VIRGINIA CYBERSECURITY PLAN

2022

VIRGINIA CYBERSECURITY PLANNING COMMITTEE
VERSION 1.1

vita.virginia.gov

JULY 31, 2023

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LETTER FROM VIRGINIA CYBERSECURITY PLANNING COMMITTEE

Greetings,

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

The VCPC includes representation from the following constituencies: eligible entity, state emergency management, public education, public health, homeland security, high-population jurisdiction, suburban jurisdiction, rural jurisdiction, rural jurisdiction, tribal, national guard, legislature, public safety, judicial, and private sector. In addition to the listed members and the areas they represent, additional stakeholders were consulted as advisors to formulate a robust and realistic cybersecurity plan.

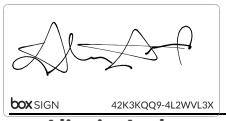
VCPC collaborated to develop the Cybersecurity Plan with actionable and measurable goals and objectives that have champions identified to ensure completion. These goals and objectives focus on: inventory and control of technology assets, software and data, threat monitoring, threat protection and prevention,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

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

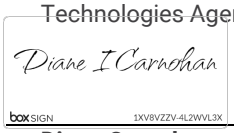
Sincerely,

Michael Watson, Chair
Chief Information Security Officer of the Commonwealth
Virginia Information Technologies Agency

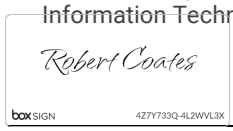
Michael Dent, Vice Chair
Chief Information Security Officer
Fairfax County Department of Information Technology



Aliscia Andrews
Deputy Secretary of Homeland Security
Office of the Governor



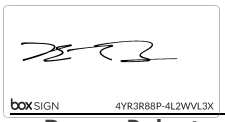
Diane Carnohan
Chief Information Security Officer
Virginia Department of Education



Robbie Coates
Director, Grant Management and Recovery
Virginia Department of Emergency Management

Adrian Compton
Tribal Administrator
Monacan Indian Nation

Charles DeKeyser
Major
Virginia Army National Guard



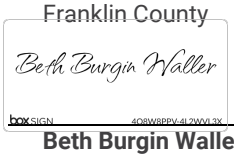
Brenna Doherty
Chief Information Security Officer
Department of Legislative Automated Systems

Eric Gowin
Major
Virginia State Police

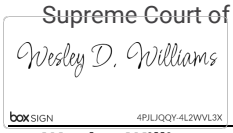
John Harrison
IT Director
Franklin County

Derek Kestner
Information Security Officer
Supreme Court of Virginia

Benjamin Shumaker
Cybersecurity Specialist
Rural Locality Representative



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



Wesley Williams
Executive Director of Technology
Roanoke City Public Schools

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

INTRODUCTION

The Cybersecurity Plan (Project Number 3) is a three-year strategic planning document that contains the following components:

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

VISION AND MISSION

This section describes the VCPC's vision and mission for improving cybersecurity:

Vision:

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

Mission:

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

Cybersecurity Program Goals and Objectives

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

Cybersecurity Program	
Program Goal	**Program Objectives**
1. Inventory and Control of Technology Assets, Software and Data	1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software)
	1.2 Ensure only authorized assets connect to enterprise systems and are inventoried
	1.3 Upgrade or replace all software no longer receiving security maintenance/support
	1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business
	1.5 Identify all government websites and migrate non .gov sites to .gov domains
	1.6 Establish and maintain inventory of administrator, service, and user accounts
2. Threat Monitoring	2.1 Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers
	2.2 Deploy network monitoring, filtering and detection at network egress and ingress points
	2.3 Centralize security event alerting
	2.4 Collect network traffic flow logs
	2.5 Audit log collection for all servers and systems hosting data in accordance with log management standards
	2.6 Web application firewall

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

CYBERSECURITY PLAN ELEMENTS

MANAGE, MONITOR, AND TRACK

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

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

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

MONITOR, AUDIT, AND TRACK

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

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

ENHANCE PREPAREDNESS

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

- Develop a comprehensive cybersecurity incident response plan which incorporates the security representatives and, if applicable, the security operations team or equivalent. In circumstances of organizations with limited security resources these should be testing processes between partners who would be most likely to make the organization aware of

a cyber security incident (*i.e.*, VA-ISAC, Multi State ISAC, law enforcement, etc.) and the organizations used to respond to an incident (i.e., cyber insurance designated services, third party contractors, in house incident response staff, etc.)

- Establish and train the security investigation and incident response team with the duties their responsible for performing when responding to malicious activity. The training of these teams should include the roles responsible for making decisions about when to engage resources as well as how to interface with Virginians about the impact of a security issue.
- Perform penetration testing or red teaming to test an organization's incident response plans. These tests should be looking to both identify weaknesses in the technology controls implemented and the processes involved in response and detection.

ASSESSMENT AND MITIGATION

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

- Conduct regular vulnerability assessments to identify potential weakness and vulnerabilities in information systems, applications, and user accounts. The use of approved automated scanning tools and assessment technology should be executed on internal and/or public facing systems and applications to understand the risk and vulnerabilities an organization is subject to.
- Deploy approved endpoint protection tools to ensure detection and prevention of malicious activity. The implementation must integrate with identified threat and security sharing services.
- Deploy tools which allow for both containment of malicious activity within the organization's environment and prevention of access to the environment.
- Provide a policy and process for mitigating vulnerabilities and issues identified within the organization.
- Conduct thorough assessments and implement robust mitigation measures to safeguard critical infrastructure against cybersecurity risks and threats that could disrupt Commonwealth information systems.

BEST PRACTICES AND METHODOLOGIES

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

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

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

SAFE ONLINE SERVICES

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

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

CONTINUITY OF OPERATIONS AND COMMUNICATIONS

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

- Implement backup and restoration validations processes and procedures to ensure adequate data recovery.
- Establish a secure offline separate backup location (i.e., vaulted backup) to protect against cyber disruptions such as ransomware.

- Implement technology allowing for continuity of services in the case of a disaster scenario.
- Identify network continuity requirements and technology in the case of an outage due to disaster or cyberattack.
- Leverage the Commonwealth Emergency Operations Plan (cyber annex) as appropriate.
- Prioritize the maintenance of uninterrupted communication.

WORKFORCE

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

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

CYBER THREAT INDICATOR INFORMATION SHARING (PROJECT NUMBER 2 IN THE WORKPLAN)

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

- The VA-ISAC will provide a shared SOC available for use by state, local, and tribal entities.
- Subrecipients must ensure they register, receive and stay updated on critical cybersecurity information and alerts provided by VA-ISAC.
- Subrecipients who receive grant funding are strongly encouraged sign up as a member of the VA-ISAC, MS-ISAC and EI-ISAC.
- The VA-ISAC will facilitate sharing for CISA's Cyber Information Sharing and Collaboration Program (CISCP) and MS-ISACs indicator feeds.
- The VA-ISAC will not displace and will work in partnership and cooperation with existing state entities and stakeholders, including the Virginia State Police, Department of Emergency Management, and Virginia National Guard. Legal authorities will be supplemented to the extent needed, and interagency agreements and documentation will be developed, to support the VA-ISAC and define roles and responsibilities.

Department Agreements

All entities receiving funds from the grant program must ensure they share their threat indicators and corresponding information from the tools implemented in the environment with the VA-ISAC to aid in measuring performance. The application for the grant program will include an MOU indicating the applicant's agreement to share data and specifying the nature of the data to be shared.

LEVERAGE CISA SERVICES

Subrecipients are required to obtain services supporting objectives in this plan using approved contracts and service providers. CISA services meeting the objectives are considered an approved service provider. Several of the program objectives include support for implementing CISA services. Applicants are strongly encouraged to enroll in CISA Cyber Hygiene Services including Web Application Scanning and Vulnerability Scanning.

INFORMATION TECHNOLOGY AND OPERATIONAL TECHNOLOGY MODERNIZATION REVIEW

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

CYBERSECURITY RISK AND THREAT STRATEGIES

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

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

RURAL COMMUNITIES

In order to help rural communities, get the most out of this program, the plan has a structured

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

FUNDING & SERVICES

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

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

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

DISTRIBUTION TO LOCAL GOVERNMENTS

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

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

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

- Contract Only – A pre-approved authorized/legal procurement vehicle. The organization is responsible for all aspects of the implementation other than establishing the contract.
- Implementation Services – Services needed to stand up the technology or processes of the initiative. Once these services are done the organization becomes responsible for running/managing the implementation.
- Full Service – The organization would like support to build, implement and run the program objective technology or processes. These services require the least amount of support from the organization.

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

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

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

ASSESS CAPABILITIES (PROJECT NUMBER 3 IN THE WORKPLAN)

A capabilities assessment process will be used to identify and evaluate threats and vulnerabilities faced by state, local, and tribal entities. This assessment will encompass a thorough examination in accordance with the State and Local Cybersecurity Improvement Act.

IMPLEMENTATION PLAN

ORGANIZATION, ROLES, AND RESPONSIBILITIES

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

In order to facilitate a centralized connection point between organizations for cybersecurity

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

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

RESOURCE OVERVIEW AND TIMELINE SUMMARY

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

METRICS

Cybersecurity Plan Sub-Objectives and Metrics			
Program Objectives	**Program Sub-Objectives**	**Associated Metrics**	**Metric Description** (details, source, frequency)
1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software) 1.2 Ensure only authorized assets connected to enterprise systems and are inventoried. 1.3 Upgrade or replace all software no longer receiving security maintenance/support. 1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business.	1.1 Implement staff augmentation or third-party services to assess technology inventory	100% of devices and software recorded in inventory – (Total devices and/or software identified) / (Submitter provided initial estimate)	Frequency: Monthly Source: Submitter provided initial estimate NOTE: documentation updating the estimate may be provided at the measurement frequency
	1.2 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

1.5 Identify all government websites and migrate non .gov sites to .gov domains. 1.6 Establish and maintain inventory of administrator, service, and user accounts	1.4 Implement staff augmentation or third-party services to assess and inventory data according to inventory requirements	100% of targeted and/or identified data sets inventoried. NOTE: If target unknown begin with estimate	Frequency: Monthly Source: Submitter provided initial estimate or target number NOTE: documentation updating the estimate may be provided at the measurement frequency
	1.5 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	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	Total number of hosts running the software out of	Frequency: Monthly

management standards. 2.5 Web application firewall	the preapproved host-based threat protection software deployment	the established target Threat information collected from deployment	Source: Asset Inventory and software deployment totals. Threat data from threat protection software.
	2.2.1 Implement third party services to install netflow monitoring at the egress of where a majority of server traffic 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 % of event log sources compliant with standards	Frequency: Monthly Source: Asset inventory and log collection system

	2.5.1 Purchase and/or license preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.
	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.
3.3 Encrypt sensitive data in transit and on devices hosting sensitive data	3.3.1 Obtain certificates to support encrypted transmissions	Number of public-facing hosted systems with approved encryption	Frequency: Monthly Sources: Websites with approved encryption
	3.3.2 Implement and/or manage zero trust network access connectivity (ZTNA VPN)	Number of non-public facing systems potentially accessible	Frequency: Quarterly Sources: Number of devices remotely accessible using multifactor login
3.4 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access	3.4.1 Implement multifactor authentication to systems. 3.4.2 Implement multifactor authentication for Virginian identities	Accounts implemented with multifactor. Target: 100% Minimum: 90%	Source: Target accounts per system or in the environment Frequency: Monthly
3.5 Domain Name System (DNS) Filtering/Firewall	3.5.1 Implement or have third party services implement and configure hosts to 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	Filters covering email users.	Sources: Number of emails in the directory

	filtering for incoming email services	Target: 100% Minimum 95%	and number of emails protected by the filter Frequency: Monthly
3.7 Centralized authentication and authorization (Single Sign On)	3.7.1 Obtain licenses for single sign on software. 3.7.2 Implement or have third party services implement single sign on 3.7.3 Manage or have a third party manage single sign on solutions	Number of organization users with single sign on Number of Virginians with single sign on	Sources: User access list Frequency: Monthly
3.8 Content and malicious traffic filtering through anti-virus and threat detection software	3.8.1 Obtain licenses for content/malicious traffic filtering 3.8.2 Implement or have third party services implement content/malicious traffic filtering 3.8.3 Maintain or have a third party maintain content/malicious traffic	Number of hosts with filtering and detection	Sources: asset inventory and protected system list Frequency: Monthly
3.9 Ensure patch management program is implemented and up to date	3.9.1 Have a third-party upgrade out of date systems 3.9.2 Obtain licenses for vulnerability management software 3.9.3 Implement or have a third party implement vulnerability management program and/or software 3.9.4 Maintain or have a third party maintain a vulnerability management program	Hosts scanned within 30 days Hosts updated to supported software within n-1 of most recent release	Source: Vulnerability software and asset inventory Frequency: Monthly
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	100% of Critical services will be brought online within 72 hours	Source: Asset inventory Frequency: Once

	all cloud based and locally stored data.		
4.2 Establish and maintain an isolated/vaulted instance of recovery data	4.2.1 Obtain licenses for a vaulted data recovery solutions 4.2.2 Implement or have a third party implement a vaulted data recovery solution for critical backups 4.2.3 Have a third party maintain a vaulted data recovery solution	90% of critical data vaulted	Frequency: Source Source: Total GB of data vaulted out of total GB of critical data
4.3 Implement disaster recovery and data recovery testing	4.3.1 Have a third party test the disaster recovery and/or business continuity plan	Successful recovery within plan established time frame	Frequency: Once Source: Disaster recovery plan information
4.4 Implement technology to support continuity of services in the case of a natural disaster or cyber attack	4.4.1 Obtain or have a third party provide services to maintain communications in the case of a regional disaster within 500 miles	Successful test of continuity services	Frequency: Semi-Annually Source: Recovery plan and certification of completion
5.1 Identify security gaps associated with program objectives which can be supported by the grant program	5.1.1 Have staff augmentation provide an assessment or have a third-party assessment of the technology environment for services supported by the grant program 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	Assessment completion within 120 days Mitigation plans can begin within 30 days Training to begin within 90 days of award	Frequency: Quarterly

	5.1.4 Obtain security training used to train or educate personnel for careers in cybersecurity *5.1.5 Obtain security awareness training for end users*		
5.2 Perform automated vulnerability scans	5.2.1 Obtain third-party services to provide a vulnerability scan and assessment of the environment	Obtain a vulnerability review report within 90 days Mitigations to be done with a target of 30 days of report	Source: Vulnerability assessment Frequency: Monthly
5.3 Network and system architecture diagram and assessment	5.3.1 Obtain software to provide a network map of the environment 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

Metrics must also include the provided the approved policy or policies supporting the lifecycle and upkeep of the objectives applied for should be included.

Metric completion also requires successful completion of data sharing agreements (if applicable) and singing up for specified threat sharing organizations.

APPENDIX A: SAMPLE CYBERSECURITY PLAN CAPABILITIES ASSESSMENT

To be completed in Project 3

COMPLETED BY Virginia Cybersecurity Planning Committee				**FOR ASSESSOR**
Cybersecurity Plan Required Elements	**Brief Description of Current Capabilities of State, Local, and Tribal entities within the Eligible Entity**	**Select capability level from:** Foundational Fundamental Intermediary Advanced	**Project # (s)** *(If applicable – as provided in Appendix B)*	**Met**
1. Manage, monitor, and track information systems, applications, and user accounts	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
2. Monitor, audit, and track network traffic and activity	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
3. Enhance the preparation, response, and resiliency of information systems, applications, and user accounts	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
4. Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
5. Adopt and use best practices and methodologies to enhance cybersecurity (references NIST)	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
a. Implement multi-factor authentication	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		

b. Implement enhanced logging	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
c. Data encryption for data at rest and in transit	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
d. End use of unsupported/end of life software and hardware that are accessible from the Internet	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
e. Prohibit use of known/fixed/default passwords and credentials	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
f. Ensure the ability to reconstitute systems (backups)	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
g. Migration to the .gov internet domain	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
6. Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
7. Ensure continuity of operations including by conducting exercises	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
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)	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
9. Ensure continuity of communications and data networks in the event of an incident involving communications or data networks	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		

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	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
11. Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
12. Leverage cybersecurity services offered by the Department	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
13. Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
14. Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
15. Ensure rural communities have adequate access to, and participation in plan activities	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		
16. Distribute funds, items, services, capabilities, or activities to local governments	The current capabilities are not comprehensive, and there is disparity in capability levels across state, local and tribal entities.	Foundational		

APPENDIX B: PROJECT SUMMARY WORKSHEET

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**.

1.	2. Project Name	3. Project Description	4. Related Required Element #	5. Cost	6. Status	7. Priority	8. Project Type
1.	Management and Administration (M&A)	Funding to provide for the administration, oversight, compliance of the grant award.	Management and Administration (M&A)	214,571	Ongoing		
2.	Cyber Threat Indicator Information Sharing Virginia information Sharing and Analysis Center	Establishing a Virginia information Sharing and Analysis Center (VA-ISAC)		300,403	Future		
3.	Cybersecurity Plan and Assessments	Establish the Virginia Cybersecurity Plan and complete cybersecurity plan capabilities assessment		128,740	Ongoing		

APPENDIX C: ACRONYMS

Acronym	Definition
Commonwealth of Virginia (COV)	A state in the Mid-Atlantic and Southeastern regions of the United States between the Atlantic Coast.
Cyber Information Sharing and Collaboration Program (CISCP)	Information sharing and collaboration with our critical infrastructure partners
Cybersecurity and Infrastructure Security Agency (CISA)	An agency of the United States Department of Homeland Security (DHS) that is responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers.
Domain Name System (DNS)	A system used to translate domain names into their corresponding IP addresses, allowing computers to locate and connect to each other.
Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC)	Operated by Center for Internet Security (CIS), a community of election officials and cybersecurity professionals working side-by-side to ensure the integrity of elections among U.S. State, Local, Tribal, and Territorial (SLTT) governments
Multi-State Information Sharing and Analysis Center (MS-ISAC)	Operated by Center for Internet Security (CIS), serves as a resource for state, local, tribal, and territorial government to enhance their cybersecurity capabilities, share threat intelligence, and collaborate on cybersecurity-related issues.
National Initiative for Cybersecurity Education (NICE)	Effort focused on enhancing the overall cybersecurity posture of the nation through education, training, and workforce development initiatives.
National Institute of Standards and Technology (NIST)	Agency under the Department of Commerce, dedicated to advancing measurement science, standards, and technology to enhance technological competitiveness.
Platform as a service (PaaS)	A capability to deploy user-created or acquired applications onto cloud infrastructure.
Security Operations Center (SOC)	A centralized unit within an organization that monitors and defends against security threats, such as cyberattacks and data breaches.
Software as a service (SaaS)	A capability to use software applications running on a cloud infrastructure and accessible from various client devices.
State and Local Cybersecurity Grant Program (SLCGP)	A grant program that provides funding to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of SLTT governments.
Virginia Cybersecurity Planning Committee (VCPC)	The committee established by Virginia law to be responsible for the State and Local Cybersecurity Grant Program (SLCGP), including crafting the cybersecurity plan for Virginia. Members are appointed by the Governor of Virginia.
Virginia Department of Emergency Management (VDEM)	An agency of the Commonwealth of Virginia and Virginia's State Administrative Agency (SAA) for FEMA purposes, including the SLCGP.
Virginia Information Technologies Agency (VITA)	An agency of the Commonwealth of Virginia and the executive branch's central information technology agency.