Virginia Cybersecurity Planning Committee

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
Cybersecurity Plan Development Report	
Goal 1: Inventory and Control of Technology Assets, Software and Data	Derek M. Kestner, Information Security Officer, Supreme Court of Virginia Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
Goal 2: Threat Monitoring	John Harrison, IT Director, Franklin County Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Goal 3: Threat Protection and Prevention	Wesley Williams, Executive Director of Technology, Roanoke City Public Schools Benjamin Shumaker, Cyber Security Specialist, King William County Government
Goal 4: Data Recovery and Continuity	Adrian Compton, Tribal Administrator, Monacan Indian Nation, Capt. Eric W. Gowin, Division Commander-Information Technology Division, Virginia State Police
Goal 5: Security Assessment	Major Charles DeKeyser, Virginia Army National Guard, Stephanie Williams-Hayes, Chief Information Security Officer, Virginia Department of Health
Discussion of Grant Prerequisites	Mike Watson
Public Comment Period	
Other Business	Staff
Adjourn	

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
January 13, 2023 – 9:00 am
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:

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

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

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

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

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

Members Participating Remotely:

Benjamin Shumaker, Cyber Security Specialist, King William County Government. Mr. Shumaker participated from his office in King William County because his physical presence was needed in the office for work.

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.

Staff Present:

Leslie Allen, Senior Assistant Attorney, Office of the Attorney General

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

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 November 7 meeting minutes were displayed on the screen. Upon a motion by Mr. Compton and duly seconded by Mr. Harrison, the committee unanimously voted to adopt the Electronic Participation Policy.

Advisors Update:

Mr. Watson provided an update on the advisors for the planning committee. Advisors will serve as technical experts and assist with seeking input and building consensus in the community during the process. Members will reach out to advisors for assistance with plan development later detailed in the meeting.

Status of the Grant:

Mr. Coates provided an overview of the status of the grant application. The grant was approved with funds to develop the cybersecurity plan for the first year. Most of the funding is on hold until the plan is fully developed and approved. Mr. Coates is reaching out to receive additional clarity on fund allocation.

Cybersecurity Plan Development:

Mr. Watson reviewed the Cybersecurity Plan Development. The draft plan objectives and goals included requirements from pgs 5-8 of the Notice of Funding Opportunity (NOFO). The objectives and goals follow the NIST framework and best practices.

There were discussions on emphasizing goals for protection and prevention of threats vs. recovery, patch management, communications plan for localities, how localities can maintain cybersecurity after grant completion, physical security, resources to implement end point security, free resources available to localities, and state SOC monitoring for localities. The committee members then chose objectives to work on, as reflected in the attached document.

Public Comment Period:

There were no public comments.

Other Business:

Mr. Watson opened the floor for other business. Ms. Ly discussed travel forms. Mr. Heslinga reminded the committee to CC the committee administrator email, cybercommittee@vita.virginia.gov, on all correspondence related to the business of the committee. He also discussed FOIA and the facilitation of meetings when there are 3 or more members. Mr. Dekeyser asked for a presentation on the locality application process at the appropriate time after the plan was completed. Mr. Coates discussed the process currently in use at VDEM for the evaluation and processing of applications which will be discussed after the submission of the plan.

Adjourn

Upon a motion by Mr. Dent and duly seconded by Deputy Secretary Andrews, the committee unanimously voted to adjourn the meeting at 11:30am.

Goal 1

Goal	Program Objectives	Target Metric	Implementation Feasibility	Support Model	Ability to Support	Supporting Technologies and/or Services
1. **Inventory and Control of Technology Assets, Software and Data**	1.1 Establish and maintain a detailed enterprise asset ~~and software~~ inventory ~~for 90%~~ of ~~owned~~ all technology assets (including hardware and software)	100%	Likely	Contract Implementation Services	Likely	Asset Management Software; SAAS Vendors; Staff augmentation to perform assessment
Members: Derek M. Kestner, Information Security Officer, Supreme Court of Virginia; Diane Carnohan, Chief Information Security Officer, Virginia Department of Education	1.2 Ensure ~~100%~~ ~~all~~ only authorized assets ~~that~~ connect to enterprise systems and are ~~authorized and~~ inventoried	100%	Likely	Contract Implementation Services	Likely	SAAS Vendors; Contractor staff augmentation to perform assessment
	1.3 Upgrade or ~~update~~ replace all software no longer receiving security maintenance/support	100%	Likely	Contract Implementation Services	Likely	Contractor to perform assessments and upgrade services
	1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business	100%	Likely	Contract Implementation Services	Likely	Contractor to perform assessment
	1.5 Identify all government websites and migrate non .gov ~~government~~ sites to .gov domains	100%	Likely	Contract Implementation Services	Likely	Contractor to perform migration
	1.6 Establish and maintain inventory of administrator, service ~~or~~ and user accounts	100%	Likely	Contract Implementation Services	Likely	Contractor to perform assessment

2. Threat Monitoring

Cybersecurity Planning Committee Members:

John Harrison	Franklin County	Director of Technology
Brenna Doherty	DLAS	CISO

Advisors & Contributors:

Rich Maidenbaum	Spotsylvania County	Deputy CIO
Charles Huntley	Essex County	Director of Technology
Lonnie Karnes	Spotsylvania County	CISO

NOTE:

- Sub-sections have been prioritized in order of criticality and relative impact.
- All "services" are available in three support tiers;

  Tier 1 = Localities that seek minimal assistance in implementation and support but require or would benefit from established contract vehicles with vetted suppliers/vendors.

  Tier 2 = Tier 1 plus assistance with implementation but not operational support.

  Tier 3 = Tiers 1 & 2 plus assistance with operational support and maintenance.

The following Tier "responses" apply to all program objectives:

Tier 1 – Contracts

Target Metric: TBD (should be usable by all)
Implementation Feasibility: Likely
Ability to Support: Likely

Tier 2 – Implementation Support

Target Metric: TBD (assuming this applies to most localities)
Implementation Feasibility: Likely
Ability to Support: Likely

Tier 3 – Full Support

Target Metric: TBD (assuming this applies to very small or non-IT staffed localities)
Implementation Feasibility: Likely
Ability to Support: Unsure

Threat Monitoring – Overall Prioritized Recommendations

1) Firewalls
    a. Next Gen Firewall (IDS, IPS, Application Awareness)
2) EDR
    a. End-Point Protection with Managed Threat Response
3) ALBERT
    a. IDS solution designed specifically for U.S. State, Local, Tribal, and Territorial (SLTT) government organizations. It is enhanced with support from CIS's 24x7x365 Security Operations Center (SOC).
4) SIEM
    a. Hosted or on-premise solution providing real-time analysis of security alerts by applications and network hardware. It includes systems like Log management, Security Log Management, Security Event correlation, Security Information management

NOTE: #2-4 are accomplished as part of or as necessary services in support of a managed SOC service. This group recommends that a managed SOC solution, able to accommodate multiple EDR platforms (e.g. vendor agnostic) be established by the state (potentially in partnership with and run by ISAC or C4-RAMPART) using the state's portion of the grant funds.

Threat Monitoring – Sub-Section Recommendations

2.2 Deploy network filtering and detection at network egress and ingress points

CIS CONTROLS = 3.3, 9.2, 9.3, 10.0, 12.2, 12.3, 12.5, 12.7, 13.3, 13.5, 13.6, 13.8, 13.10

Supporting Technologies and/or Services:

1. Next Generation Firewalls (Deep packet inspection, malware detection, application awareness, intrusion detection and prevention)
2. CISA Albert Sensor
3. Data Classification and Data Loss Prevention

Magic Quadrant: Firewalls

2.1 Deploy host intrusion detection/prevention for all workstations and servers /2.5 Deploy endpoint detection and response

CIS CONTROLS = 2.3 – 2.6, 4.4, 4.5, 7.5, 7.7, 9.1, 9.6, 9.7, 10.1 – 10.7, 13.2, 13.5, 13.7, 13.10

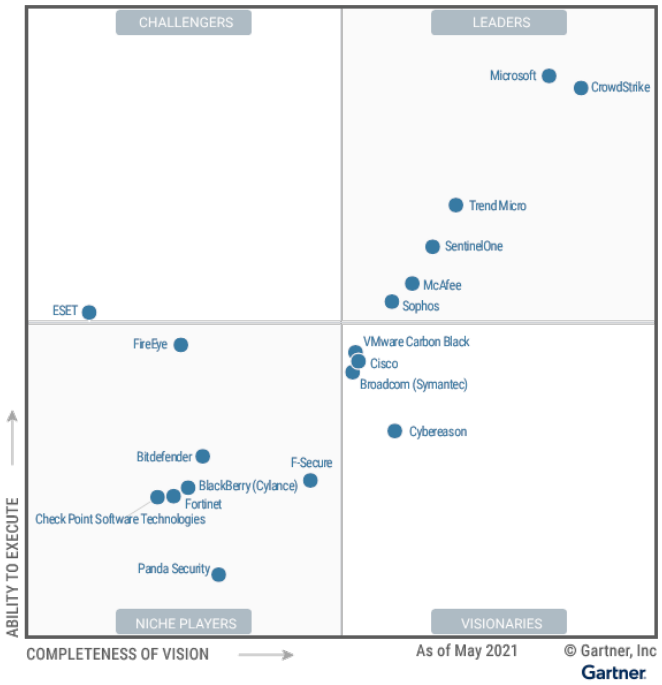
Supporting Technologies and/or Services:

1. Client-based Endpoint Protection with Endpoint Detection & Response (EDR)

   1b. Managed Threat Response (MTR)

   1c. Extended Detection & Response (XDR)

Magic Quadrant: Endpoint Protection



2.4 Collect network traffic flow logs

CIS CONTROLS = 8.1 – 8.3, 8.5 – 8.7, 8.11, 13.1, 13.6, 13.11

Supporting Technologies and/or Services:

1. Security Information and Event Management-SIEM (On-Premises or Cloud based)
2. NetFlow Analyzer Software

Magic Quadrant: SIEM

2.6 Audit log collection for all servers and systems hosting data in accordance with federal enterprise log management standards

CIS CONTROLS = 1.4, 3.14, 8.1 – 8.12, 13.6,

Supporting Technologies and/or Services:

1. Security Information and Event Management-SIEM (On-Premises or Cloud based)
2. Log Analyzer
3. SysLog Server

2.3 Centralize security event alerting

CIS CONTROLS = 8.9, 10.6, 13.1

Supporting Technologies and/or Services:

1. Security Information and Event Management-SIEM (On-Premises or Cloud based)
2. Hosted SOC Service (C4, ISAC, ad infinitum)
3. Regional Security Operations Center-SOC (C4, ad infinitum)
4. State SOC

2.7 Web application firewall

CIS CONTROLS = 9.2 – 9.4, 9.6, 9.7, 13.10

Supporting Technologies and/or Services:

1. Client-based Endpoint Protection with Web Filtering Included
2. DNS/Proxy Filter
3. Web Security and Filtering Service/Product

Goal 3

Goal	Program Objectives	Target Metric	Implementation Feasibility	Support Model	Ability to Support	Supporting Technologies and/or Services
3. **Threat Protection and Prevention**	3.1 Implement and manage firewalls on all end point devices (i.e. user workstations, servers)	90% target rate / Request reporting	Easy/Likely	Contract or Implementation services / Full Service	Unsure (Depends on resources at locality) Long-term sustainability dependent on staffing and training. Minimal resources needed to maintain.	• SonicWall • Sophos • Cisco • Bit Defender • Norton • Qualys • Barracuda • Palo Alto • Intune Central management
Members: Wesley Williams, Executive Director of Technology, Roanoke City Public Schools, Benjamin Shumaker, Cyber Security Specialist, King William County Government	3.2 Implement and manage network firewalls for ingress and egress points	Reporting	Medium / Uncertain	Contract or Implementation services / Full Service	Unsure (Depends on IT size and expertise) Long-term sustainability dependant on internal/external expertise. Minimal staff required to maintain.	• Fortinet • SonicWall • Cisco • Palo Alto • F5 Technologies BIG IP
	3.3 Encrypt sensitive data in transit and on devices hosting sensitive data	Created Procedure/Policy | Reporting if centrally managed	Hard / Not likely	Contract / Implementation services/ Full Service	Not likely / Unsure (varies by locality) Long-term sustainability likely if implementation is strong and has associated procedures.	• Office365 encryption • Bit Locker • Code42 • Proofpoint • Digital • Guardian • Zscaler

Goal 3

Goal	Program Objectives	Target Metric	Implementation Feasibility	Support Model	Ability to Support	Supporting Technologies and/or Services
	3.4 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access	100% (90%) / reporting	Medium / uncertain	Implementation services / Full Service	Likely / uncertain Long-term sustainability likely with appropriate procedures. Minimal staffing required to maintain.	• Microsoft Authenticator • Duo Security • Google Authenticator
	3.5 Domain Name System (DNS) Filtering/Firewall	Yes/No | Weekly Reporting on threats, what is getting blocked, queries	Easy / very likely	Contract / Implementation services (minimal)/ Full Service	Likely Minimum documentation and staffing needed for long-term sustainability.	• Contact your ISP • GoDaddy • Palo Alto • MS-ISAC Sec • Neustar
	3.6 Email filtering and protection	Yes/No | Reporting	Easy / Likely	Contract or Implementation services	Likely Long-term sustainability requires expertise and training. Maintaining would require minimal staffing hours.	• Barracuda • FortiMail • SolarWinds • SecureWorks • Office365 • Qualys (Smtp)
	3.7 Centralized authentication and authorization (Single Sign On)	Yes/No | Report | Interfaces with all systems	Not likely	Contract / Implementation services/ Full Service	Unsure Long-term sustainability dependent on	• CyberArk • ForgeRock • Microsoft Azure AD

Goal 3

Goal	Program Objectives	Target Metric	Implementation Feasibility	Support Model	Ability to Support	Supporting Technologies and/or Services
					internal/external expertise	
	3.8 Content and malicious traffic filtering through anti-virus and threat detection software	Do you have next-gen antivirus installed? Yes/No |Reporting Tools	Easy	Contract or Implementation services	Likely Requires minimal interaction if configured properly. Long-term sustainability applicable with appropriate training or external support	• Sophos • CrowdStrike • SentinelOne • Qualys • DarkTrace • ConnectWise • LightSpeedSystems • Barracuda
	3.9 Ensure patch management program is implemented ~~software is patched~~ and up to date	Do you have documentation detailing your program? Yes/No | Procedures, Reports, Success of patch jobs, Number of devices patched	Medium / Likely depending on staffing	Contract / Implementation services/ Full Service	Not Likely / Uncertain Long-term sustainability requires training internally. Requires staffing and patch management expertise. Change management will be an on-going challenge.	• Avira • Avast • ManageEngine • Qualys • Tenable • Nessus

Goal 4

Cyber Planning Committee Objectives

Adrian Compton, Tribal Administrator, Monacan Indian Nation,

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

4.1 Establish and maintain a data recovery process

Target Metric: Develop a current inventory of critical systems based on business impact analysis.

Develop a business continuity plan or disaster recovery plan that enables the recovery of critical information systems that support business processes for all cloud based and locally stored data.

Implementation Feasibility: Likely for cloud-based solutions, for locally stored data more uncertain.

Support Model: Support model will depend greatly on the size of the entity consuming the service. Smaller entities may require full support while larger agencies with more robust technology sets may only require contractual support.

Cost of cloud-based solutions, local solutions add additional risk but can be obtained for less cost.

Ability to Support: Likely, with consideration of ongoing recurring cost for smaller entities. Cost for contractual services and hardware and software (annual recurring cost).

Supporting Technologies and Features: Contractual services provided by various vendors to conduct initial assessments and development of plans.

Cost reducing bulk software purchases.

Federal and State resources which include templates and guidance for plan production.

4.2 Establish and maintain an isolated/vaulted instance of recovery data

Target Metric: Business identifies and maintains inventory of critical data within DR or business continuity plan.

Data is stored in separate site geographically located away from primary site., this would include cloud environments.

Backup data is encrypted at rest and in transit.

Implementation Model: Likely, Cost of cloud-based solutions, local solutions add additional risk but can be obtained for less cost. Consideration surrounding using hardware backups as compared to cloud-

based solutions which would require additional implementation on behalf of the entity and additional security concerns.

Support Model: Contract/ Implementation/ Full Service, with consideration of ongoing recurring cost for smaller entities. Cost for contractual services and hardware and software (annual recurring cost).

Ability to Support: Likely, with consideration of ongoing recurring cost for smaller entities. Cost for contractual services and hardware and software (annual recurring cost).

Supporting Technologies and features: Cloud Solutions, outsourced managed facilities. Mirrored sites and electronic vaults provided by vendors. Additional options remain such as internal hard drives, removable storage, tape drives, and other locally managed software/hardware.

4.3 Implement disaster recovery and data recovery testing

Target Metric: Initial testing of the originally implemented DR or BCP to ensure functionality of accompanying hardware, software, and plans.

Continuous regularly scheduled testing to ensure relevancy of plan and operational effectiveness.

Implementation Model: Likely, for the majority, again resources need to be identified for entities that have limited resources.

Support Model: Contract/ Implementation/ Full Service, with consideration of ongoing recurring cost for smaller entities. Cost for contractual services and hardware and software (annual recurring cost).

Ability to Support: Likely with continued funding based on the nature of the solution. Hardware solutions could bring additional probability of support. Software solution will be easier to support and test.

Supporting Technologies and features: contractual services which conduct testing (depending on complexity)

4.4 Implement technology to support continuity of services in the case of a natural disaster or cyber attack

Target Metric: Software which supports the notification of critical staff, (everbridge systems).

Software and available hardware implemented which enables remote work and offsite locations.

Implementation of fully developed and redundant hardware and software with telecommunications telephone and utility connectivity.

Goal 4

Intruder detection/monitoring software and features (preemptive measures) in place.

Implementation Model: Likely, for the majority, again resources need to be identified for entities that have limited resources.

Support Model: Contract/ Implementation/ Full Service, with consideration of ongoing recurring cost for smaller entities. Cost for contractual services and hardware and software (annual recurring cost).

Ability to Support: Likely with continued funding based on the nature of the solution. Hardware solutions could bring additional probability of support. Software solution will be easier to support and test.

Supporting Technologies and features: Cloud based data backups, redundant connectivity (difficult for localities and tribal partners due to limited broadband accessibility).

Redundant physical locations.

Affordability ongoing services.

Cybersecurity Planning Committee – 03122023

Step #1

Goal: Perform an on-site and remote cybersecurity review.

Objective: Conduct a self-assessment or third-party assessment of the cybersecurity practices for the purpose of identifying cybersecurity gaps (i.e., the absence of recommended cybersecurity practices or controls or presence of vulnerabilities).

Option 1: Self-Assessment:

The organization could conduct the assessment using a government or private-sector method approved by the Cybersecurity Planning Committee, such as those from an approved Commonwealth of Virginia (COV) vendor, Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), or International Organization for Standardization ISO).

Option 2: Third-Party Assessment.

The organization could hire a third-party vendor to perform an assessment using the Commonwealth of Virginia (COV) Security Standards or National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Outcome:

The self-assessment or third-party assessment should be performed/completed within the 90-120 days of contract award.

Step #2

Risk Mitigation.

Goal: Identify significant cybersecurity deficiencies, such as defects in design, operations, absence of a practice or control, or presence of a vulnerability, that has a critical or high risk of being exploited, either directly or indirectly, to compromise an operational technology or could potentially compromise the continuity of business operations.

Objective: The organization should provide a risk mitigation plan to address cybersecurity gaps identified during the assessment, specifically including any significant deficiencies designated by the Cybersecurity Planning Committee.

A. Submit a risk mitigation plan that would list planned mitigation actions and schedules. (Note: We should offer a template that describes the planned mitigation, target completion dates, responsible party, status, and explanatory notes. We may need a resource designated for technical assistance.)
B. Identify any additional resources that could be used to address these cybersecurity gaps.
C. The Committee will review the risk mitigation plan.

D. The organization will provide quarterly updates on risk mitigation progress.

E. Outcomes:

1. The self-assessment or third-party assessment should be completed within the 120-180 days of contract award.
2. The risk mitigation plan, which describes the planned mitigation, target completion dates, responsible party, status, and explanatory notes, should be submitted for review in 60-90 days after the initial assessment.

Goal: Assess cybersecurity workforce, identify critical gaps in the cybersecurity staffing, and improve positions descriptions in recruitment.

Objective: Use the National Initiative for which categorizes and describe cybersecurity work.

Option 1: Skills Assessment.

1. The organization could hire a third-party vendor to perform a skills assessment of the cybersecurity workforce using the NICE Cybersecurity Workforce Framework including surveys, interviews, reviewing job descriptions, performance reviews, and performing skills assessment tools.
2. The organization should provide the report to include areas of evaluation such as task, knowledge, skill, and competence area for each cybersecurity role within the organization. This individual should be employees of the organization, not vendor or contractors.
3. The organization should identify existing contractors or vendor and their cybersecurity support role or services to the organization for addressing skills gaps. The service level agreement/contract should be included/referenced.
4. The organization should identify any critical staff that should assist in support cybersecurity toles.
5. The organization should submit a risk mitigation plan that would list planned mitigation actions and schedules. (Note: We should offer a template that describes the planned mitigation, target completion dates, responsible party, status, and explanatory notes. We may need a resource designated for technical assistance.)

F. Outcomes:

3. The third-party skills assessment should be completed within the 120-180 days of contract award.
4. The risk mitigation plan, which describes the planned mitigation, target completion dates, responsible party, status, and explanatory notes, should be submitted for review in 60-90 days after the initial assessment.
5. Provide a training and development plan to aid the cybersecurity team in performing job roles in the role/position/title.

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