VIRGINIA IT AGENCY

Information Technology Advisory Council (ITAC)

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.

VIRGINIA IT AGENCY

CYBERSECURITY OVERVIEW

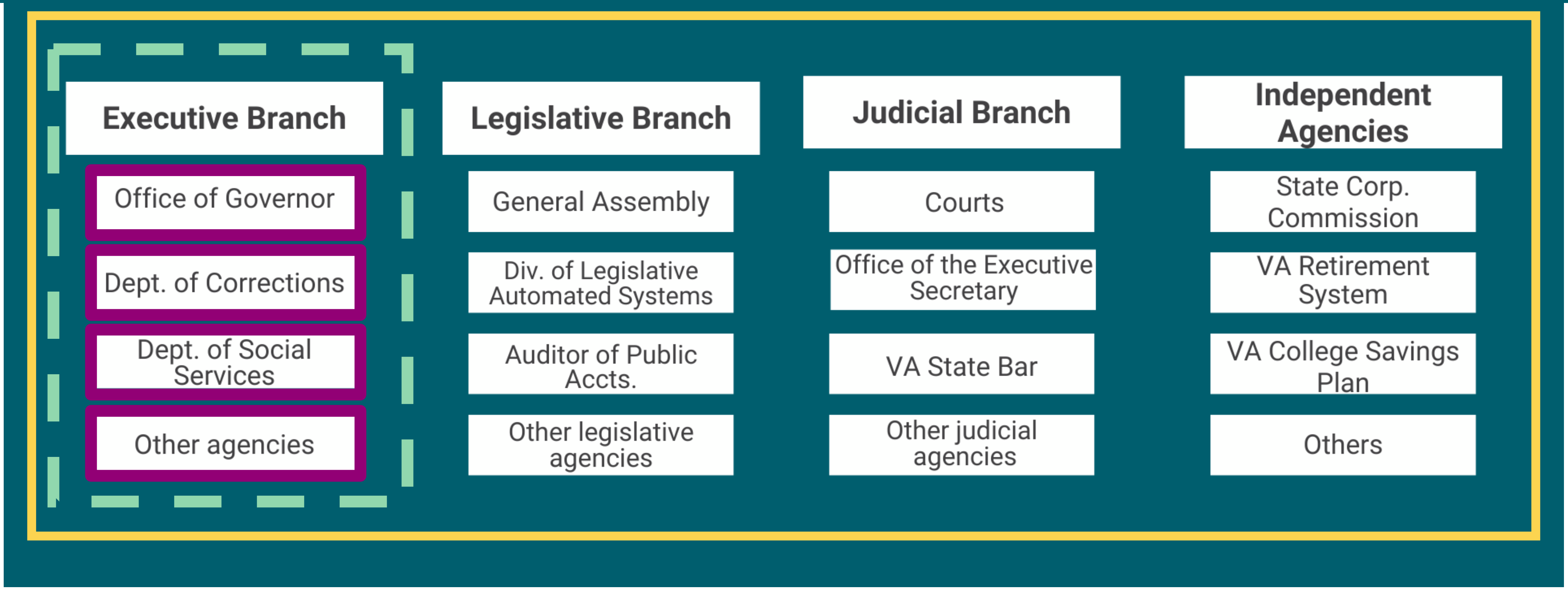
MIKE WATSON

Chief Information Security Officer

ITAC

12/08/22

SCOPE OF VITA CYBERSECURITY



Executive Branch	Legislative Branch	Judicial Branch	Independent Agencies
Office of Governor	General Assembly	Courts	State Corp. Commission
Dept. of Corrections	Div. of Legislative Automated Systems	Office of the Executive Secretary	VA Retirement System
Dept. of Social Services	Auditor of Public Accts.	VA State Bar	VA College Savings Plan
Other agencies	Other legislative agencies	Other judicial agencies	Others

LEGEND:

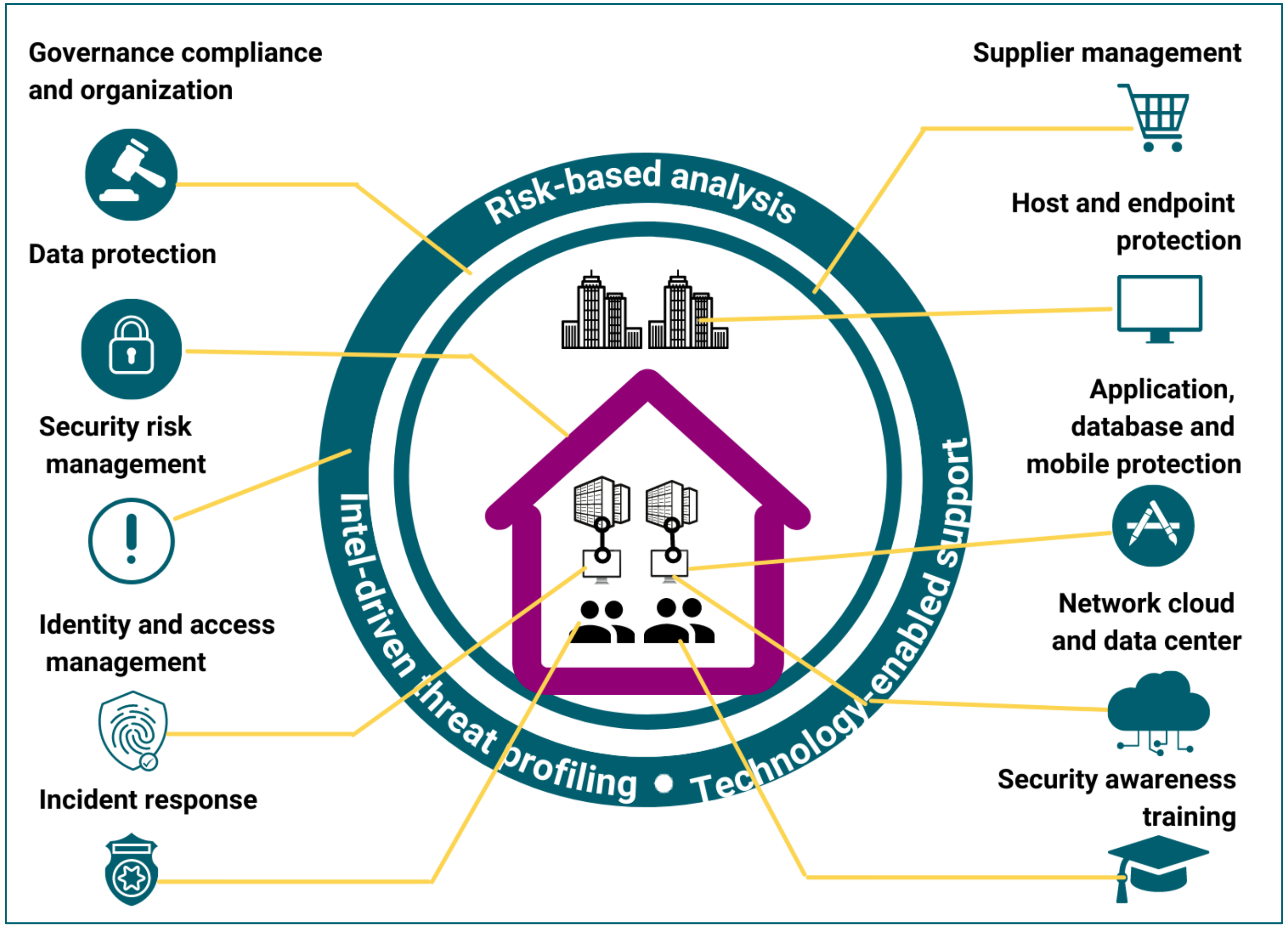
▬ Security policies and standards developed by VITA apply throughout state government

▬ Infrastructure (including security) services and oversight provided by VITA within executive branch

□ Applications are administered by agencies, including security monitoring and configuration

HOW VITA FULFILLS STATE CYBERSECURITY RESPONSIBILITIES

- Strong standards and cybersecurity framework built off federal standards (NIST)
  - ✓ Agencies receive training and held accountable for implementation
- Cyberattack monitoring for state systems
  - ✓ Data protection and security breach containment focus
  - ✓ Tabletop exercises
- IT risk management program
  - ✓ Third-party risk evaluated in each contract
  - ✓ Liability controls
  - ✓ Cyber insurance


Governance compliance and organization
Data protection
Security risk management
Identity and access management
Incident response
Supplier management
Host and endpoint protection
Application, database and mobile protection
Network cloud and data center
Security awareness training
Risk-based analysis
Intel-driven threat profiling
Technology-enabled support

CYBERSECURITY RESPONSIBILITIES

VITA'S SECURITY RESPONSIBILITIES

- Security policies, standards, and governance, including for:
  - IT security auditing
  - Data protection
- Information security training curriculum and materials
- IT risk management program
- Threat management and response, including vulnerability scanning
- IT infrastructure security, administration, and tools, including cloud oversight

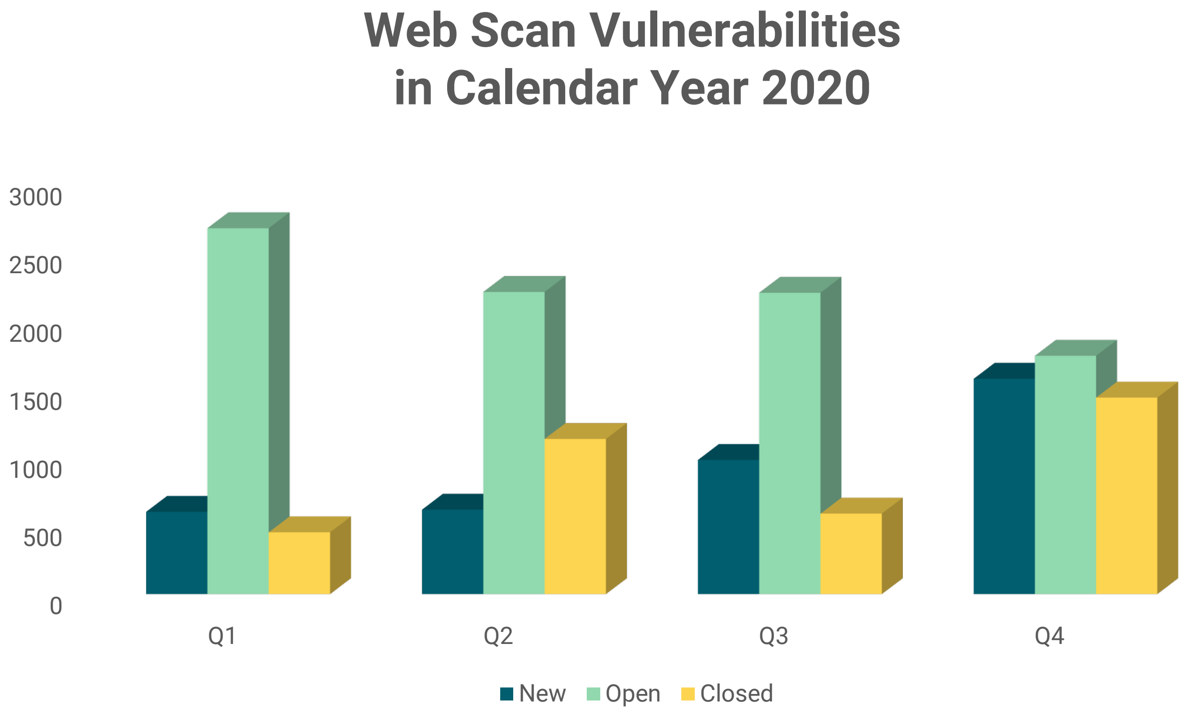
EACH AGENCY'S SECURITY RESPONSIBILITIES

- Appoint an information security officer
- Ensure compliance with security policies and standards, including data classification and ownership
- Train employees
- Participate in IT risk management program
- Report security incidents (executive branch agencies only under current law)
- Application security and administration

THREAT LANDSCAPE

- Recent cyber threats
  - Ransomware
  - Cyber-related fraud
  - Phishing attacks
  - Supply chain cyberattacks
  - Critical infrastructure (state, local, and private)
- Environmental drivers
  - Ransomware as a service
  - Successful extortion and fraud
  - COVID-related architecture changes

The Commonwealth experienced over 66 million cyberattack attempts in the last year. Security teams blocked over 50,000 pieces of malware.



CYBERSECURITY PRIORITIES

- Improving response coordination, planning, and information to address threats
- Driving threat reduction and technology improvements (*e.g.*, Log4j and SolarWinds)
- Implementing leading security architecture (Zero Trust Framework), which is important to support a distributed workforce and cloud environments
- Improving security for operational technology (OT) – *i.e.*, systems with direct impact on the physical world
- Implementing the enterprise cyber recovery solution
- Increasing critical infrastructure cybersecurity engagement
- Augmenting workforce and resources

INCIDENT REPORTING LEGISLATION

Enacted as 2022 Va. Acts chapters 626 & 627

Past requirement

- Executive branch agencies report cybersecurity incidents within 24 hours to VITA.

New requirement

- All public bodies (state and local) report cybersecurity incidents within 24 hours to the Virginia Fusion Center, which will share them with VITA.
- Added to Va. Code 2.2-5514, effective July 1, 2022.

WHY REPORTING IS IMPORTANT

- Supports building a cohesive and comprehensive cyber ecosystem across the Commonwealth.
- Helps raise enhanced awareness across the ecosystem and offers the opportunity for shared support and protective actions in situations when every moment counts.
- Cybersecurity planning
- https://www.reportcyber.virginia.gov/

WHAT TO REPORT

- An incident should be reported if any of the following occur:
  - An adverse event to an information system, network, and/or workstation **OR**
  - The exposure, or an increased risk of exposure, of Commonwealth data **OR**
  - A threat of the occurrence of such an event or exposure.
- FAQs: https://www.reportcyber.virginia.gov/faqs/

STATE & LOCAL CYBERSECURITY GRANT PROGRAM

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

- Part (Division D, Title I, Subtitle B) of the Infrastructure Investment and Jobs Act, passed in 2021
- Provides $1 billion in grant funding for cybersecurity to state and local government entities
  - 4-year program
  - Federal funding share declines over those four years, with state matching fund share rising
- Intended to address gaps in government cybersecurity programs. Encourages states to adopt and implement an effective cybersecurity plan, through an intergovernmental planning committee with members that have cybersecurity experience.

Item 93(F)

STATE AND LOCAL CYBERSECURITY GRANT FUNDING

The 2022 Appropriation Act (a.k.a. the budget) appropriates

- ~$4.92 million GF (the estimated total state matching funds) and
- ~$21.4 million (the estimated total federal grant funding available to Virginia).

The budget also directs VITA to take the steps necessary for the state and local cybersecurity grant program.

STATE & LOCAL CYBERSECURITY GRANT PROGRAM

GRANT GOAL

Assist state, local, and territorial governments with managing and reducing systemic cyber risk.

ADMINISTRATION

Grant administration through the State Administrative Agency (SAA) with FEMA (which is VDEM in Virginia)

GRANT OBJECTIVES FOR FY22

1. Develop and establish appropriate governance structures, including developing, implementing or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations
2. Understand current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments
3. Implement security protections commensurate with risk
4. Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility

CYBERSECURITY PLANNING COMMITTEE

BROAD, INTERGOVERNMENTAL, EXPERIENCED MEMBERSHIP

- Chaired by CISO (delegated by CIO)
- Vast majority of members have specific IT and cyber experience
- Representation from:
  - state (or other eligible entity group) and localities (county, city and town),
  - legislative and judicial branches
  - institution of public education,
  - institution of public health,
  - jurisdictions diverse by population type (rural, suburban and high-population),
  - public safety, homeland security, emergency management, and law enforcement
  - elections
  - State National Guard
  - others w/expertise and skillsets to represent cybersecurity interests across state

CYBERSECURITY PLANNING COMMITTEE – RESPONSIBILITIES

PLANNING COMMITTEE RESPONSIBILITIES (SEE NOFO PP.4-5, 64)

- Assisting with development, implementation, and revision of the cybersecurity plan (and projects pursuant to it)
- Formally approving cybersecurity plan
  (state CIO/CISO and feds [CISA] must also approve)
- Assisting with determination of effective funding priorities (*i.e.*, work with entities in jurisdiction to identify and prioritize individual projects)
- Coordinating with other committees/entities w/goal of maximizing coordination and reducing duplication
- Creating a cohesive planning network that builds and implements cyber preparedness initiatives
- Ensuring investments support closing capability gaps or sustaining capabilities; and
- Ensuring local government members providing consent for services, capabilities, or activities provided by the eligible entity through this program

CYBERSECURITY PLAN

CYBERSECURITY PLAN BASICS (SEE NOFO PP.66)

- Comprehensive strategic plan to reduce cyber security risk and increase capability
- State-wide, not for any single entity or level of government within the staet
- Should cover 2-3 years
- Certain required elements, with discretion to add others
- Individual projects then align to the plan
- Exception allowed completing the cybersecurity plan during the first year (by Sept. 30, 2023), which helps produce a better plan and is what Virginia has chosen to do

CYBERSECURITY PLAN – KEY BEST PRACTICES

REQUIRED TO BE INCLUDED IN THE PLAN AND PROJECTS (SEE NOFO P.5)

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

As cybersecurity maturity increases, more advanced best practices (such as endpoint detection & response and regular penetration testing) will be recommended.

THANK YOU!

QUESTIONS?

VIRGINIA
IT AGENCY

ENTERPRISE IT MODERNIZATION

LYN MCDERMID

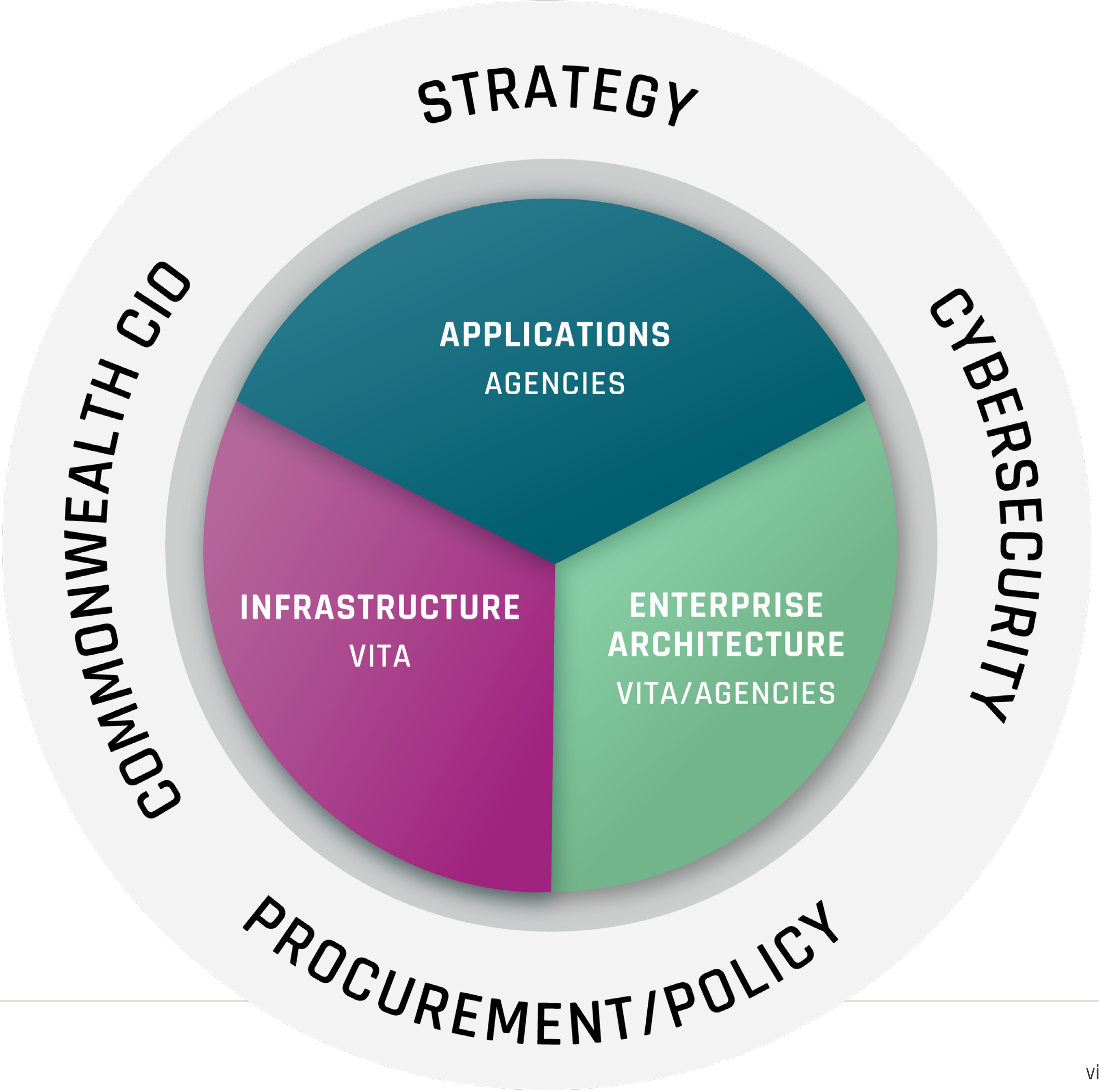
Secretary of Administration

BOB OSMOND

CIO

ITAC

12/08/22



STRATEGY

CYBERSECURITY

PROCUREMENT/POLICY

COMMONWEALTH CIO

APPLICATIONS

AGENCIES

INFRASTRUCTURE

VITA

ENTERPRISE ARCHITECTURE

VITA/AGENCIES

THE EXECUTIVE BRANCH IT SCOPE OF SERVICE

DATA CENTERS

PHYSICAL DATA CENTERS
QTS
MESC

VIRTUAL DATA CENTERS
AWS
AZURE
OCI

65

EXECUTIVE BRANCH AGENCIES

1,700

LOCATIONS SERVED IN VIRGINIA

ENTERPRISE APPLICATION SOLUTIONS

MICROSOFT POWER PLATFORM
SALESFORCE
DOCUSIGN (EPEN)
UIPATH RPA
APP INT SERVICES (IBM
DIGITAL EXPERIENCE PLATFORM (T4)

Cybersecurity in everything

MANAGED STORAGE ~2.5 PETABYTES

MAINFRAMES IBM

VITA MANAGES

COMPUTERS
62,117 PCs
5,161 SERVERS

COMMUNICATIONS
25,000 VOIP PHONES
3,200 CIRCUITS

PRINTERS
3,735 NETWORK
21,971 DESKTOP

MAILBOXES
60,936 ACCOUNTS
9,477 MANAGED NETWORK COMPONENTS

PROCUREMENTS
200 STATE CONTRACTS, 8 MSIs, 260 ECOS

ENTERPRISE-WIDE APPLICATIONS: BY THE NUMBERS

2,396 Total number of applications	**2,381** Total number of data assets (databases etc.)	**1,063** Number of applications that address agency core business (vs. back-office functions)
276 Applications that are accessible by the general public	**1,372** Number of applications that access/contain sensitive data	**351** Number of applications that are 20 years old or more

COMMONWEALTH STRATEGIC INITIATIVES

COMMONWEALTH STRATEGIC INITIATIVES

Strategy at the state level	
1.	Improve the customer IT experience
2.	Cybersecurity for VITA, enterprise customers and the whole Commonwealth
3.	Power the COV transformation with enterprise technology solutions
4.	Drive efficiency to provide higher value by streamlining operations
5.	Apply smart governance to help customers succeed

TOP 15 AGENCIES SPEND

In FY22, with independent agencies & higher education agencies removed, the top 15 executive branch agencies spent 86% of IT dollars in Cardinal:

#	Agency Name	IT Spend	% change (from FY11 Top 15)	#	Agency Name	IT Spend	% change (from FY11 Top 15)
1	Dept. of Transportation	$111,007,051	47.65%	9	Dept. of Accounts	$32,732,637	N/A
2	Dept. of Social Services	$99,162,802	53.52%	10	Dept. of Housing & Community Development	$28,005,287	N/A
3	Dept. of Medical Assistance Services	$96,750,303	199.11%	11	Dept. of Taxation	$24,664,206	-11.40%
4	Dept. of Health	$64,271,708	95.11%	12	Dept. of Behavioral Health & Developmental Services	$19,473,048	N/A
5	Dept. of Corrections	$58,484,913	91.09%	13	Dept. of Juvenile Justice	$10,691,828	23.46%
6	Dept. of Motor Vehicles	$45,504,867	-6.44%	14	Dept. of Environmental Quality	$8,710,890	32.82%
7	Virginia Employment Commission	$44,441,708	N/A	15	Dept. for Aging and Rehabilitative Services	$8,225,911	N/A
8	Dept. of State Police	$34,393,964	124.31%				

NEAR-TERM ASSESSMENTS AND INITIATIVES

Near-term assessments

- MSI Model (Symbio) to assess the performance of the MSI operating model and the vendors in the towers
- Source 2 pay Application(s) to assess the applications that support core enterprise capabilities (procurement).
- COV IT Strategy (Gartner) to assess the overall IT operational and governance model.
- Cybersecurity Zero Trust (Deloitte) to assess the Commonwealth’s cybersecurity practices

Near-term operational improvements

- Complete the migration from Google to Microsoft 365 (Outlook) (currently at 50%)
- Consolidate the remote network solution (VPN) from Cisco to Global Protect (currently at 15%)
- Complete enterprise upgrades to Windows 11 and Microsoft 365
- Complete the SD-WAN network modernization project
- Modernize VITA financial and telecom enterprise management