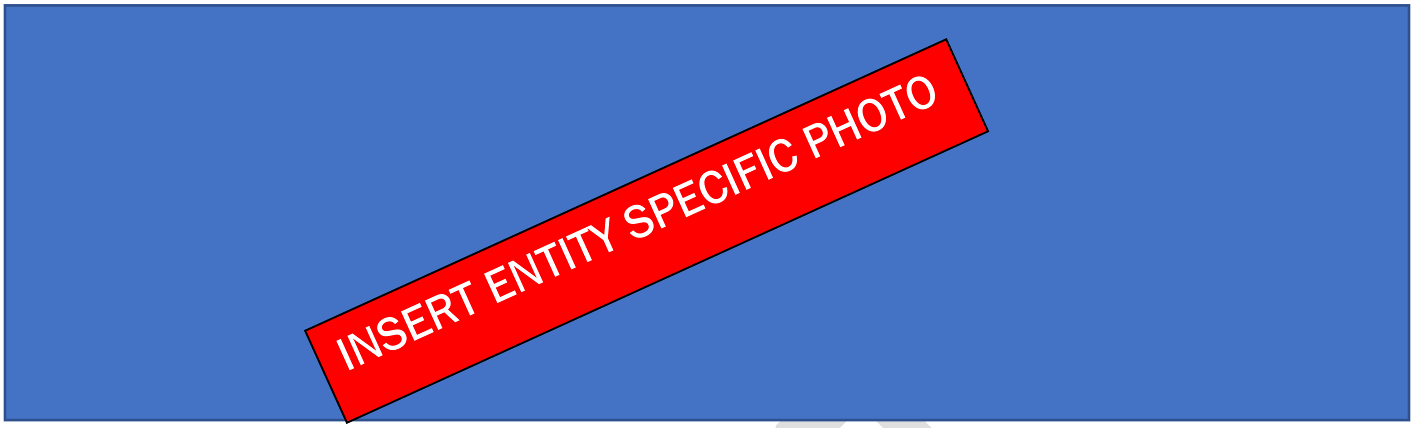
____

[CIO, CISO, CSO NAME]
[ENTITY TITLE]
[DEPARTMENT]

____

[Chair of Cybersecurity Planning Committee]
[ENTITY TITLE]
[DEPARTMENT]

INTRODUCTION



[A Cybersecurity Plan is a key component to helping you build cyber resilience. As applicable, eligible entities should use existing plans, structures, and other relevant efforts to build your comprehensive cybersecurity plan. Building upon existing structures and capabilities allows you to provide governance and a framework to meet your critical cybersecurity needs while making the best use of available resources. For example, consider referencing your emergency management plan to address potential downstream impacts affecting health and safety when responding to or recovering from a cybersecurity incident. For Entities, describe how you will consult, solicit, and incorporate feedback from local governments and association of local governments into your cybersecurity plan.

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 resilience interoperability over the next one-to-three-years.
- **Organization, and Roles and Responsibilities:** Describes the current roles and responsibilities, and any 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. The Cybersecurity Plan is a guiding document and does not create any authority or direction over any of [the entity's] or local systems or agencies.
- **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.

[The following provides an example of how the The National Institute of Standards and Technology (NIST) Cybersecurity Framework can be used. It is not required to adopt the NIST Cybersecurity Framework or any other specific framework, but such frameworks do provide a consistent model to gauge progress over time.] The National Institute of Standards and Technology (NIST) Cybersecurity Framework[1], included in Figure 1, helps guide key decision points about risk management activities through various levels of an organization from senior executives to business and process level, as well as implementation and operations.

[1] https://www.nist.gov/cyberframework/getting-started

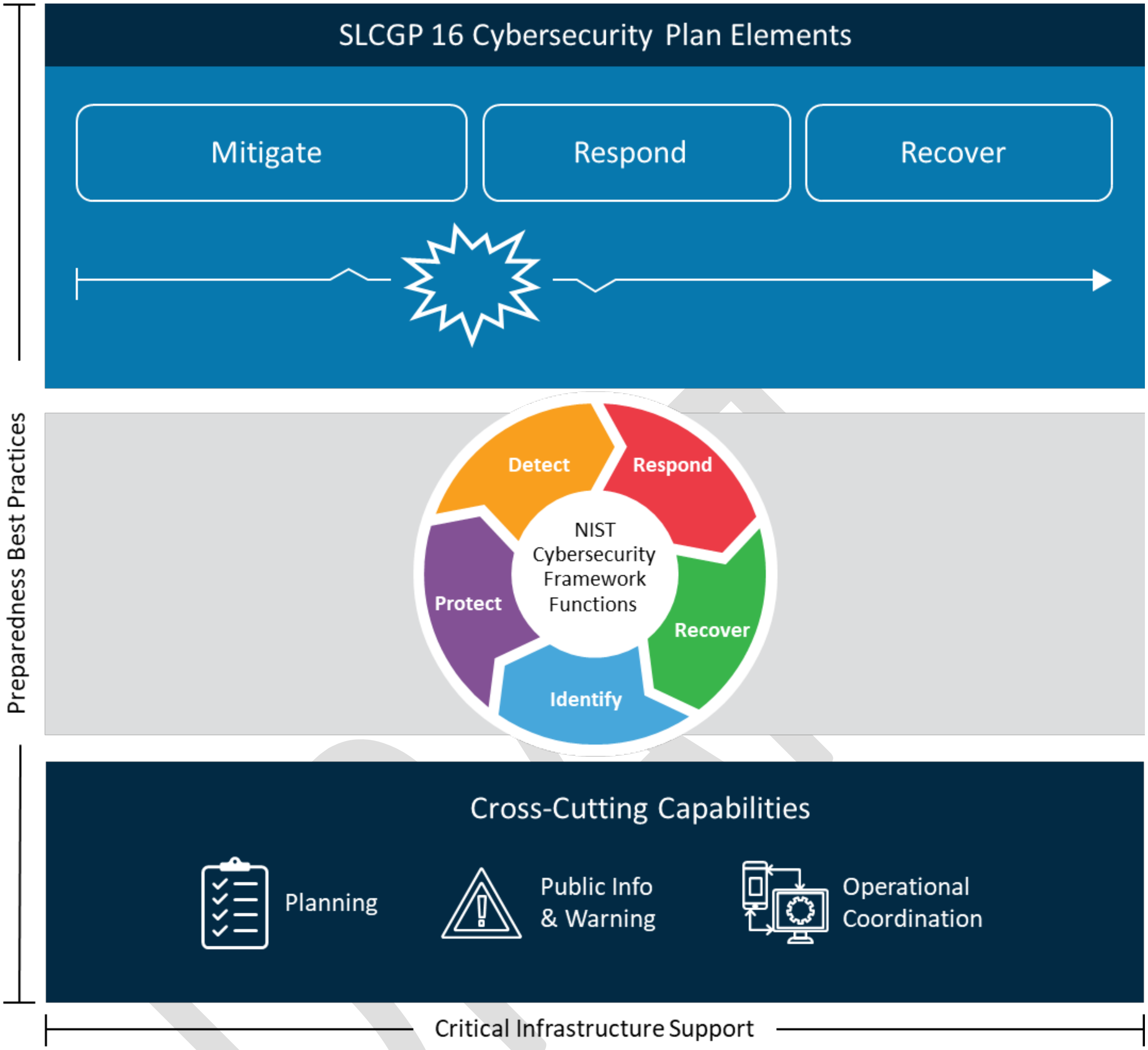

SLCGP 16 Cybersecurity Plan Elements
Mitigate
Respond
Recover
Preparedness Best Practices
Detect
Respond
NIST Cybersecurity Framework Functions
Protect
Recover
Identify
Cross-Cutting Capabilities
Planning
Public Info & Warning
Operational Coordination
Critical Infrastructure Support

Figure 1: Achieving Cyber Resilience Through Comprehensive Cybersecurity Plans

Vision and Mission

This section describes [ENTITY'S] vision and mission for improving cybersecurity:

Vision:

INSERT VISION

Mission:

INSERT MISSION

Cybersecurity Program Goals and Objectives

[The following goals and objectives are different than the SLCGP's goals and objectives. The entity's goals set's the desired and achievable outcome that is typically broad and long-term. Objectives are specific, measurable actions that will be taken to achieve each goal.]

[Entity] 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

Program Goal	Program Objectives
	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
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
	4.1 Establish and maintain a data recovery process
4. Data Recovery and continuity	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
	5.1 Identify security gaps associated with program objectives which can be supported by the grant program
5. Security Assessment	5.2 Perform automated vulnerability scans
	5.3 Network and system architecture diagram and assessment

CYBERSECURITY PLAN ELEMENTS

Note: If you have an existing plan that can meet any of the sections below, incorporate by reference. For example: Document Name in Section XXX.XX and describe the way in which the eligible entity meets each of the plan elements.

Delete before final draft.

This plan incorporates the following plans:

- [Insert plan citation and summary of intent]
- [Insert plan citation and summary of intent]

- [Insert plan citation and summary of intent]

Note: The Cybersecurity Plan is intended to be a strategic plan for the entire entity. Descriptions for each of the following required elements should not focus of a single entity. Instead, the focus should be on setting the desire end state and approach for improving SLTT capabilities within each element across the eligible entity. The plan should address the next 2 to 3 years, recognizing that it can be updated s frequently are necessary.

Delete before final draft.

Manage, Monitor, and Track

[Describe the strategic approach to improve the management, monitoring, and tracking of information systems, applications, and user accounts. Activities can include managing, monitoring, and tracking hardware, software, and services (such as software as a service, cloud services, etc.) that you use for day-to-day business.

NOTE: Systems and technology that are no longer supported by the manufacturer are particularly vulnerable to cybersecurity threats. These legacy systems may require additional effort managing, monitoring, and tracking to effectively protect, detect, respond to, and recover from cybersecurity incidents.

Monitor, Audit, and Track

[Describe the strategic approach to improve the monitoring, auditing, and tracking of network traffic and activity. This could include your security / information technology operation centers, partnerships such as CISA services, MS-ISAC and/or vendor network monitoring, auditing, and tracking services or other specific solutions you use.

Enhance Preparedness

[Describe the strategic approach to enhancing the preparation, response, and resiliency of your information systems, applications, and user accounts against cybersecurity risks and threats. This element addresses the need for comprehensive planning – beyond response to include planning, organization, equipment, training, and exercises.

Assessment and Mitigation

[Describe the strategic approach to implementing a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk. These efforts are to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts you own or are operated on your behalf.

Best Practices and Methodologies

[Describe the strategic approach for adopting and using best practices and methodologies to enhance cybersecurity. The following cybersecurity best practices must be included:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit.
- End use of unsupported/end of life software and hardware that are accessible from the Internet.
- Prohibit use of known/fixed/default passwords and credentials.
- Ensure the ability to reconstitute systems (backups).
- Migration to the .gov internet domain.

These are not required to be implemented immediately, but all Cybersecurity Plans must clearly articulate efforts to implement these best practices across the eligible entity within a reasonable timeline. Individual projects that assist SLTT entities adopt these best practices should also be prioritized.

Additional best practices that the Cybersecurity Plan can address include:]

NIST Principles

[… the cybersecurity framework (CSF) developed by the National Institute of Standards and Technology (NIST) (while adopting the NIST CSF is not required - adoption of a recognized framework will significantly improve your ability to meet this requirement)]

Supply Chain Risk Management

[… cyber supply chain risk management (C-SCRM) best practices identified by NIST. This involves identifying, prioritizing, and assessing information technology suppliers, vendors, and service providers to understand the related and/or cascading risks to your (and, as applicable, all your jurisdictions) supply chain]

Tools and Tactics

[… knowledge bases of adversary tools and tactics. This may involve engaging the MS-ISAC, CISA, and other partners and systems to gain access to knowledge bases of adversary tools and tactics to improve your cybersecurity efforts.

Safe Online Services

[Describe the strategic approach that will promote the delivery of safe, recognizable, and trustworthy online services (including using the .gov internet domain).

Continuity of Operations

[Describe the strategic approach to ensure continuity of operations (COOP) in the event of a cyber incident. Include conducting exercises to practice COOP response actions. This may involve referencing, linking to, or incorporating your continuity of operations plans, systems, and personnel in your cybersecurity plan.

Workforce

[Describe the strategic approach to using the National Initiative for Cybersecurity Education (NICE) Workforce Framework to identify and mitigate any gaps in your cybersecurity workforce. This includes enhancing recruitment and retention efforts, as well as bolstering your personnel's knowledge, skills, and abilities to address cybersecurity risks and threats (for example, providing cyber hygiene training for personnel entity wide).

Continuity of Communications and Data Networks

[For Entities, describe how you will ensure continuity of communications and data networks – across jurisdictions in your purview – in the event of an incident involving those communications or data networks.

Assess and Mitigate Cybersecurity Risks and Threats to Critical Infrastructure and Key Resources

[Describe the strategic approach to the assessment and mitigation, to the greatest degree possible, of cybersecurity risks and threats relating to critical infrastructure and key resources (such as power and telecommunications) that may impact the performance of information systems within your purview.

Cyber Threat Indicator Information Sharing

[Describe the strategic approach to enhancing capabilities to share cyber threat indicators and related information. This may involve leveraging CISA's Cyber Information Sharing and Collaboration Program (CISCP), CISA's Automated Indicator Sharing capability and systems and subscribing to and participating in the MS-ISAC Real-Time Indicator Feeds or other applicable systems and processes to share cyber threat indicators and related information.]

Department Agreements

[Describe how you will share cyber threat indicators and related information with local governments – including by expanding information sharing agreements with CISA.

Leverage CISA Services

[Describe the strategic approach to leveraging cybersecurity services offered by CISA.

Information Technology and Operational Technology Modernization Review

[Describe the strategic approach to your implementation of a modernization review process that ensures alignment between information technology and operational technology cybersecurity objectives.

- Information technology – systems that use, store, retrieve, send, process information, and
- Operational technology – or industrial controls systems, including hardware and software that manages, monitors, and causes physical changes to systems such as water, power, fuels, wastewater, mechanical, industrial, safety, and other systems and process.

Cybersecurity Risk and Threat Strategies

[Describe how the Planning Committee will develop and coordinate strategies to address cybersecurity risks and cybersecurity threats with other organizations, including consultation with local governments and associations of local governments within their jurisdiction, neighboring entities, Territories, and Tribal governments (as applicable), or members of an ISAC; and neighboring countries (this may involve existing international cooperation frameworks, mutual aid, and other agreements with neighboring countries consistent with your authorities and law).]

Rural Communities

[Describe the strategic approach to ensuring rural communities (as described by section 5302 of title 49 of the USC) have adequate access to and are able to participate in cybersecurity services and activities.

FUNDING & SERVICES

[Provide a narrative overview for the program, highlighting key initiatives to strengthen cybersecurity for the eligible entity.]

Distribution to Local Governments

[Describe the strategic approach to the distribution of funds, items, services, capabilities, or activities to local governments, including plans to distribute 25% of cybersecurity grant funding received to rural areas.

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

[Provide an overview of the relationship between the cybersecurity organizations in the entity. Define roles and responsibilities; and if entity is a state, the organizational structure, and identified roles and responsibilities assumed.

Each goal and its associated objectives have a timeline with a target completion date, and one or more owners that will be responsible for overseeing and coordinating its completion. Accomplishing goals and objectives will require support and cooperation from numerous individuals, groups, or agencies, and may be added as formal agenda items for review during regular governance body meetings.

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

[As able, provide an overview of resources needed to implement the plan, as well as the projected timeline to implement the entity's cybersecurity plan.

By documenting, as able, the necessary resources and a projected timeline you demonstrate you're your comprehensive cybersecurity plan meets requirement **in the State and Local Cybersecurity Improvement Act: e.2.E.**]

METRICS

[describe the metrics the eligible entity will use to measure progress towards

- Implementing the Cybersecurity Plan
- Reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.]
- You may use the following table for reporting metrics. Please note: This table requests **PROGRAM OBJECTIVES NOT THE CYBERSECURITY PLAN OBJECTIVES**

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	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

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
administrator, service and user accounts	1.5 Implement staff augmentation or third party services to migrate existing websites to .gov addresses. This migration must include the primary government website (i.e. localityname.gov)	100% of targeted websites	Frequency: Monthly Source: Sites publicly available
	1.6.1 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.

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
	2.2.1 Implement third party services to install netflow monitoring at the egress of where a majority of server traffic is traversing or the location that has the most amount of network traffic and will support an approved configuration	At least 1 device deployed and reporting data Target coverage 90% of assets	Frequency: Completion of installation and quarterly review of data
	2.2.2 Implement third party services to deploy and/or manage firewall, IDS/IPS technology at an organizations egress with deep packet inspection, malware detection, application awareness, intrusion detection and intrusion prevention	Devices deployed Reports on threat activity available Target coverage 90%	Frequency: Completion of information and quarterly review of data
	2.3.1 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	Frequency: Monthly

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
		% of event log sources compliant with standards	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.
	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	3.4.1 Implement multifactor	Accounts implemented with multifactor	Source: Target accounts per system or in the environment

Cybersecurity Plan Sub-Objectives and Metrics

Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
compatible externally exposed systems, network access, and/or administrative access	authentication to systems 3.4.2 Implement multifactor authentication for Virginian identifies	Target: 100% Minimum: 90%	Frequency: Monthly
3.5 Domain Name System (DNS) Filtering/Firewall	3.5.1 Implement or have third party services implement and configure hosts to utilize approved DNS filtering services	Hosts leveraging DNS filtering / Total hosts in the environment Target: 100% Minimum: 90%	Sources: Number of devices in organization inventory Frequency: Monthly
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	3.9.1 Have a third party upgrade out of date systems	Hosts scanned within 30 days	Source: Vulnerability software and asset inventory

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
implemented and up to date	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 updated to supported software within n-1 of most recent release	Frequency: Monthly
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

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
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 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*	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)
5.2 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 SLTT 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

UPDATE ALL ACRONYMS IN TABLE

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 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