VIRGINIA IT AGENCY

Information Technology Advisory Council (ITAC)
May 23, 2023 – 10 a.m.
The Boulders, Mary Jackson Conference Room

Agenda

Call to Order and Welcome	John Craft, Chair
Rollcall	Staff
Review of Agenda	Staff
Approval of Minutes	Staff

<u>Presentations</u>

Commonwealth of Virginia Technology Strategy	Steve Nichols, Gartner Bob Osmond, Commonwealth CIO
Break	
VITA's Zero Trust Strategy and Roadmap	Rob Hankinson, Cybersecurity Architect, Deloitte & Touche LLP
Website Modernization	Bob Amani, Program Lead & Advisor, VITA
Public Comment Period	
Other Business	
Adjourn	

VIRGINIA IT AGENCY

Information Technology Advisory Council (ITAC)
December 8, 2022 – 1 p.m.
The Boulders, Mary Jackson Conference Room

Call to Order and Welcome

The Information Technology Advisory Council meeting was called to order at 1:02 p.m. Mr. Bob Osmond, CIO of the Commonwealth welcomed all the members.

Administering/coordinating (in the absence of a Chair and Vice-Chair):

Joshua Heslinga, Director, Legal and Legislative Services, Virginia IT Agency.

Members Present:

Bob Osmond, CIO of the Commonwealth

Lyn McDermid, Secretary of Administration

John A. Craft

Goutam Gandhi

Anthony T. Gitalado

Cherif Kane

James S. Kraemer

Constantina Kozanas

Adam S. Lee

Dr. Timothy M. Tillman

Virtual Members:

George "Bryan" Slater, Secretary of Labor

Senator Bill DeSteph of Virginia Beach

Senator Jennifer B. Boysko of Northwestern Fairfax

Senator John J. Bell of Loudoun

Members Not Present:

Phea Ram

Robert I. Turner

Staff Present:

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

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

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

Mike Watson, 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.

ITAC Legislation Overview

Mr. Heslinga provided an overview of the ITAC Legislation reviewing new legislation, composition of members and its role as an advisory body.

Overview of Roberts Rules of Order

Ms. Ly provided an overview of Roberts Rules of Order.

Electronic Participation Policy

Ms. Ly provided an overview of the Electronic Participation Policy. Upon a motion by Mr. Gandhi and duly seconded by Mr. Craft, the committee unanimously voted to adopt the Electronic Participation Policy.

Welcome Electronic Members

Upon adoption of the Electronic Participation Policy, ITAC welcomed its virtual members.

Charter and Bylaws

Mr. Heslinga provided an overview of the Charter and Bylaws. Upon a motion by Mr. Kraemer and duly seconded by Mr. Lee, the committee unanimously voted to adopt the Charter and Bylaws.

Nominations and Voting for Chair and Vice-Chair

Mr. Heslinga reviewed eligibility for Chair. The Secretary and CIO cannot be Chair of the council. The floor was opened for self-nominations. Mr. Craft and Dr. Tillman self-nominated for the position of chair. Mr. Gandhi and Ms. Kozanas self-nominated for the position of Vice-Chair. The nominees for Chair provided brief overviews of their

background. By a show of hands Mr. Craft received nine (9) votes, a majority of the votes for Chair. Mr. Gandhi and Ms. Kozanas provided a short speech on their background. By a show of hands Ms. Kozanas received ten (10) votes, a majority of votes for Vice-Chair.

Break

Cybersecurity in the Commonwealth

Mr. Watson presented on Cybersecurity in the Commonwealth which covered the scope of VITA cybersecurity responsibilities, threat landscape, cybersecurity priorities, incident reporting and the state and local cybersecurity grant program. There were discussions on VITA's role with local government, MS-ISAC, cybersecurity insurance coverage and work being done to help teachers access student data.

Information Technology Modernization

Secretary McDermid and Mr. Osmond presented on IT Modernization which covered the executive branch scope of service, Commonwealth strategic initiatives, Commonwealth IT Investment Management, assessments, and initiatives.

Public Comment Period

There were no public comments.

2023 Meeting Dates

Proposed 2023 meeting dates were presented to the members. Three meetings are planned, in May, September, and December. Members will be polled to confirm the May meeting date.

Other Business

Mr. Heslinga reminded the council to copy the ITAC email (itac@vita.virginia.gov) when corresponding related to ITAC business and invited feedback for the next meeting. Ms. Ly covered travel forms for the council members. There was a discussion on how the council could best support the administration.

Adjourn

Upon a motion by Mr. Craft and duly seconded by Mr. Kraemer, the meeting was adjourned at 2:58 p.m.
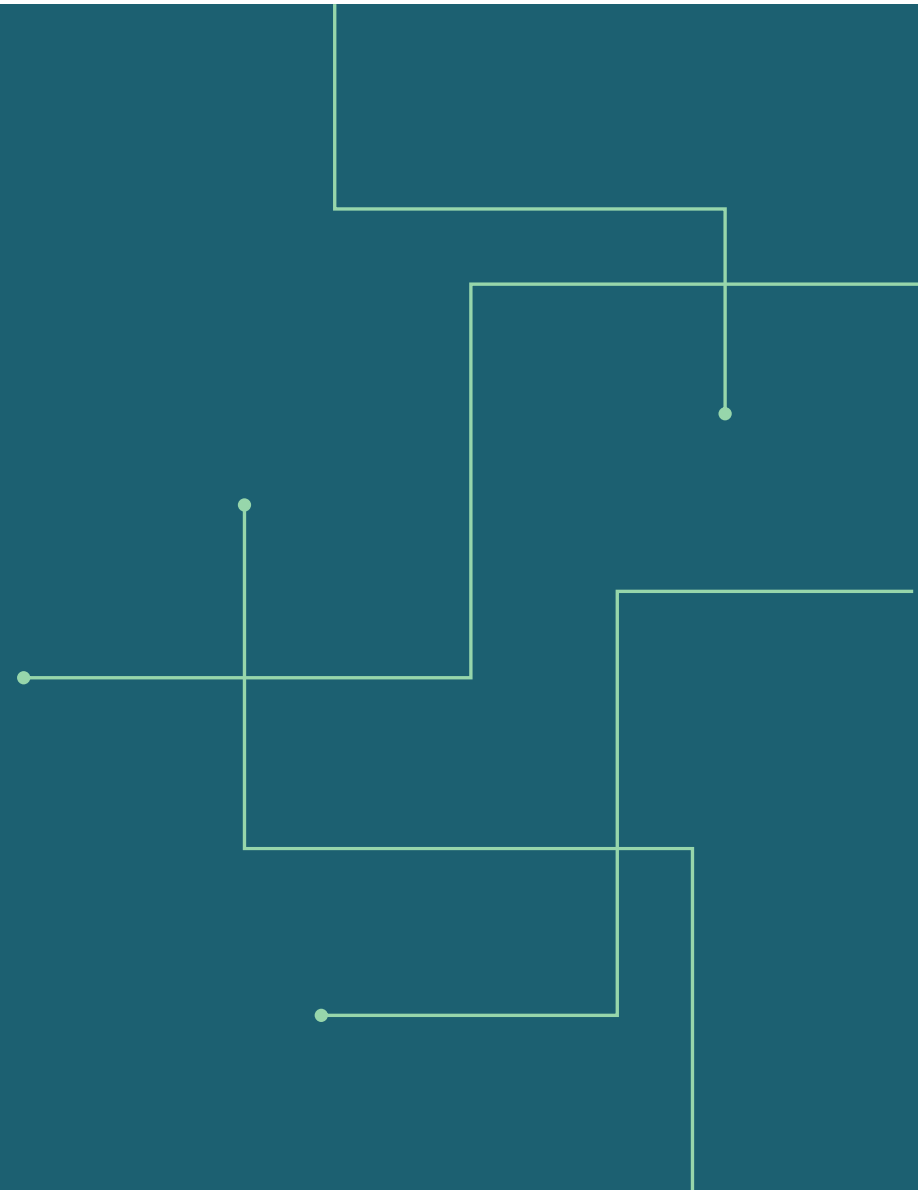
COMMONWEALTH OF VIRGINIA TECHNOLOGY STRATEGY

STEVE NICHOLS (GARTNER) &
COMMONWEALTH CIO BOB OSMOND

ITAC

05/23/23

Governor Youngkin has challenged us to make government work better…

- In order to create a positive impact to the benefit of all Virginians, we must empower our agencies to deliver higher quality services with greater efficiency while also utilizing the strength that comes from working together.

- While each agency has their respective mission, vision, strategy, objectives, and initiatives to achieve key performance results*, this plan defines how technology serves the business goals of the agencies* while highlighting the overall areas of targeted and focused technology ecosystem improvements that will help agencies optimize technology usage, investments, and improvements.

- This audience for this technology strategy plan includes:

  ✓ The Commonwealth agencies seeking to better apply technology within their agencies.

  ✓ Technology practitioners that want to enhance their delivery of technology solutions.

  ✓ Public bodies looking to leverage Commonwealth technology best practices to improve their own organizations.

  ✓ Vendor partners that want to provide technology goods, software, and services to Commonwealth buyers.

- As the Commonwealth addresses massive challenges such as learning loss as a result of the pandemic, the rebuilding of our public safety institutions (Operation Bold Blue Line), regulatory reform, all-of-the-above energy policy, and the crisis of mental health (Right Help Right Now), *improving our application of technology is an essential ingredient in responding to those challenges.*

COMMONWEALTH OF VIRGINIA TECHNOLOGY VISION:

Trusted. Virginian-Centric. High-Performing.

MISSION:

Power an innovative, resilient and competitive Commonwealth through high-impact technology that enhances the lives of Virginians and creates a best-in-class government.

GUIDING PRINCIPLES:

Our guiding principles define the core values underlying the Commonwealth's purpose and use of technology to better achieve agency and business outcomes.

One Team Commonwealth	Virginian-Centric	Disciplined, Innovative Delivery	Maximized Technology Value	Cyber Stewardship

1. **Transform the Virginian experience**

2. **Deliver with a Commonwealth mindset**

3. **Protect Virginians through cybersecurity**

4. **Drive better, faster decision-making through data**

5. **Advance government excellence and adaptability**

6. **Optimize partner ecosystem**

7. **Cultivate statewide IT talent capability**

INITIATIVE 1.1

Transform and secure the online experience

EXPECTED OUTCOMES

- ❑ Online COV services
- ❑ Increased transactions completed through digital channels
- ❑ Compliance on security, web, and accessibility standards

INITIATIVE 1.2

Promote Virginian engagement and operational effectiveness

EXPECTED OUTCOMES

- ❑ Improved satisfaction with government services
- ❑ Reduced time to completion for common processes

INITIATIVE 1.3

Expand Commonwealth connectivity and broadband access

EXPECTED OUTCOMES

- ❑ Expanded broadband coverage across underserved areas
- ❑ Accessible digital skills training programs for all

INITIATIVE 2.1

Integrate Business-Technology strategic planning

EXPECTED OUTCOMES

- ❑ Integrated and streamlined IT Strategic Planning (ITSP) process

INITIATIVE 2.2

Promote operational efficiency through shared infrastructure

EXPECTED OUTCOMES

- ❑ Increased agency cloud adoption
- ❑ Increased IT return on investment

INITIATIVE 2.3

Expand reuse and consolidate Commonwealth shared applications through Enterprise Architecture

EXPECTED OUTCOMES

- ❑ Reduction of point solutions

INITIATIVE 3.1

Fortify cybersecurity

EXPECTED OUTCOMES

- ❑ Improved resistance to cyberattack
- ❑ Implemented Zero Trust security strategy

INITIATIVE 3.2

Embed and advance cybersecurity

EXPECTED OUTCOMES

- ❑ Increased employee participation in security training
- ❑ Secured backups to combat ransomware
- ❑ Accelerated incident reporting and vulnerability remediation

INITIATIVE 3.3

Extend enterprise cybersecurity best practices (Zero Trust)

EXPECTED OUTCOMES

- ❑ Improved collaboration with cybersecurity partners
- ❑ Compliance with security requirements

INITIATIVE 4.1

Drive timely, data-driven decision making

EXPECTED OUTCOMES

- ❑ Better, more timely data
- ❑ Increased data and analytics training opportunities

INITIATIVE 4.2

Establish data exchange and enterprise platforms

EXPECTED OUTCOMES

- ❑ Expanded agency enrollment in Data Trust
- ❑ Increased number of datasets in Data Trust

INITIATIVE 4.3

Optimize data assets and resources

EXPECTED OUTCOMES

- ❑ Increased Data Trust utilization
- ❑ Better agency use of data assets and practices

INITIATIVE 5.1

Streamline internal processes to improve operational efficiency and transparency

EXPECTED OUTCOMES

- Increased First Contact Resolutions (FCR) and Mean Time to Restore (MTTR)
- Increased time recaptured through automation

INITIATIVE 5.2

Consolidate procurement processes

EXPECTED OUTCOMES

- Accelerated procurement cycle time
- Optimized procurement value

INITIATIVE 5.3

Scale and deploy organizational change management (OCM) capability

EXPECTED OUTCOMES

- Improved service value feedback and service adoption
- Increased Commonwealth change management maturity level

INITIATIVE 6.1

Optimize partner ecosystem

EXPECTED OUTCOMES

- ❑ Improved MSI Performance metrics
- ❑ Increased number of successful standard platform onboarding
- ❑ Increased low-code capabilities

INITIATIVE 6.2

Expand capabilities and opportunities for innovation and cost savings

EXPECTED OUTCOMES

- ❑ Increased innovation opportunities
- ❑ New forums for idea sharing across Commonwealth
- ❑ Accelerated Robotic Process Automation deployments

INITIATIVE 7.1

Refresh and promote IT careers

EXPECTED OUTCOMES

- ❑ Increased number of established development programs
- ❑ Reduced turnover
- ❑ Improved career advancement opportunities for Commonwealth IT employees

INITIATIVE 7.2

Develop a tech-ready workforce

EXPECTED OUTCOMES

- ❑ Increased IT educational opportunities for Virginians

INITIATIVE 7.3
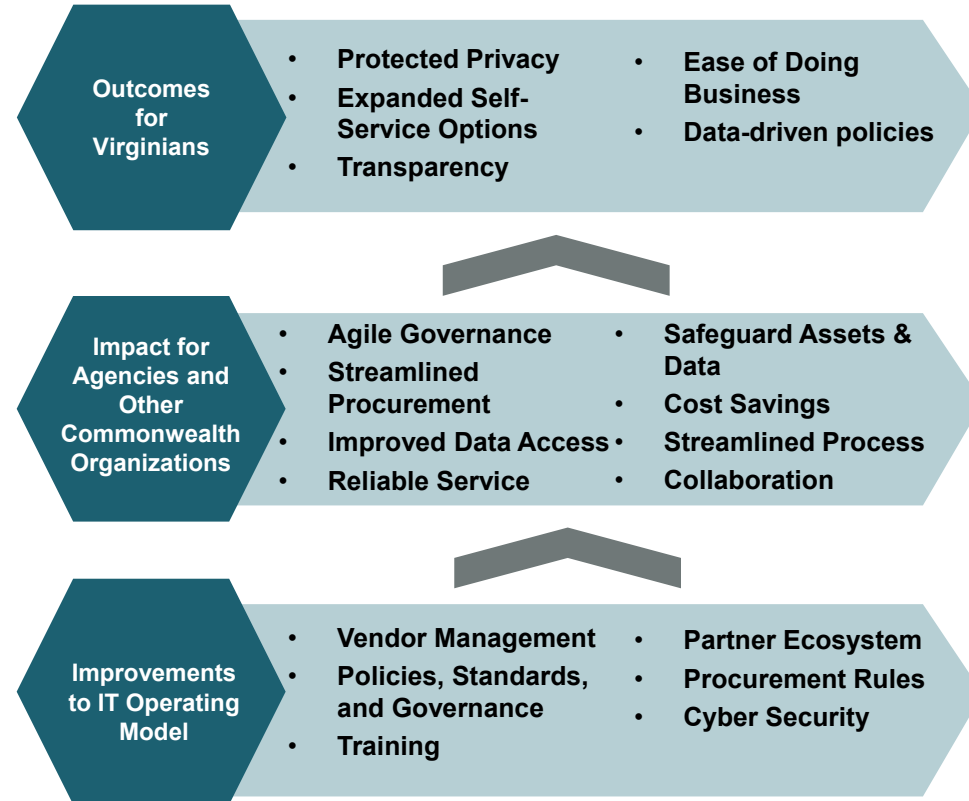
Expand thought leadership and innovation

EXPECTED OUTCOMES

- ❑ Increased collaboration across the Commonwealth

NEXT STEPS:

- The Commonwealth has a shared responsibility to ensure that technology is harnessed to achieve our vision of an **innovative, resilient and competitive Commonwealth that enhances the lives of Virginians and creates a best-in-class government.**

- To operationalize this strategy, the Office of the Commonwealth CIO will share the plan with Commonwealth agencies, partners, and others, define the specific actions and resources to support the strategic initiatives, and identify leadership roles to implement action steps.

- The CIO Advisory Council (CAC) with participants from Commonwealth agencies will be charged with regularly reviewing the plan, measuring progress against strategic goals and presenting results.

Outcomes for Virginians
- Protected Privacy
- Expanded Self-Service Options
- Transparency
- Ease of Doing Business
- Data-driven policies

Impact for Agencies and Other Commonwealth Organizations
- Agile Governance
- Streamlined Procurement
- Improved Data Access
- Reliable Service
- Safeguard Assets & Data
- Cost Savings
- Streamlined Process
- Collaboration

Improvements to IT Operating Model
- Vendor Management
- Policies, Standards, and Governance
- Training
- Partner Ecosystem
- Procurement Rules
- Cyber Security

VIRGINIA
IT AGENCY

vita.virginia.gov | Virginia IT Agency

Zero Trust Strategy and Roadmap

ITAC May 23, 2023

What is Zero Trust

VIRGINIA IT AGENCY

Only allow access to a specific service for a controlled time to a user with valid credentials originating from a compliant device.

FACTS

Zero Trust is based on the premise of least privilege access and microsegmentation

What is Zero Trust?

Better Security Through Increased Visibility and Automation

Continuously Verify and Validate Identities, Device Posture, and Behaviors

MISCONCEPTIONS

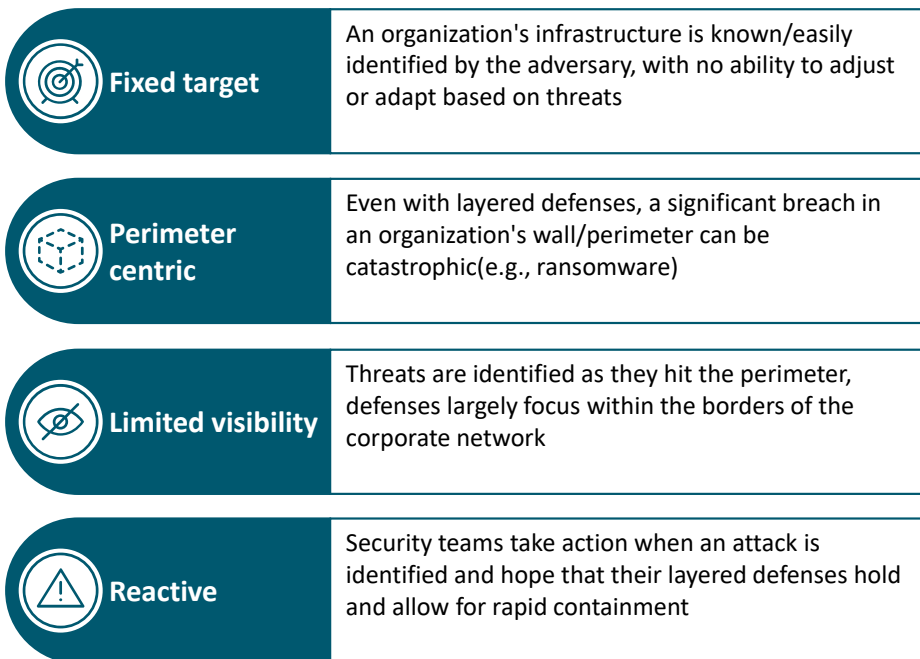Zero Trust will give you everything you need for Cyber Security
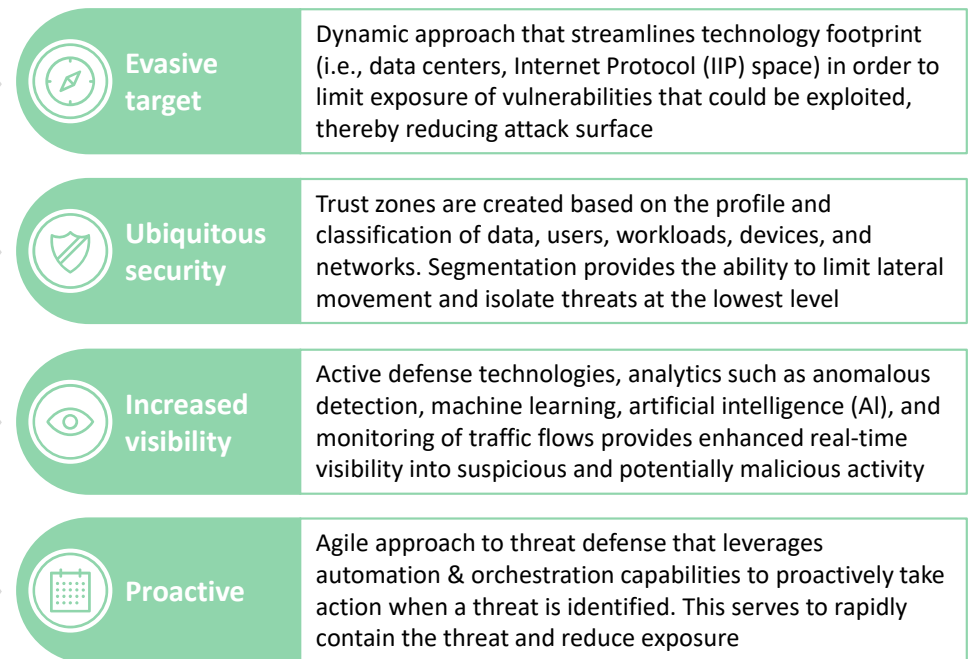
I can just buy Zero Trust

Zero Trust can be implemented quickly and easily

VIRGINIA IT AGENCY

CHALLENGES OF THE TRADITIONAL MODEL

Fixed target
An organization's infrastructure is known/easily identified by the adversary, with no ability to adjust or adapt based on threats

Perimeter centric
Even with layered defenses, a significant breach in an organization's wall/perimeter can be catastrophic(e.g., ransomware)

Limited visibility
Threats are identified as they hit the perimeter, defenses largely focus within the borders of the corporate network

Reactive
Security teams take action when an attack is identified and hope that their layered defenses hold and allow for rapid containment

BENEFITS OF ZERO TRUST

Evasive target
Dynamic approach that streamlines technology footprint (i.e., data centers, Internet Protocol (IIP) space) in order to limit exposure of vulnerabilities that could be exploited, thereby reducing attack surface

Ubiquitous security
Trust zones are created based on the profile and classification of data, users, workloads, devices, and networks. Segmentation provides the ability to limit lateral movement and isolate threats at the lowest level

Increased visibility
Active defense technologies, analytics such as anomalous detection, machine learning, artificial intelligence (AI), and monitoring of traffic flows provides enhanced real-time visibility into suspicious and potentially malicious activity

Proactive
Agile approach to threat defense that leverages automation & orchestration capabilities to proactively take action when a threat is identified. This serves to rapidly contain the threat and reduce exposure

Executive Order 14028, Improving the Nation's Cybersecurity

Published May 2021, EO 14028 describes actions federal agencies must take to better identify, deter, protect, detect, and respond to cybersecurity threats. Included are requirements to move the federal government towards secure cloud services, Zero Trust architectures, and the use of MFA and encryption.

KEY REQUIREMENTS:

- Defines Zero Trust Architecture as a security model, set of design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both within and beyond traditional network boundaries
- Develop a plan to implement Zero Trust Architecture in accordance with NIST standards and guidance
- Continue using cloud technologies and implement those with a Zero Trust Architecture
- Zero Trust eliminates implicit trust and requires continuous verification of both identities and devices
- Zero Trust Architecture is built on least privilege principles, providing users the minimum access and permissions necessary to perform their duties
- In the event of a compromise, Zero Trust can assist with containing damage

- Zero Trust Architecture Model assumes a breach is inevitable or has likely already occurred, so access is limited to only what is needed and looks for malicious activity
- Zero Trust Architecture embeds comprehensive security monitoring, granular risk-based access controls, and system security automation throughout all aspects of the infrastructure to protect data in real-time within a dynamic threat environment
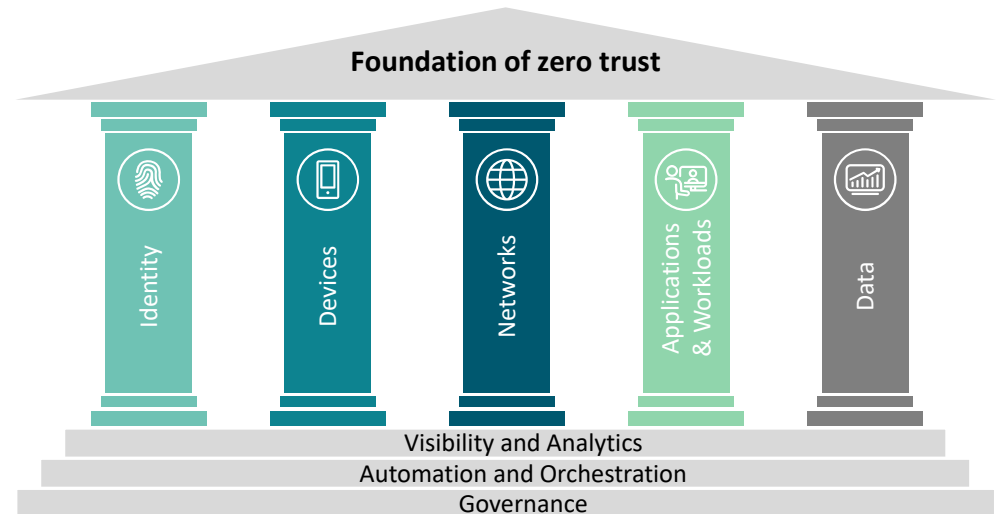
Link: Executive Order on Improving the Nation's Cybersecurity | The White House

VIRGINIA IT AGENCY | Zero Trust Framework

Published April of 2023, the CISA Zero Trust Maturity Model v2 defines five pillars of Zero Trust used as the basis for Deloitte's Zero Trust framework and associated assessments. The Model also defines levels of maturity organizations typically are categorized into. The Model provides a framework to assist organizations in transitioning to Zero Trust.
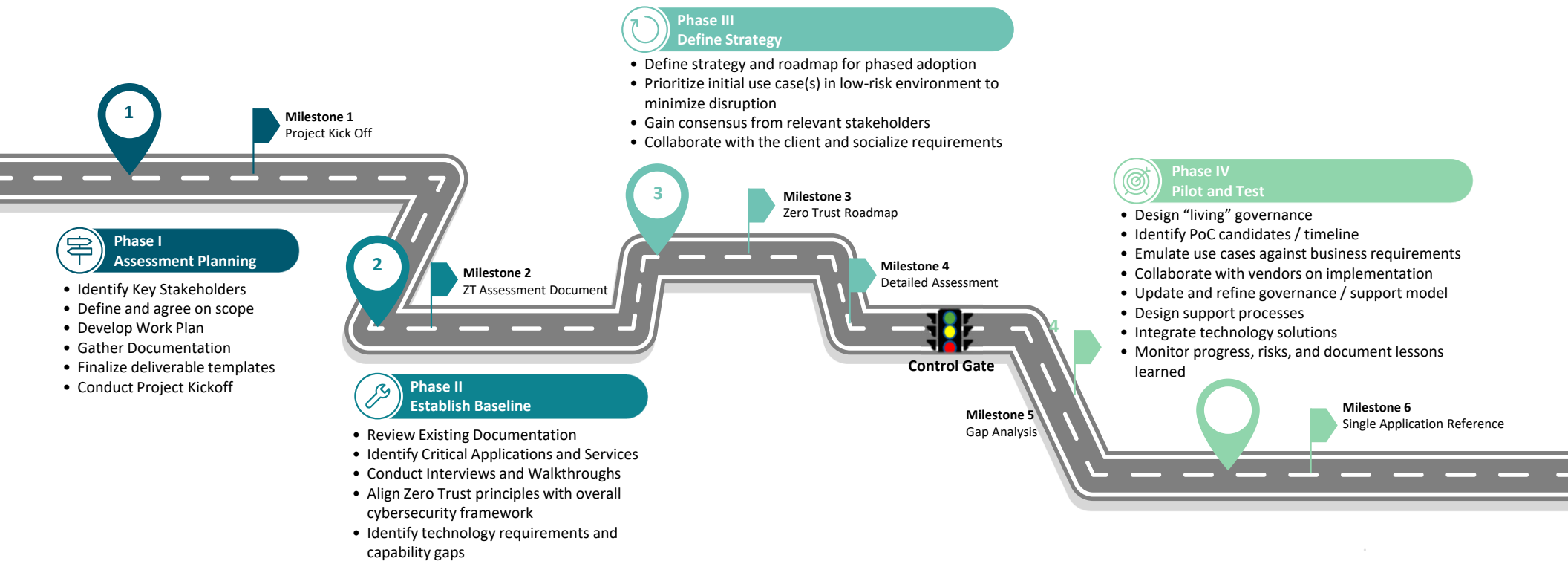
FIVE PILLARS OF ZERO TRUST:

- **Identity:** Zero Trust shifts toward continuous verification and validation to ensure user identity. These checks are done throughout the duration of the user session.
- **Device:** Having a full inventory of each device, and what device is connected to the organization at what time plays a huge role in overall security protections. Zero Trust takes policy away from on-prem and allows for connectivity without traditional access points.
- **Network:** To properly align with a Zero Trust architecture, organizations need to consider transitioning from the original network model towards a tightly controlled network segmentation method that focuses on the requirements of application and system workflows. This allows organizations to provide services and applications to remote users and outside offices.
- **Application Workload:** This pillar puts emphasis on implementing security measures more closely to the application workflows. This bases application access more on identity and device compliance by applying continuous integration and deployment methods to consider user activity at various steps, increasing the security surface.

- **Data:** To shift towards a Zero Trust environment, organizations should focus on protecting their data. This includes both data at rest and data in transit. Data should be inventoried, and logs kept for analytics. Organizations should prioritize data protections towards high value assets (HVAs) first and consider additional critical assets that may need data protections. Shifting towards a data-centric security approach can help organizations prepare for the move towards a Zero Trust model.

Foundation of zero trust

Identity | Devices | Networks | Applications & Workloads | Data

Visibility and Analytics
Automation and Orchestration
Governance

![Virginia IT Agency logo]

VITAs Roadmap to Designing a Zero Trust Reference Architecture

The roadmap below depicts the high-level approach to dive deeper into the initial maturity self-assessment and conduct detailed assessments and gap analysis which will result in the design of a Zero Trust reference architecture focused on one application from a prioritized technology cluster.

Phase III
Define Strategy

- Define strategy and roadmap for phased adoption
- Prioritize initial use case(s) in low-risk environment to minimize disruption
- Gain consensus from relevant stakeholders
- Collaborate with the client and socialize requirements

1

Milestone 1
Project Kick Off

3

Milestone 3
Zero Trust Roadmap

Phase IV
Pilot and Test

- Design "living" governance
- Identify PoC candidates / timeline
- Emulate use cases against business requirements
- Collaborate with vendors on implementation
- Update and refine governance / support model
- Design support processes
- Integrate technology solutions
- Monitor progress, risks, and document lessons learned

Phase I
Assessment Planning

- Identify Key Stakeholders
- Define and agree on scope
- Develop Work Plan
- Gather Documentation
- Finalize deliverable templates
- Conduct Project Kickoff

2

Milestone 2
ZT Assessment Document

Milestone 4
Detailed Assessment

Control Gate

Phase II
Establish Baseline

- Review Existing Documentation
- Identify Critical Applications and Services
- Conduct Interviews and Walkthroughs
- Align Zero Trust principles with overall cybersecurity framework
- Identify technology requirements and capability gaps

Milestone 5
Gap Analysis

Milestone 6
Single Application Reference

![Virginia IT Agency logo] VIRGINIA IT AGENCY

VITA Zero Trust Strategy and Roadmap

ZERO TRUST IMPLEMENTATION PLAN SCOPE

- Developed a recommended implementation plan based on VITA's current capabilities
- Aligned VITA's architecture with the Zero Trust model, in order to achieve its highest priority of securing systems and providing technical leadership to the rest of the Commonwealth agencies
- Identified any completed activities related to Zero Trust that will provide the most immediate security impact

PROJECT PURPOSE

- Analyzed VITA's current state Zero Trust capabilities, gaps and maturity in relation to the requirements set forth in the CISA Zero Trust Maturity Model
- Collaborated with VITA on a Zero Trust Strategy and Roadmap that depicts the actions required by the agency to successfully deploy a fully mature Zero Trust architecture.

PROJECT OBJECTIVES

- Established the foundation for a secure, accessible, and effective working environment for years to come.
- Delivered a Zero Trust Strategy and Roadmap Report (and accompanying presentation) that is actionable and detailed.
- Achieved its highest priority of securing systems and providing technical leadership to the rest of the Commonwealth agencies
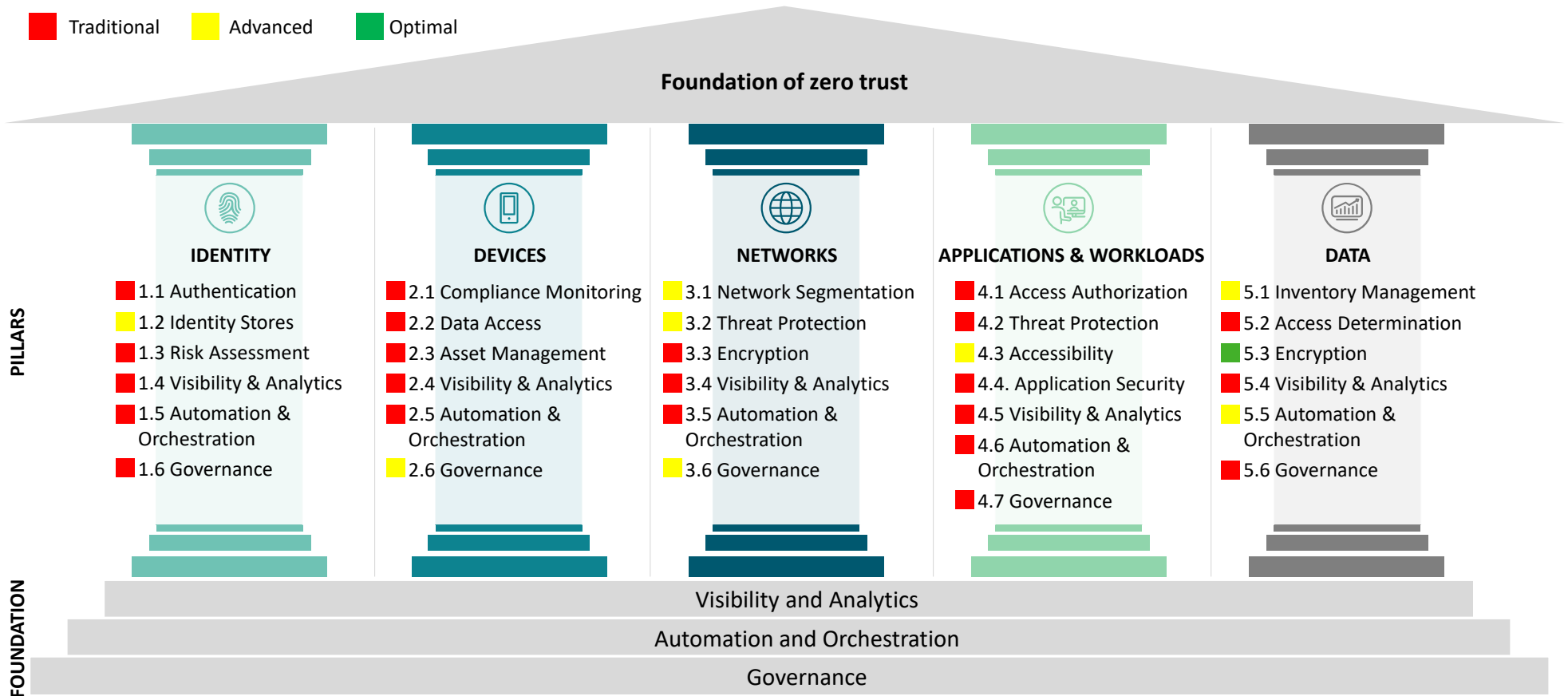- Identified steps that have been completed by VITA toward ZTA implementation

METHODOLOGY

- Evaluated VITA's Current state Zero Trust capabilities in accordance with CISA Zero Trust maturity model v1, OMB M-22-09, & VITA's vision.
- Document maturity levels of VITA's cybersecurity capabilities from a ZT perspective, including the 5 CISA ZT Pillars and 3 Cross Cutting domains
  - **Identity, Device, Network, Application Workload, Data**
  - **Automation & Orchestration, Analytics & Visibility, Governance**

- Conducted **25+** live assessment interviews, spanning **200+** questions, with **20+** stakeholders to identify current capabilities and gaps.

![Virginia IT Agency logo] **Assessment Results**

21 capabilities found to be operating at the Traditional level (68%). There were 9 capabilities found to be operating at the Advanced level (29%). There was 1 capability found to be operating at the Optimal level (3%.)
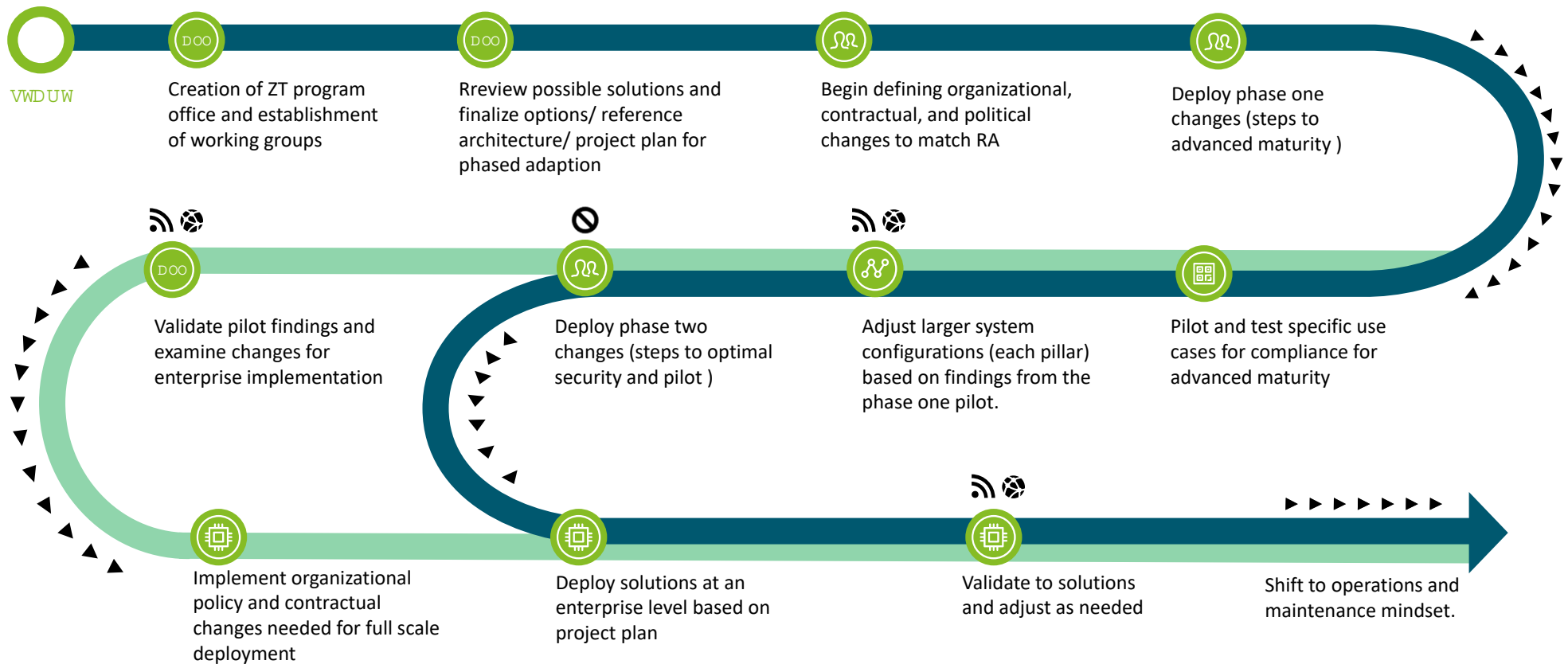
🟥 Traditional   🟨 Advanced   🟩 Optimal

Foundation of zero trust

PILLARS

IDENTITY
- 🟥 1.1 Authentication
- 🟨 1.2 Identity Stores
- 🟥 1.3 Risk Assessment
- 🟥 1.4 Visibility & Analytics
- 🟥 1.5 Automation & Orchestration
- 🟥 1.6 Governance

DEVICES
- 🟥 2.1 Compliance Monitoring
- 🟥 2.2 Data Access
- 🟥 2.3 Asset Management
- 🟥 2.4 Visibility & Analytics
- 🟥 2.5 Automation & Orchestration
- 🟨 2.6 Governance

NETWORKS
- 🟨 3.1 Network Segmentation
- 🟨 3.2 Threat Protection
- 🟥 3.3 Encryption
- 🟥 3.4 Visibility & Analytics
- 🟥 3.5 Automation & Orchestration
- 🟨 3.6 Governance

APPLICATIONS & WORKLOADS
- 🟥 4.1 Access Authorization
- 🟥 4.2 Threat Protection
- 🟨 4.3 Accessibility
- 🟥 4.4. Application Security
- 🟥 4.5 Visibility & Analytics
- 🟥 4.6 Automation & Orchestration
- 🟥 4.7 Governance

DATA
- 🟨 5.1 Inventory Management
- 🟥 5.2 Access Determination
- 🟩 5.3 Encryption
- 🟥 5.4 Visibility & Analytics
- 🟨 5.5 Automation & Orchestration
- 🟥 5.6 Governance

FOUNDATION

Visibility and Analytics

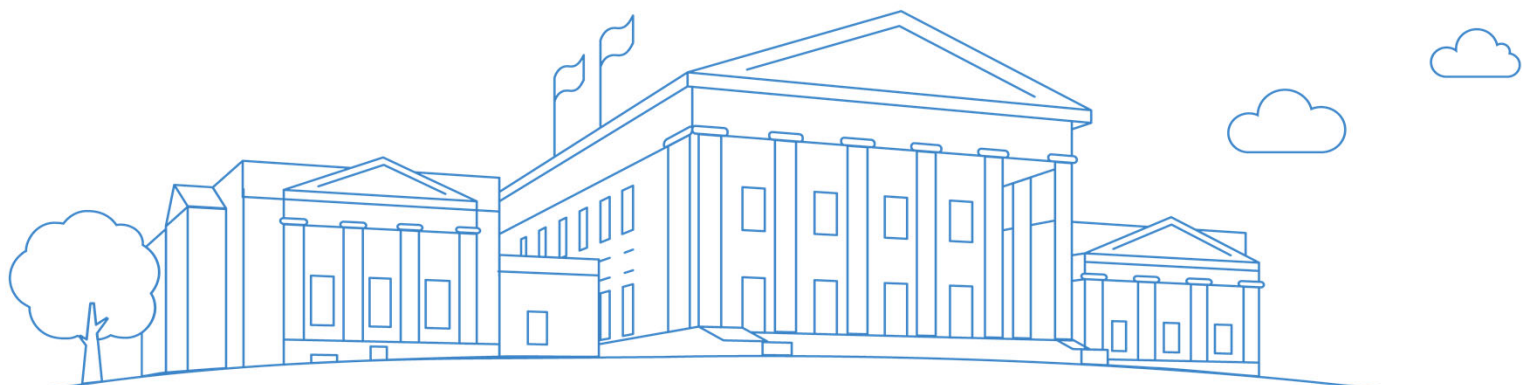Automation and Orchestration

Governance

VIRGINIA
IT AGENCY

1. Implement a ZT Program Office to coordinate, manage, and measure ZT Implementation across the Commonwealth.
2. Deploy centralized ICAM solution and federate with other identity stores for a complete inventory of the Commonwealth's users (both Person and Devices)
3. Deploy phishing-resistant MFA to all users.
4. Expand usage of existing security tools (SIEM/SOAR/XDR) and integrate with SOAR for rapid detection and response.
5. Deploy application microsegmentation technologies to baseline and protect workflows.
6. Deploy continuous device monitoring and adaptive authentication capabilities.
7. Deploy AI/ML solution to better monitor and respond to anomalous activities.
8. Inventory, tag, and categorize data to provide better protections and granular access management.
9. Deploy improved cryptographic key management solution to better control encryption of data both at rest and in transit. Improves quantum readiness through crypto agility.

VIRGINIA
IT AGENCY

Diagram of high-level sequenced tasks to achieve optimal Zero Trust maturity.

VWDUW

Creation of ZT program office and establishment of working groups

Rreview possible solutions and finalize options/ reference architecture/ project plan for phased adaption

Begin defining organizational, contractual, and political changes to match RA

Deploy phase one changes (steps to advanced maturity)

Validate pilot findings and examine changes for enterprise implementation

Deploy phase two changes (steps to optimal security and pilot)

Adjust larger system configurations (each pillar) based on findings from the phase one pilot.

Pilot and test specific use cases for compliance for advanced maturity

Implement organizational policy and contractual changes needed for full scale deployment

Deploy solutions at an enterprise level based on project plan

Validate to solutions and adjust as needed

Shift to operations and maintenance mindset.

Commonwealth of Virginia

Website Modernization Project

ITAC Brief

May, 2023

VIRGINIA IT AGENCY

➢ **Project Vision and Scope**
➢ **Agency Website Key Stats**
➢ **Website Modernization Snapshot Progress**
➢ **Website Modernization Project Overview**
➢ **Key Accomplishments to Date**
➢ **Next Steps**
➢ **Appendix:** *New Branding*

PROJECT VISION AND SCOPE

VISION STATEMENT

Improve citizen trust and engagement with Virginia government agencies thru websites that are modern, consistently branded, secure, 508 accessible and digitally responsive.

COMPLETED INITIATIVES

- ✓ Update web standards to include naming standardization
    - ✓ Deploy a standard look and feel template
    - ✓ Gov Domain Naming Requirement
    - ✓ Website Metrics and Analytics
- ✓ Provide resources to agencies
    - ✓ Deploy a content management solution to remove outdated and irrelevant content
    - ✓ Pre-qualified vendors
    - ✓ Security training and tools
- ✓ Implement a 508-accessibility training and compliance program
    - ✓ Enterprise licenses for Siteimprove to monitor and maintain compliance
- ✓ Coordinate agency remediation & implementation planning and execution tracking
    - ✓ Project management
    - ✓ Monthly All Hands meetings
    - ✓ Individual agency reports and review of progress
    - ✓ Customer Advisory Council Updates

AGENCY WEBSITE KEY STATS

Deployed Two Enterprise
Tools for Agencies:
*Siteimprove (Accessibility)
*Acunetix 360 (Security)

All New Sites Must Be
Reviewed And Approved By
Enterprise Architecture
(detailed in standard WEB-38)

Retiring Sites
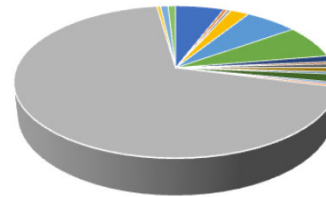
- DGS
- DMAS
- DMV
- DOE
- DRPT
- DWR
- ELECT
- LVA
- MRC
- NSU
- SCHEV
- TAX
- VADOC
- VDDHH
- VDOT
- VEDP
- VITA
- VSP

New Style Guide & Concierge Service

Thirteen Agencies Redoing Their Websites

- Department of Behavior Health and Development Services
- Department of Education
- Department of Emergency Management
- Department of Fire Programs
- Department of Historic Resources
- Department of Labor and Industry
- Department of Motor Vehicles
- Department of Rail and Public Transportation
- Department of Small Business and Supplier Diversity
- Department of Veterans Services
- Elections
- Virginia Board for People with Disabilities
- Virginia Commission for the Arts
- Virginia Department of Transportation
- Virginia Energy

Security 2022 Q4 Vulnerability Report

20 Agencies, 27%

16 Agencies, 21%

39 Agencies, 52%
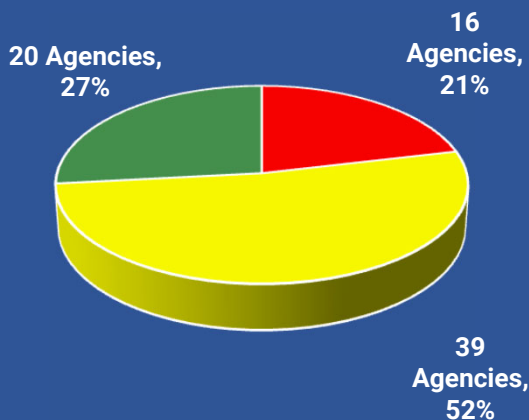
Agencies Have 30 Days To Remediate High And Critical Vulnerabilities

New Statewide Logo

Executive Branch Sites
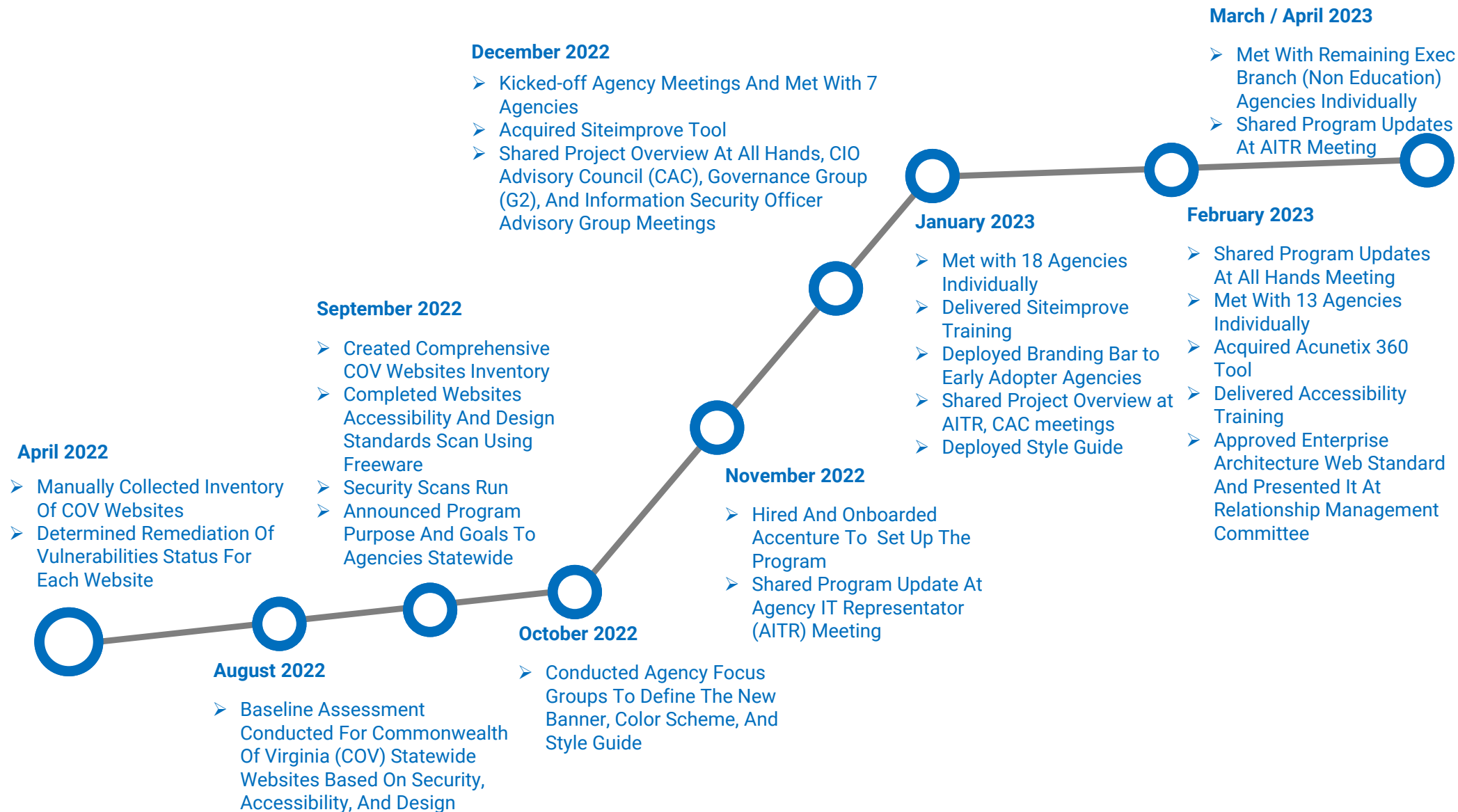429

URLs Scanned By Security
2,616

WEBSITE MODERNIZATION SNAPSHOT PROGRESS

AUGUST 2022	APRIL 2023
No Central Comprehensive Website Inventory	Solid Inventory. Confirmed Agency Websites. Inventory Validated And Verified Monthly.
No Ability To Track Web Pages, Documents Or Content	Agency Sites Have Been Inventoried For Page Counts, Compliance With The 3-Year Look-Back, Documents And Other Key Content
Agencies Had Non-Standard URLs	New Agency Standard Requires .Gov URL
Inconsistent Website Look & Feel	Website Branding Package With New Logo & Bar
Outdated 2017 Web Standard	New Statewide Web Systems Standard
No Agency Scanning Tool Contracts For 508 Accessibility Or Security	Siteimprove (508) And Acunetix (Security) Agency Scanning Tool Provided To Each Agency
Website Analytics Not Used Across Commonwealth	Use Of Analytics Required In Web Standards. Siteimprove Analytics Available For Agencies
No Agency Tools Or Contracts For Agency Level Translation Or Authentication	Purchasing Tools And Solutions For Program Including Captcha For Authentication And Language Translation

KEY ACCOMPLISHMENTS TO DATE

April 2022
➢ Manually Collected Inventory Of COV Websites
➢ Determined Remediation Of Vulnerabilities Status For Each Website

August 2022
➢ Baseline Assessment Conducted For Commonwealth Of Virginia (COV) Statewide Websites Based On Security, Accessibility, And Design

September 2022
➢ Created Comprehensive COV Websites Inventory
➢ Completed Websites Accessibility And Design Standards Scan Using Freeware
➢ Security Scans Run
➢ Announced Program Purpose And Goals To Agencies Statewide

October 2022
➢ Conducted Agency Focus Groups To Define The New Banner, Color Scheme, And Style Guide

November 2022
➢ Hired And Onboarded Accenture To Set Up The Program
➢ Shared Program Update At Agency IT Representator (AITR) Meeting

December 2022
➢ Kicked-off Agency Meetings And Met With 7 Agencies
➢ Acquired Siteimprove Tool
➢ Shared Project Overview At All Hands, CIO Advisory Council (CAC), Governance Group (G2), And Information Security Officer Advisory Group Meetings

January 2023
➢ Met with 18 Agencies Individually
➢ Delivered Siteimprove Training
➢ Deployed Branding Bar to Early Adopter Agencies
➢ Shared Project Overview at AITR, CAC meetings
➢ Deployed Style Guide

February 2023
➢ Shared Program Updates At All Hands Meeting
➢ Met With 13 Agencies Individually
➢ Acquired Acunetix 360 Tool
➢ Delivered Accessibility Training
➢ Approved Enterprise Architecture Web Standard And Presented It At Relationship Management Committee

March / April 2023
➢ Met With Remaining Exec Branch (Non Education) Agencies Individually
➢ Shared Program Updates At AITR Meeting

Website Modernization
An official program of the Commonwealth of Virginia

VIRGINIA IT AGENCY

6

NEXT STEPS

Meet With Non Executive Branch Agencies

Conduct Universal Tracking Of Website Traffic/Metrics

Finish Phase 2 Branding Bar With Enterprise Search Roll-Out

Performance Metrics For Websites Based On New Standard

Checklist For Agencies Go Live For Websites Based On New Standard

Continue Working with Agencies on Website Modernization Estimates

Appendix

PRIMARY COLORS

#242424

#183055

#3E81C4

#BF1313

#FFCE00

#FFFFFF

NEW LOGO

NEW BRANDING BAR

Governor of Virginia
An official website of the Commonwealth of Virginia   Here's how you know ∨

Commonwealth of Virginia ∨
Services and Resources

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

The following is the remote or electronic participation policy of the Information Technology Advisory Council (ITAC).

Member Remote Participation

Individual ITAC members may participate in meetings of ITAC by electronic communication means to the full extent permitted by applicable law, including § 2.2-3708.3 of the Code of Virginia. (As of December 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.

Whenever a member wishes to participate from a remote location, the law requires a quorum of ITAC to be physically assembled at the primary or central meeting location.

Virtual Meetings

ITAC may hold all-virtual public meetings to the full extent permitted by applicable law, including Virginia Code § 2.2-3708.3(C). (As of December 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 ITAC conduct an all-virtual public meeting shall be conveyed to VITA staff who shall then relay such requests to the Chair of the ITAC.

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 ITAC shall vote whether to allow such participation.

The request for remote participation or that ITAC conduct an all-virtual public meeting shall be recorded in the minutes of the meeting. If ITAC 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 ITAC 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.
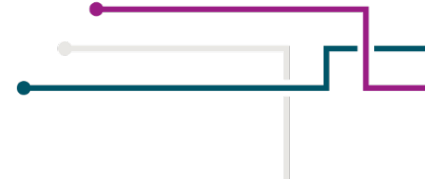
Information Technology Advisory Council

Charter & Bylaws

ARTICLE I.   Applicability.

SECTION 1.   General.

The Information Technology Advisory Council (ITAC) was created and has the authority to adopt a charter and bylaws pursuant to the Va. Code § 2.2-2699.6. The provisions of these Charter and Bylaws are applicable to all proceedings of the Information Technology Advisory Council ("ITAC") 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.

The council is constituted under Va. Code §§ 2.2-2699.5, *et seq.* and §2.2-2100 as a "Advisory Council." As a "Advisory" council pursuant to Va. Code §2.2-2100, the Council is specifically charged with the duties and responsibilities set forth in the basic law governing the actions of the Council. As set forth and consistent with basic law, the Council shall be responsible for advising, and making recommendations to, the Chief Information Officer of the Commonwealth (CIO) and the Secretary of Administration regarding information technology in the Commonwealth, as detailed in § 2.2-2699.6.

ARTICLE II.   Members

SECTION 1.   Members.

ITAC shall consist of not more than 20 members as follows: (i) the Secretary of Administration, or his designee, the CIO, and another of the Governor's Secretaries as defined in subsection E of § 2.2-200, or his designee, all of whom shall serve ex officio with voting privileges; (ii) four members of the House of Delegates, to be appointed by the Speaker of the House of Delegates; (iii) three members of the Senate, to be appointed by the Senate Committee on Rules; and (iv) an even number, not to exceed 10, of nonlegislative citizen members to be appointed by the Governor and serve with voting privileges. Nonlegislative member vacancy other than by expiration of term shall be filled by the Governor for the unexpired term. Legislative members and ex officio members of the ITAC shall serve terms coincident with their terms of office.

SECTION 2.   Officers

ITAC shall elect a Chair and Vice Chair annually from among the members, except that neither the Secretary of Administration nor the CIO may serve as chairman. A Chair and Vice Chair shall be elected from among the voting members through nomination and formal vote. The Chair shall preside at all ITAC meetings. 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.

SECTION 3.   Representation of ITAC.

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

ARTICLE III.   Meetings and Public Disclosure.

SECTION 1.   Regular Meetings.

Regular meetings of ITAC may be held up to four times per year, at such time and place as ITAC, or the Chair as needed, may determine. No business requiring a vote or final decision of ITAC may be conducted in the absence of a quorum, as defined in Article III, Section 4.

SECTION 2.　　　Subcommittees and Work Groups.

The ITAC may appoint advisory subcommittees consisting of individuals with expertise in particular subject areas and information technology to advise the ITAC on the utilization of nationally recognized technical and data standards in such subject areas. If such a subcommittee is appointed by the ITAC, the CIO, or his designee, shall be an ex officio member and the Secretary of Administration may appoint representatives from other relevant Secretariats or state agencies as may be appropriate. Any such subcommittee may be appointed for a period of two years and may be reappointed by the ITAC at the end of any two-year period. 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 ITAC 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 majority of appointed members shall constitute a quorum.

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 ITAC, 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, ITAC 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, ITAC 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 advisory council 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 ITAC review and approval, normally through presentation at the next meeting.

ARTICLE IV. Amendments to the Charter and Bylaws

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

These Bylaws were adopted by ITAC, and became effective, on December 8, 2022, and remain in effect until subsequently amended.
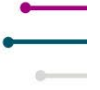
September 5, 1 p.m. – 4 p.m., Tuesday
December 5, 1 p.m. – 4 p.m., Tuesday