VIRGINIA IT AGENCY

Information Technology Advisory Council (ITAC)
August 13, 2025 - 10:00 am

Agenda

Call to Order and Welcome	Chair and Staff
Rollcall	Staff
Review of Agenda	Staff
Readoption of Remote Participation Policy	Staff
Approval of Minutes	Staff
Presentations and Discussion	
Application Modernization and Six-Year Plan Update	Richard Matthews Chief Customer Experience Officer
Cybersecurity Risk Management	Michael Watson Chief Information Security Officer
Officer Elections	Joshua Heslinga Director, Legal and Legislative Services
Public Comment	Staff
Other Business	Staff
Adjourn	

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 July 2024, 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. A member with a disability shall count toward the quorum as physically present, in accordance with law.

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 July 2024, such all-virtual public meetings are limited by law to two meetings per calendar year or 50 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.

When audio-visual technology is available, a member of a public body shall, for purposes of a quorum, be considered absent from any portion of the meeting during which visual communication with the member is voluntarily disconnected or otherwise fails or during which audio communication involuntarily fails.

Requests and Minutes

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. A record of such a request should be submitted via email to itac@vita.virginia.gov. If a request is made in another manner, staff shall ensure a record exists of the request and its handling.

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 legal 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, or the member of the body is a caregiver who must provide care for a person with a disability at the time of the meeting, thereby preventing 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.

This policy was originally adopted at the ITAC meeting on August 8, 2024, and shall be reviewed and adopted once annually by recorded vote at a public meeting.

Information Technology Advisory Council (ITAC)
MINUTES – April 24, 2025 – 1:00 p.m.
The Boulders, Mary Jackson Conference Room

Call to Order and Welcome

The Information Technology Advisory Council meeting was called to order at 1p.m. Ms. Kozanas welcomed all the members. Ms. Ly called the roll.

Presiding:

Constantina Kozanas, Vice Chair

Members Present:

Adam S. Lee

Anthony T. Gitalado

Bob Osmond, CIO of the Commonwealth

Delegate Fernando "Marty" Martinez

Delegate Jackie H. Glass

Delegate Michael Feggans

Demetrios Melis on behalf of Secretary Slater

Dr. Timothy M. Tillman

Lyn McDermid, Secretary of Administration

Senator Bill DeSteph

Senator Jennifer B. Boysko

Senator Saddam A. Salim

Virtual Members:

Cherif Kane

James S. Kraemer

Ms. Kozanas, Mr. Kramer and Mr. Kane participated remotely from their primary residence due to distance.

Members Not Present:

Delegate Joshua E. Thomas

John Craft, Chair

Phea Ram

Robert Turner

Sam Nixon

Staff Present:

Dan Lewis, Project Management Center of Excellence Leader

Mike Watson, Chief Information Security Officer

Joshua Heslinga, Director, Legal and Legislative Services

Mylam Ly, Policy & Governmental Affairs Manager

Julie Chatman, Deputy Chief Information Security Officer for Finance

Review of Agenda

Ms. Ly provided an overview of the agenda.

Minutes

The December meeting minutes were displayed on the screen. Upon a motion by Senator Boysko to approve the minutes, and duly seconded by Delegate Feggans, the motion was unanimously approved through a voice vote.

Finance Agency Cyber Project

Ms. Chatman and Mr. Watson presented on Finance Agency Cyber Project, which focuses on cyber assessments across finance agencies. These finance agencies are responsible for controlling many Commonwealth financial assets. The assessment covers agencies including TAX, TRS, DOA, ABC, VALottery, VRS and Virginia529 due to their financial assets management, critical operations, and citizen impact, representing 40% of funding for the Commonwealth. Mr. Watson provided a risk environment review, initial steps, and next steps in the process.

Discussion addressed whether the assessment was informed by AP audits. It was clarified that findings are taken from any source (including third-party audits, agency audits, or VITA audits) to help with broader decision-making processes. Questions arose regarding consistent application of best practices and community outreach. In response to a question about how many state websites exist, the council was informed of an inventory of 1,500-1,600 websites recently conducted for modernization with security concerns and current web practices.

The extension of best practices to 300+ localities was discussed. Connection points to localities have controls at VITA level and efforts are underway to ensure localities have necessary resources to protect their environments. The state and local cybersecurity grant

program provides some assistance though funding is limited. It was suggested localities should first identify their biggest risks through cyber assessment.

The council noted they are using standard templates and standardized support to break down silos and suggested infrastructure checks should occur every three months rather than every five years as a strong recommendation to localities rather than a mandate.

Insights on insider threats were requested. Mistakes and bad actors were identified as the biggest threats in the industry. Mistakes are managed through drilling, training and monthly phishing tests. Finance insider threats are address through multiple authorizations, and special records flagged for access issues.

The distinction between critical data versus critical systems prioritization was explored. Operations systems that are critical receive highest investment, with access controls and detection measures in place. Planning for control failures and rapid response capabilities was emphasized.

The council noted agencies operate on air-gapped networks, making it primarily a people issue requiring awareness, automation and detection tools. Vulnerability and compliance management operates on a 30-day confirmation cycle.

Concerns were raised about single points of failure such as datacenters and power grids, with suggestions for standardization across agencies, while acknowledging differences between independent agencies. It was recommended that the next iteration should include law enforcement, finance, and election data as critical assets.

Joint Subcommittee on Cyber Risk

Mr. Watson then presented on a new joint subcommittee on cyber risk which was established in language in the biennial budget.

Twice per year, confidential briefings would be provided semi-annually by VITA and the Virginia Fusion Center, in consultation with Secretaries of Administration, Finance and Public Safety and Homeland Security. Subjects would include:

- Security incident trends
- Risk areas
- Vulnerabilities of critical systems
- Recommendations
- Cyber threat landscape in state government

Discussion focused on what information should be provided in presentations on organization cyber risk management programs. Questions were raided regarding which agencies fall under VITA and which pieces of critical infrastructure fall under VITA oversight, noting that inside or outside manipulation could be catastrophic for the Commonwealth.

The need for prioritization of funding needs was emphasized to provide appropriations councils with sufficient background information to manage the biggest risks. Suggestions included showing budget allocations to demonstrate correlation between risk and spending, justifying further expenditures, and evaluating effectiveness of current spending.

The council discussed addressing future risk considering the growing reliance on technology for citizen and operation data, and the correlation between more data and increased risk. Recommendations included sharing incidence response reports, remediation efforts, and best practices through coordination of all incident response stakeholders. Health and human services and public safety were identified as critical data sectors for future focus.

Legislative Update

Mr. Heslinga provided a legislative update on the 2025 legislative session with more than 2,300 bills introduced. See the presentation for details.

Key legislative outcomes include (see slides for details):

- ODGA integration into VITA. Chief data officer remains a gubernatorial appointee while the rest of ODGA becomes part of VITA.
- Project management center of excellence established to provide greater project management support for high-risk projects.
- Public sector AI bills failed, so EO30 regarding AI remains current state of policy and governance, with policy and technical standards on the VITA website
- Standard terms in IT contracts are addressed by an amendment to the Virginia Public Procurement Act that reduces risk and facilitates business. SWaM program bill passed but was vetoed, so that area continues to be governed by EO35.
- IT accessibility law updated and signed by governor. Broadens existing IT access act.

Application Modernization Progress Update

Mr. Lewis presented on application modernization cycle.

1. Data collection on applications used at the agency
2. Analysis of agency information in review with subject matter experts and agencies with IT strategic plan

3. Validation and agency feedback
4. 6-year ITSP submitted by agency
5. CIO review/approval
6. Share modernization needs with stakeholders
7. IT decision package development

2,552 applications were reviewed and assessed. Next steps include continuing analysis (April/May), ITSP submission, sharing application modernization analysis in July/August, and budget decision packages in August-September.

Discussion focused on evaluating competing priorities among agencies and ensuring the process isn't solely VITA-owned. Recommendations included streamlining background checkpoints to enable businesses to move faster, noting that permitting implementation across agencies with customer efficiency and end-user experience are important considerations.

Questions arose regarding agencies self-identification of applications and recommendations on the "7R's" approach, with suggestions this could be a continuous improvement process. it was noted this would be part of yearly strategic plans.

The importance of prioritizing emergency modernization needs, and non-functioning systems was emphasized when considering funding requests. The council acknowledged the value if continuity at VITA and the importance of knowledge regarding registered applications and visibility. Suggestions included creating space for agency personnel to bring forward applications such as live coding and AI, potentially expanding the governor's transformation office to focus on citizen-centric innovation and incorporating change management at the agency level.

Project Management Center of Excellence Update

Mr. Lewis then presented on the project management center of excellence (PMCoE). The goal is to improve planning with agencies, contracts, and contract delivery. Risk management and organizational change management determine program success. VITA is involved in 79-80% of projects, primarily high-risk projects (not necessarily the more expensive). Efforts focus on solidifying reporting from vendor management perspective, bringing vendor grading to analysis, enhancing deliverable and milestone requirements, using project delivery advisory, and improving training and project management staffing.

Current state assessment data shows 72% of spend goes to 11 largest projects. Effective statues, culture and relationship development are in place, but opportunities exist in:

- Inconsistent project planning
- Contracting and requirement gathering
- Resource limitations (skills and staffing)
- Inadequate metrics and reporting

The development timeline includes the PMCoE in the FY 25 Q4 with the launch of advisory services in FY26 Q1 and Operational status in FY26 Q2.

Discussion addressed the use of PMBOK and earned value management systems and the importance of PMI certifications for project managers, The commonwealth tool “Planview” was noted as having capabilities beyond current usage.

Questions arose regarding inclusion of 508 compliance, SEC501, AI and cloud considerations in project management, with emphasis on changing culture to incorporate these elements. Report cards and grading matrices were referenced as potential models. Further discussion about prioritizing deliver of PMCoE critical functionality was suggested for follow-up.

Public Comment Period

There were no public comments.

Other Business

Mr. Heslinga discussed the election of Chair and Vice Chair, which will occur during the next meeting. Members interested in serving or in nominating someone else should email staff at ITAC@vita.virginia.gov.

Adjourn

At 2:50 p.m., the meeting was adjourned after a motion was made by Senator Boysko and seconded by Senator Salim.

VIRGINIA IT AGENCY

Information Technology Advisory Council (ITAC) Meeting

VITA staff

August 13, 2025

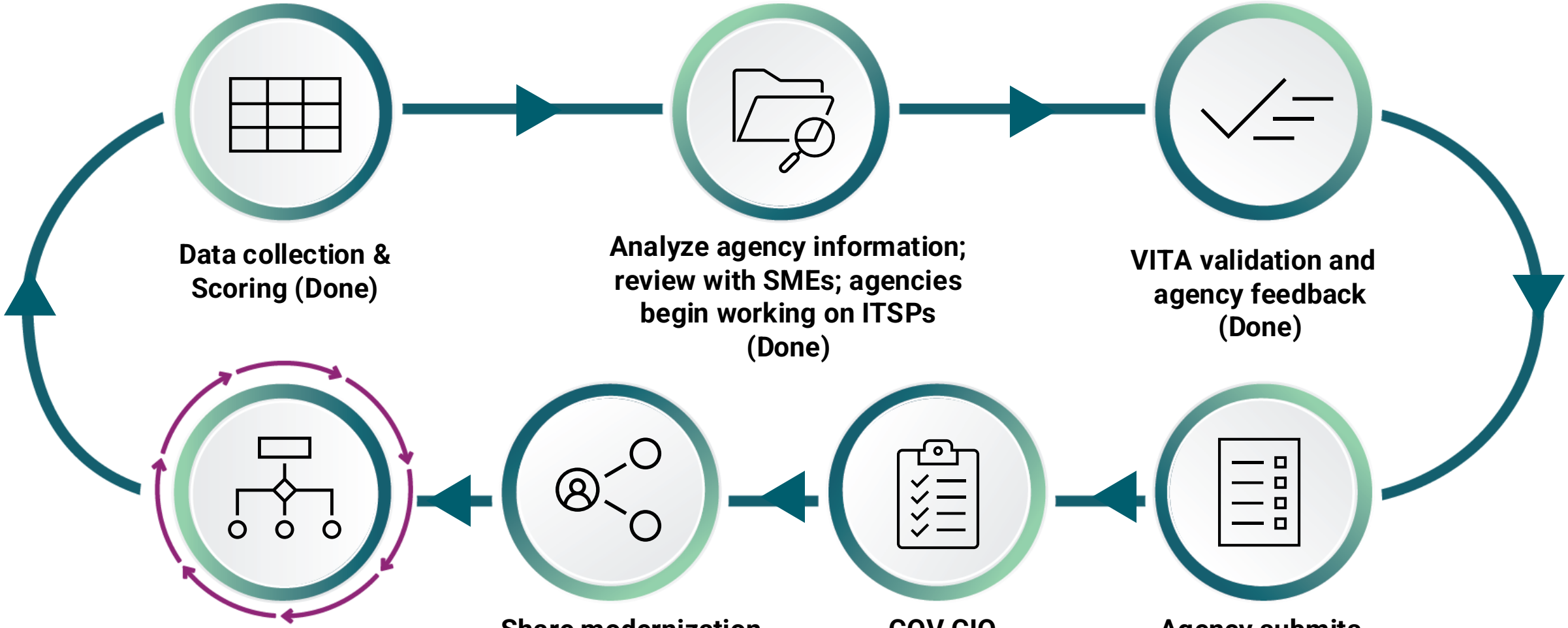
Agenda

Readoption of Remote Participation Policy	Staff
Approval of minutes	Staff
Application modernization and six-year plan update	Richard Matthews Chief Customer Experience Officer
Cybersecurity risk management: • Public briefing • Joint Subcommittee on Cyber Risk follow-up • State and Local Cybersecurity Grant Program update	Michael Watson Chief Information Security Officer
Officer Elections	Staff
Public Comment	
Other Business	Staff
Adjourn	

Application modernization and six-year plan update

Richard Matthews
Chief Customer Experience Officer

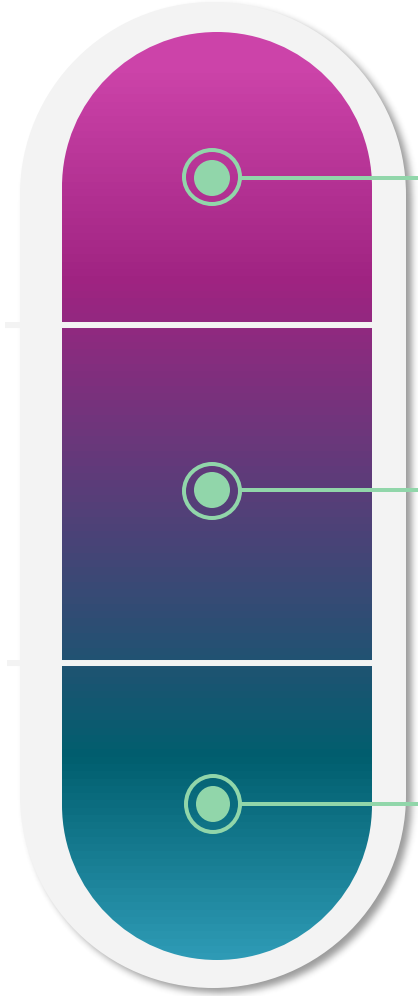
FY26 Application Modernization Cycle (As of August 2025)



Comprehensive Application Assessment Scoring Results

2552

Total number of apps



Acute need
344 applications must be urgently addressed (part of 6Y plan)

Impending need
521 applications will need to be addressed later (part of 6Y plan)

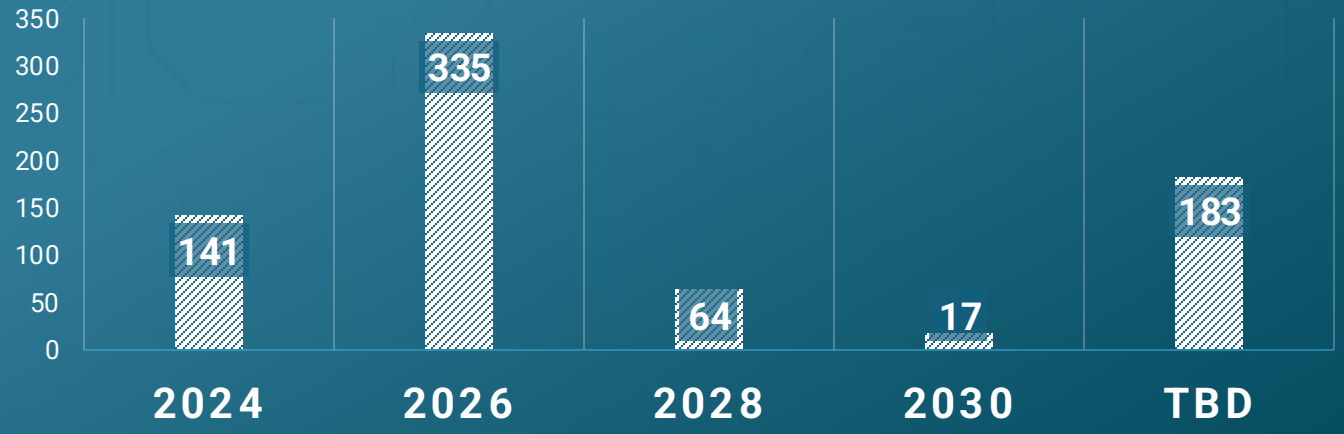
Maintain (Tolerate/Keep)
1687 applications are in relatively good shape for now

Commonwealth Applications Roadmap By The Numbers

865 Acute and impending needs from the comprehensive assessment

740 In scope applications by biennium

Application roadmap by biennium (start)



Key findings from agency plans (ITSP)

- 141 applications are already being addressed in FY24/25
- 399 applications are planned for FY26/27 and FY28/29
- 200 applications are unsolutioned or planned post FY30 and need more work to address earlier

VIRGINIA IT AGENCY

vita.virginia.gov

What is the plan to address the modernization need?

The SYP (Six Year Plan) Consists of Multiple Strategies. Some applications are already being:

- Addressed through existing Commonwealth projects in progress – Active Project Portfolio
- Planned through the Commonwealth project planning process – Planned Project Portfolio
- Planned and addressed (notably smaller projects under $250K) within existing agency IT Strategy Plans (ITSPs) as previously noted

In collaboration with the agencies, VITA is engaged to identify opportunities to consolidate and assist their efforts through enterprise solutions. Our team is offering:

- Technical advisory services for analysis, architecture, and development
- Platforms for rapid development (Microsoft Power, Box, Docusign, and more)
- Enterprise solutions for shared and common needs (developed software) via an application store and as enterprise solutions
- Business process automation and artificial intelligence

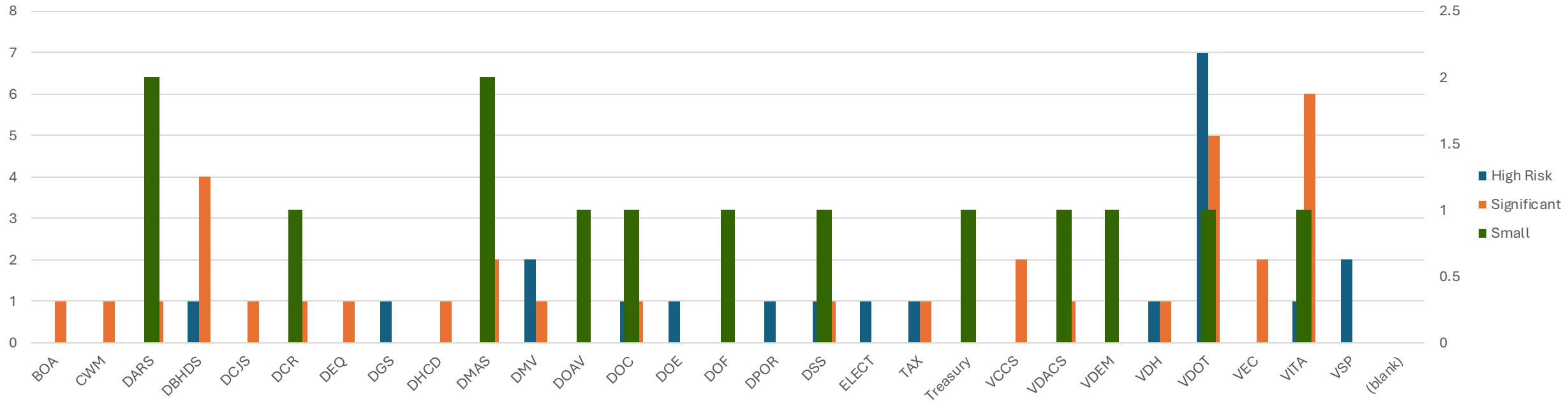
Discussion:

1. **There exists a significant amount of application modernization work that agencies plan to address in FY26/27. How can we better help our agencies?**
2. **Agencies will require additional capacity, beyond what they currently have, to remediate the identified applications. How do we get them that help?**

The active project portfolio represents a significant investment

65 Active projects with a **total value of $683.5M** that address replacing or improving current applications

- 21 Projects are High Risk ($5M+) ($589M)
- 34 Projects are Significant ($1M - $5M)
- 14 Projects are smaller (Under $1M)

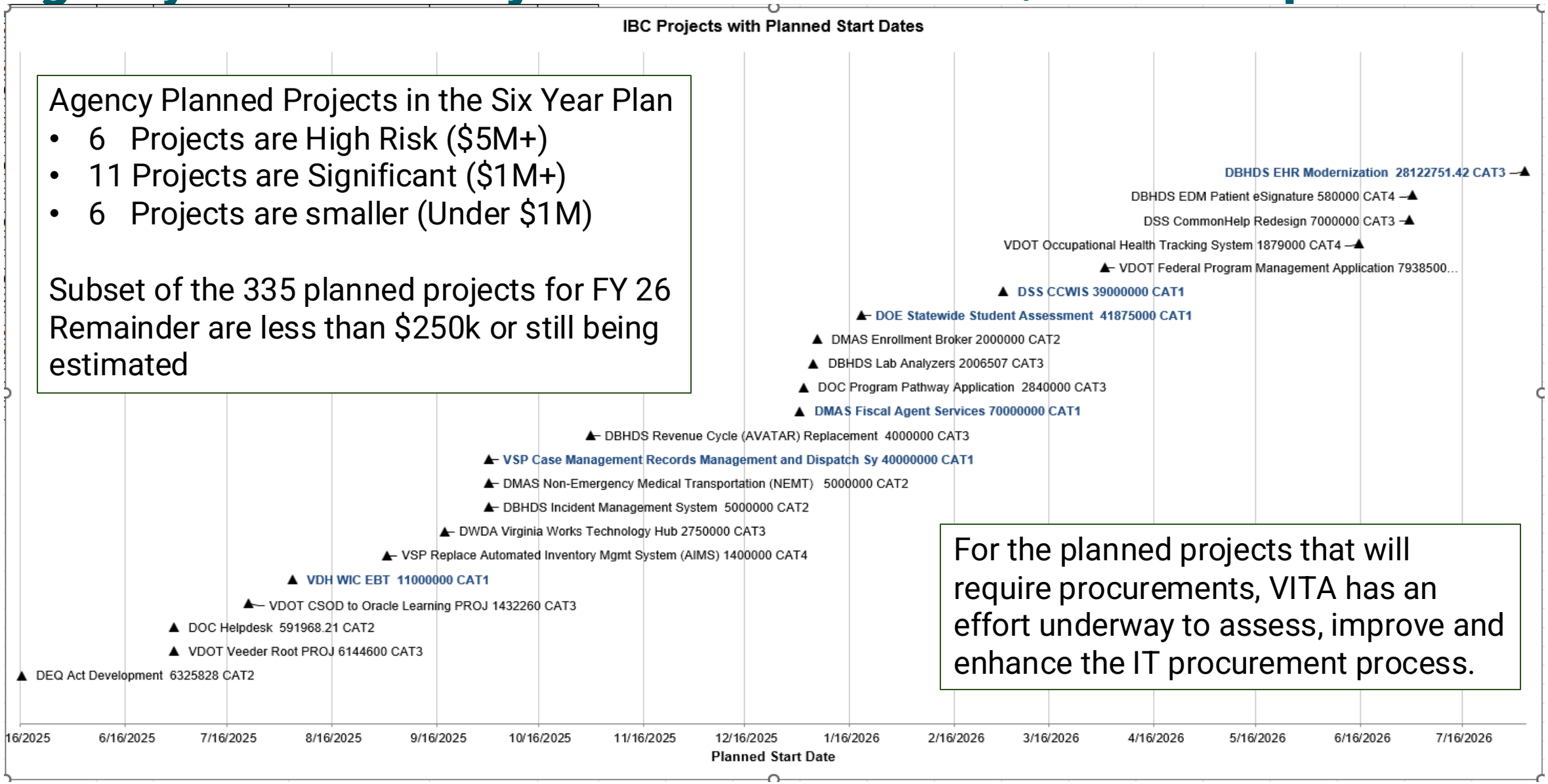


Agency Planned Projects in SYP – Over $250K Scope

Agency Planned Projects in the Six Year Plan

- 6 Projects are High Risk ($5M+)
- 11 Projects are Significant ($1M+)
- 6 Projects are smaller (Under $1M)

Subset of the 335 planned projects for FY 26
Remainder are less than $250k or still being estimated



For the planned projects that will require procurements, VITA has an effort underway to assess, improve and enhance the IT procurement process.

Enterprise and Cloud Technology Solutions Will Help

Complements the newly formed Project Management Center of Excellence (PMCOE) that supports the delivery of the Commonwealth's portfolio of high-risk IT projects.

Provides enterprise and cloud advisory services to deploy enterprise technology skills and capabilities (architecture, analysis, development and testing) to help agencies remediate or replace applications.

Offers staffing/resources, consolidated enterprise software, platform technologies, and artificial intelligence capabilities on COV hosted platforms.

Builds and supports technology communities of practice so that agencies can learn from each other.

Targeted at the unmet needs in the agencies including the 200 applications without solutions.

Enterprise and Cloud Technology Solution Offerings

Enterprise and cloud solutions

COV-wide Applications/Advisory

- Analyze application portfolios and design modernization roadmaps
- Identify opportunities for consolidation and shared services
- Build cloud migration playbooks and FinOps framework
- Implement secure, scalable enterprise and cloud software

1

3

Business Platform Solutions

Accelerating with modern tools

- Deploy modern low-code/no-code platforms (Power Platform, RPA, Box ECM, Adobe)
- Communities of Practice

Commonwealth AppStore:
Reusable apps for faster time-to-value

2

AI-Driven Innovation

Prototyping and Operating AI Initiatives

- AI powered search and document summarization
- Conversational AI and virtual assistants for enhanced user experience

5

- **Development Acceleration:** GitHub Copilot for code generation and legacy code remediation

4

Discussion:

Any additional feedback/thoughts on how we can improve the six-year application modernization planning process?

Cybersecurity risk management

Michael Watson
Chief Information Security Officer

Cyber landscape

Cyber threats: Common cyber threat actors and cybercriminal tactics and techniques

- **Social Engineering**
  - Social engineering against Clorox Corporation Help Desk
- **Compromise the Technology Supply Chain**
  - Large scale compromise of telecommunication company data (Salt Typhoon)
- **AI Powered Cyberattack Campaigns**
  - AI being used to create convincing phishing emails and voice calls
  - Employee impersonation from foreign adversaries
- **Ransomware-as-a-service (RaaS) Operations**
  - Targeting smaller organizations (i.e. localities)
  - Leverages remote management tools for persistent access
- **Exploitation of Control Systems and IoT Devices**
  - Attackers exploit security weaknesses in IoT devices to gain entry into critical infrastructure

Cyber landscape

Cyber Threats: State-sponsored cyber threat actors

State-sponsored cybercriminals are individuals or groups who engage in cyberattacks, espionage, or other malicious activities on behalf of a nation-state or government entity. These actors are often highly skilled and well-resourced, benefiting from the financial and technological support of their sponsoring government.

- **China**
  - **APT 41** (AKA: Double Dragon, Barium, Winnti, Wicked Panda, Wicked Spider, TG-2633, Bronze Atlas, Red Kelpie)
    - SharePoint compromise of the U.S. National Security Administration (NNSA)
- **Iran**
  - **APT 34** (AKA: OilRig, Earth Simnavaz, and Helix Kitten)
    - Utilized spear phishing emails to deliver custom malware disguised as PDF files to enable data exfiltration
- **Russia**
  - **APT 28** (AKA: Fancy Bear, Pawn Storm, the Sednit Gang and Sofacy)
    - Conducted cyberattack targeting French government agencies involved in planning the 2024 Paris Olympic Games
- **North Korea**
  - **APT 38** (AKA: Lazarus Group)
    - $1.5 billion theft from the Bybit cryptocurrency exchange

Trends of Cyber Incidents

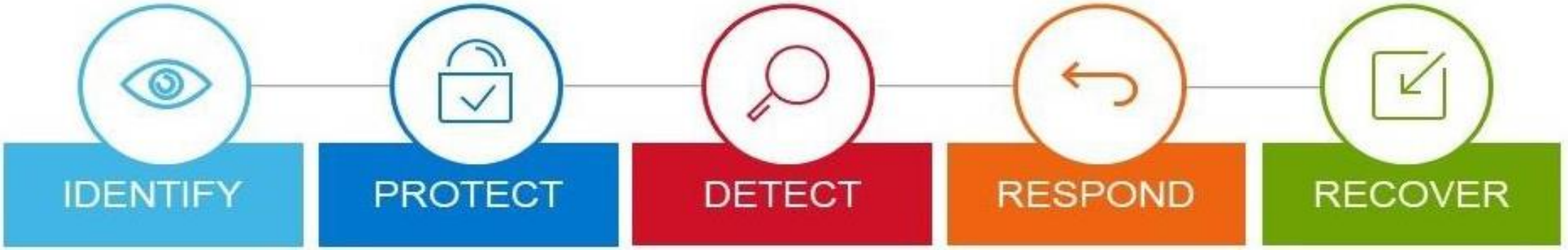
2024 MS-ISAC National Cybersecurity Review State, Local, Tribal, and Territorial (SLTT)

		2024 Selection rate	2023 Selection rate	2022 Selection rate	2021 Selection rate
1	Lack of sufficient funding	73%	70%	72%	73%
2	Increasing sophistication of threats	65%	64%	63%	63%
3	Emerging technologies	49%	46%	40%	38%
4	Lack of documented processes	48%	44%	43%	39%
5	Inadequate availability of cybersecurity professionals	33%	35%	38%	37%

Virginia security program challenges mirror national patterns reported by CISA

- Poor cyber hygiene
- Password reuse
- System misconfigurations
- Poor patch management
- Privileged account misuse
- Phishing / Business Email Compromise (BEC)

NIST Cybersecurity Framework



Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Virginia roles and responsibilities

Virginia Information Technologies Agency

- Lead and manage cyber responses involving Executive Branch
- Coordinate with VFC
- Serve as technical advisor on cyber response task force
- Identify and establish cyber recovery protocols
- Develop incident specific plans to expedite recovery

Virginia Department of Emergency Management

- Serve as technical advisor on cyber response task force
- Activate COVEOP if appropriate

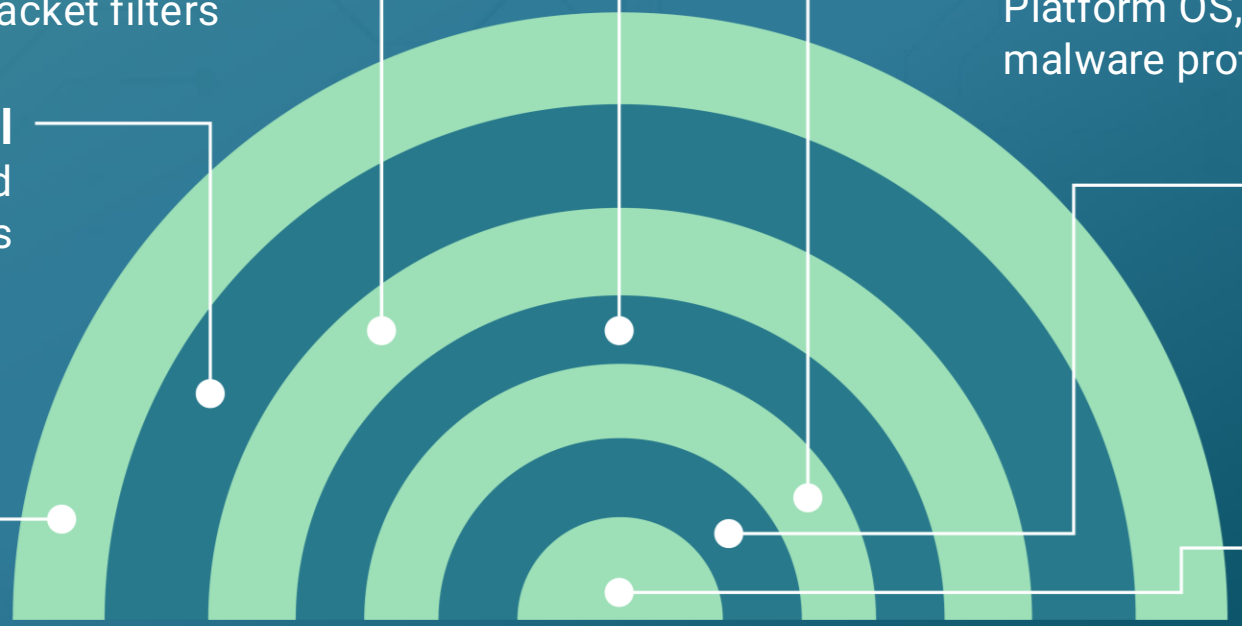
Virginia State Police and Virginia Fusion Center

- Initial contact, triage for cyber incident
- Lead agency for criminal investigation
- Lead response taskforce
- Coordinate notification process and disseminate information on cyber attack

Virginia Department of Military Affairs

- Serve as technical advisor on cyber response task force
- Provide incident response and recovery resources
- Vulnerability assessment service for localities

Current threat defense model: defense in depth



Internal network
Firewall, intrusion detection and encryption

Perimeter
Firewall, VPN and packet filters

Physical
Locks, fences and security guards

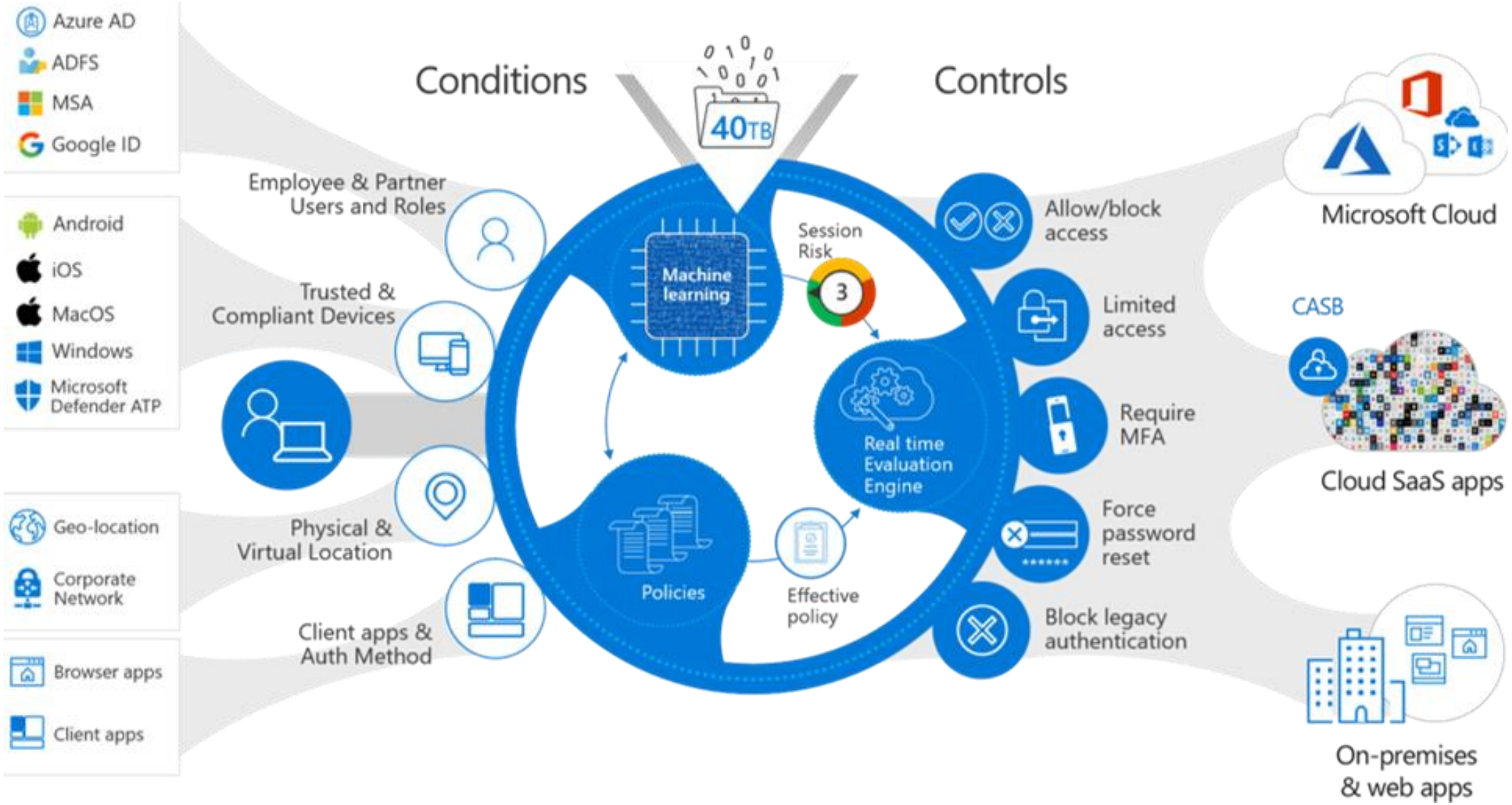
Policies, procedures and awareness
Passwords, policies and data classification

Host
Platform OS, patches and malware protection

App
SSO, authentication and authorization

Data
Database, content and message security

Future Threat Defense Model: Trust-Based



Cybersecurity Projects Completed

- Released data classification standard (SEC540)
- MFA was updated to OKTA Verify, eliminating use of SMS for authentication
- Security services migration underway with the roll out Splunk to agencies to facilitate automation and incident response orchestration
- Upgrading capabilities to identify and manage attack surface management (Nucleus, Acunetix, Axonius)
- MSS Contract in progress – will be awarded in 2025
- Additional security technology included to support our public cloud datacenters (cloud-native application protection platform - Cloud Native Application Protection Platform (CNAPP)
- Finance Cyber Risk Program continues cyber risk assessments for Finance Agencies and will expand to all agencies once that phase is complete
- State and Local Cyber Grant Program (see later slide)

CISO Cybersecurity Scope of Services

Policies, standards and governance, education and outreach (most of state)

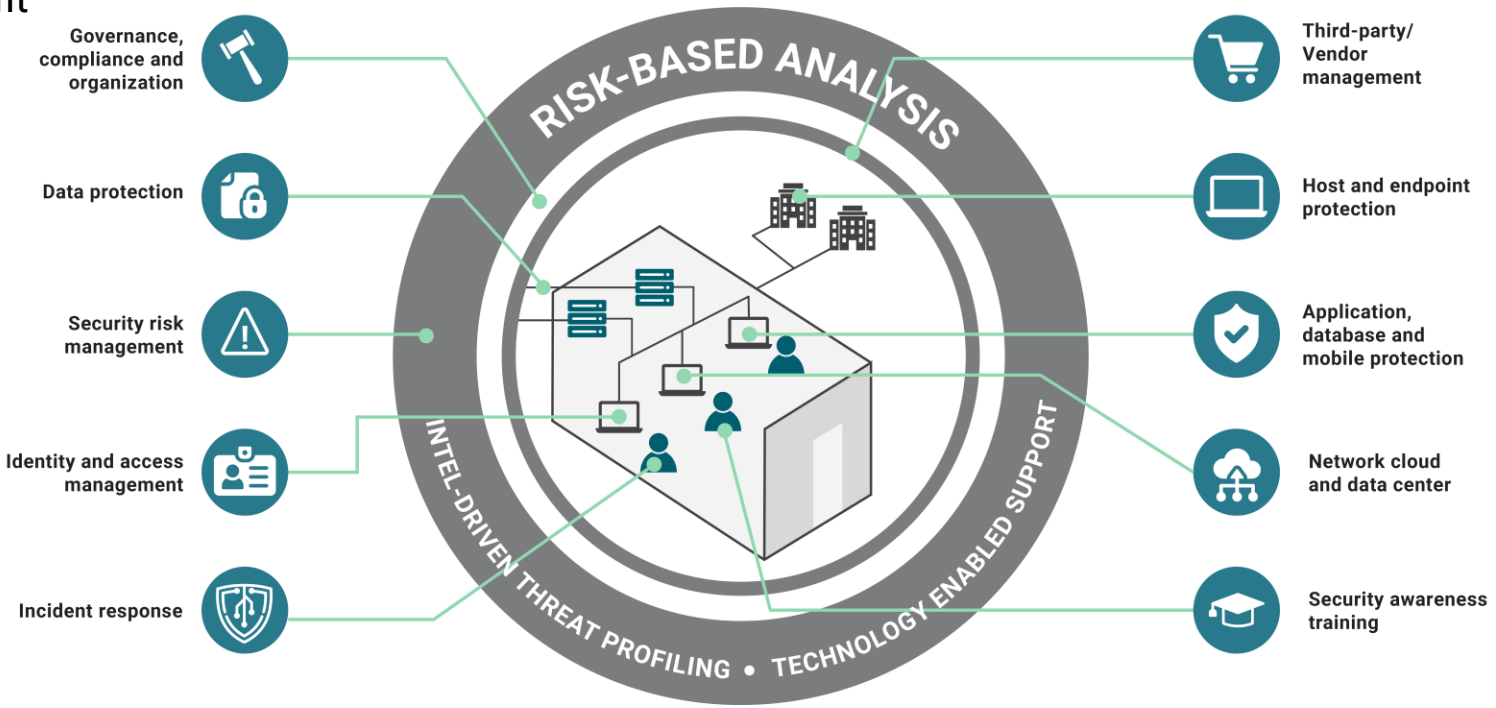
•Strong standards and cybersecurity framework built from federal standards (NIST)
•COV KnowBe4 Training

IT risk management program (65 agencies)

•Third party risk assessment & monitoring (COV RAMP for ~ 482 cloud applications)
•Input into cyber insurance policies

Threat management (65 agencies)

•Data protection and security breach containment
•Vulnerability Management
•Cyberattack Monitoring & Incident Response



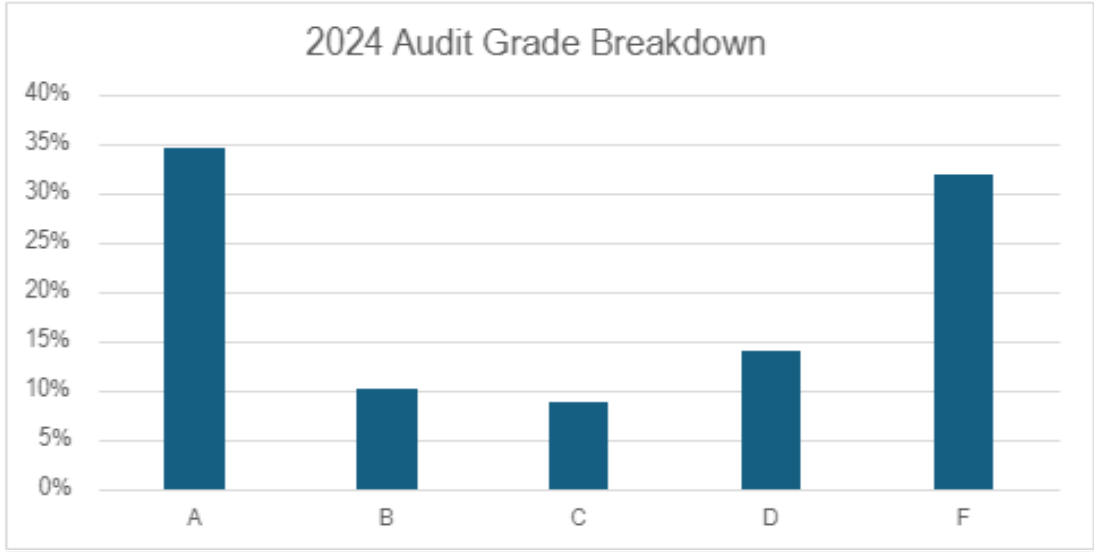
Infrastructure managed security (65 agencies)

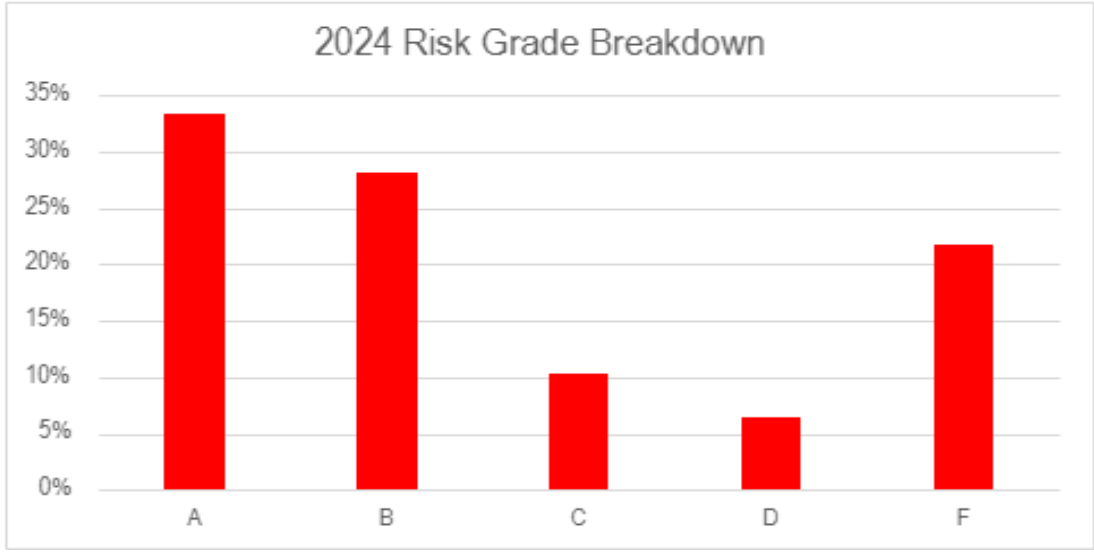
•End point protection, server hardening, firewall management, network traffic analysis, host intrusion, scanning, group policies, application filters, security operations center, etc.

Cybersecurity Program Status in 2024

Agencies Need More Help

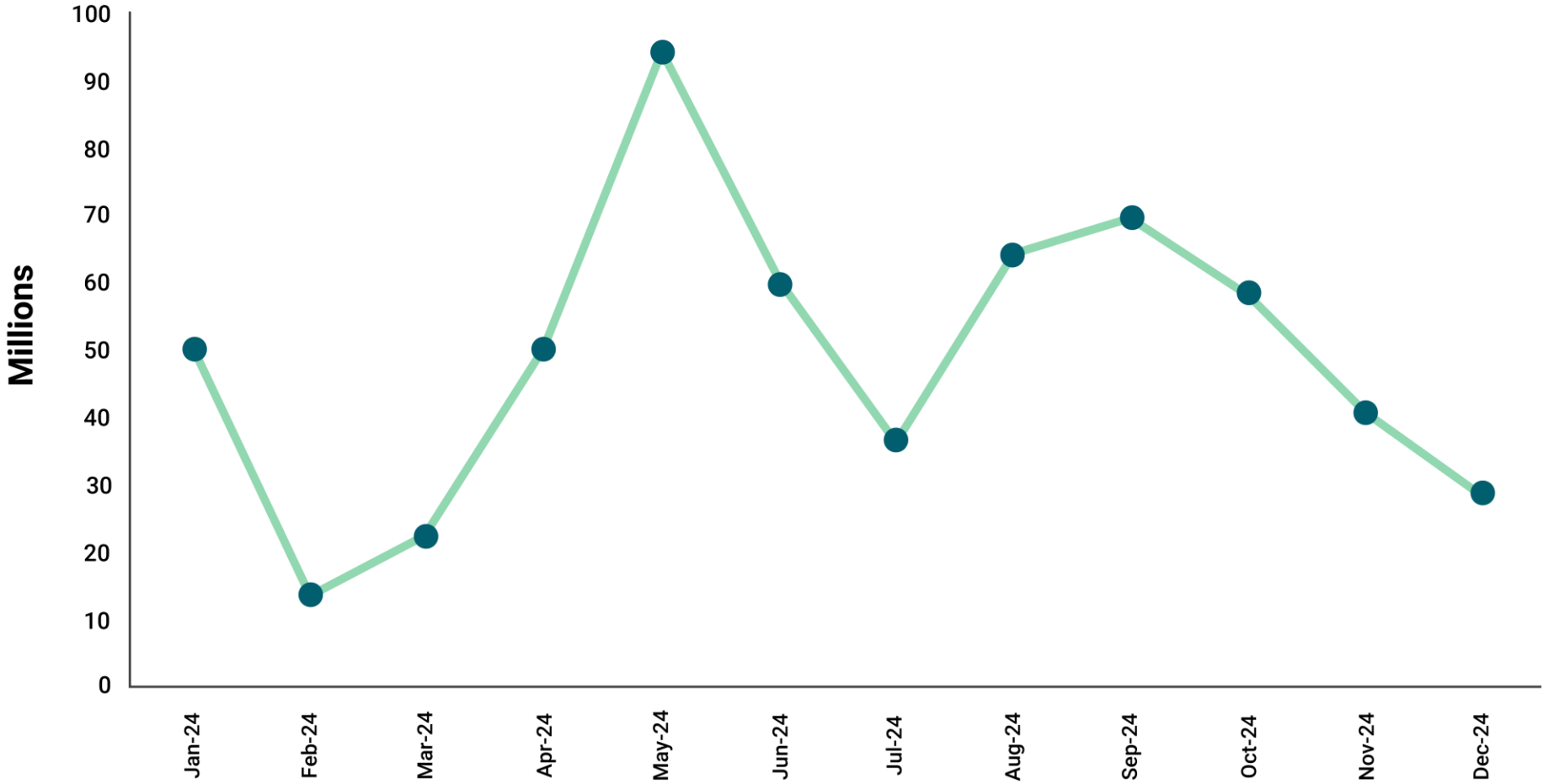
- VITA leads a statewide cybersecurity audit program (VITA + third parties) for the 65 agencies
- Foundational security program measurements
  - Identifies if adequate cybersecurity program exists at agencies based on agency audits and risk assessments
- Indicator about organization's understanding of cybersecurity risk
  - Agencies with a C or below typically struggle to understand the impact of a cybersecurity incident





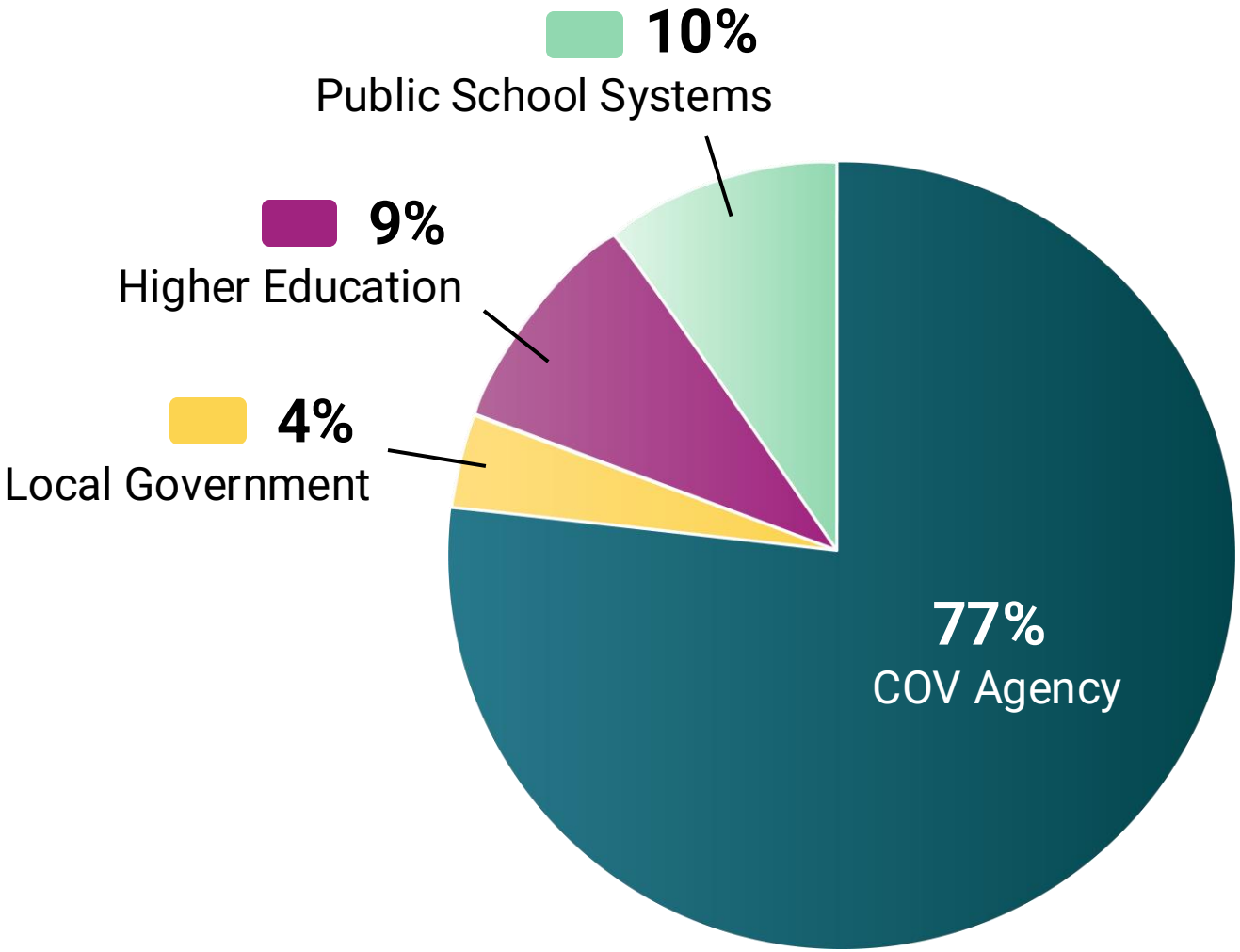
591,110,270 Attack Attempts on COV Networks

2024



Whole-of-State Security Events by Category

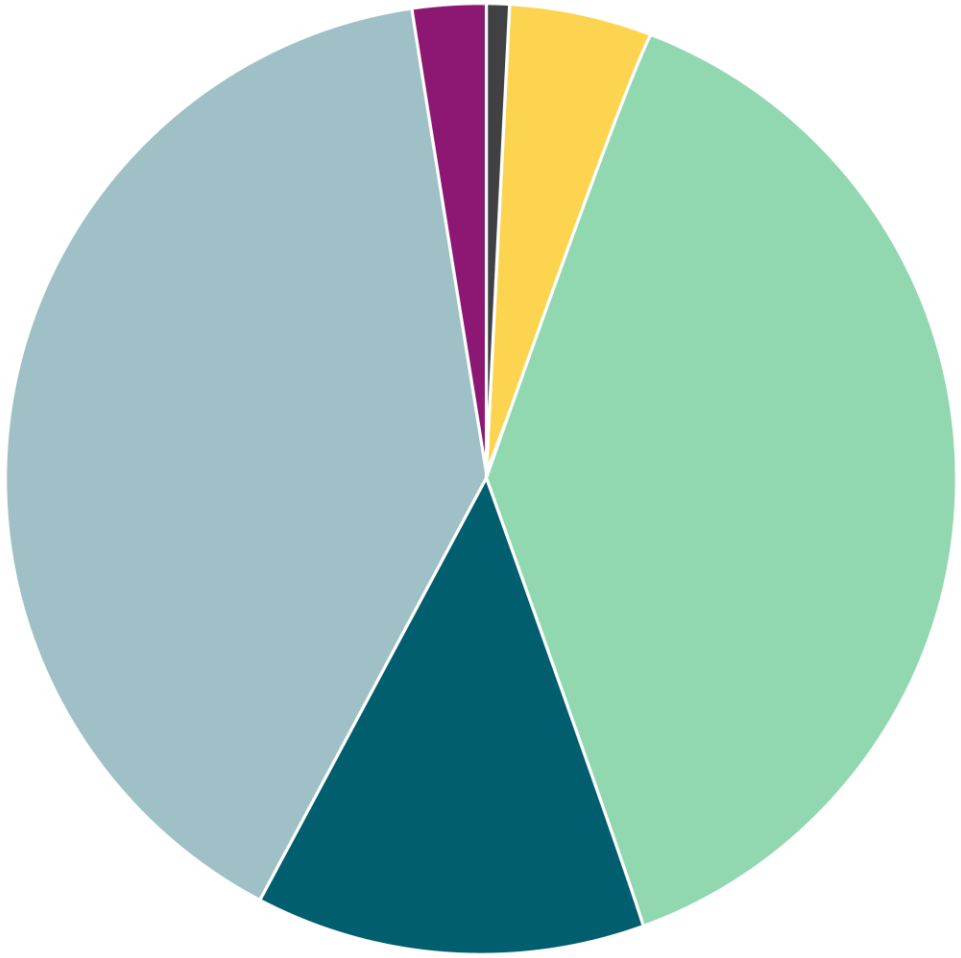
From 2024



Virginia Code § 2.2-5514 requires all public bodies to report cyber incidents to the VFC within 24 hours of discovery

- Reports Since Legislation: 517
- Entities need to do a better job of reporting events
- VITA plans to promote collaboration

VITA Security Incidents by Category (P1 and P2)
Year 2024 or 2025?



Definitions:

- P1 – unauthorized access to the environment
- P2 – attempted access that was blocked

- Information disclosure- **39.80%**
- Physical loss - **38.98%**
- Social engineering- **13.06%**
- Malware - **4.90%**
- Unauthorized access- **2.45%**
- Denial of service - **0.82%**

Total COV = 490 (only one P1)

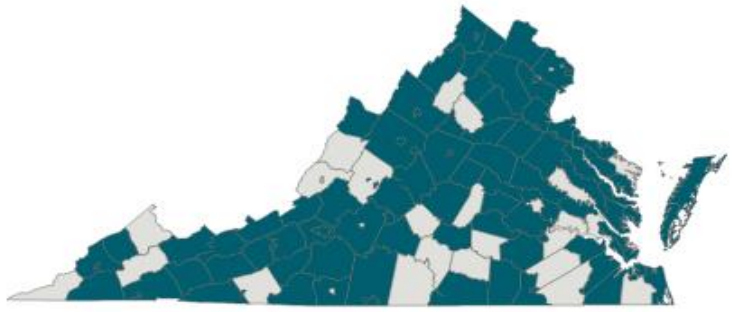
Whole of State Cybersecurity: State and Local Cyber Grant Program

VIRGINIA IT AGENCY

vita.virginia.gov

SLCGP Update – Locality Grants

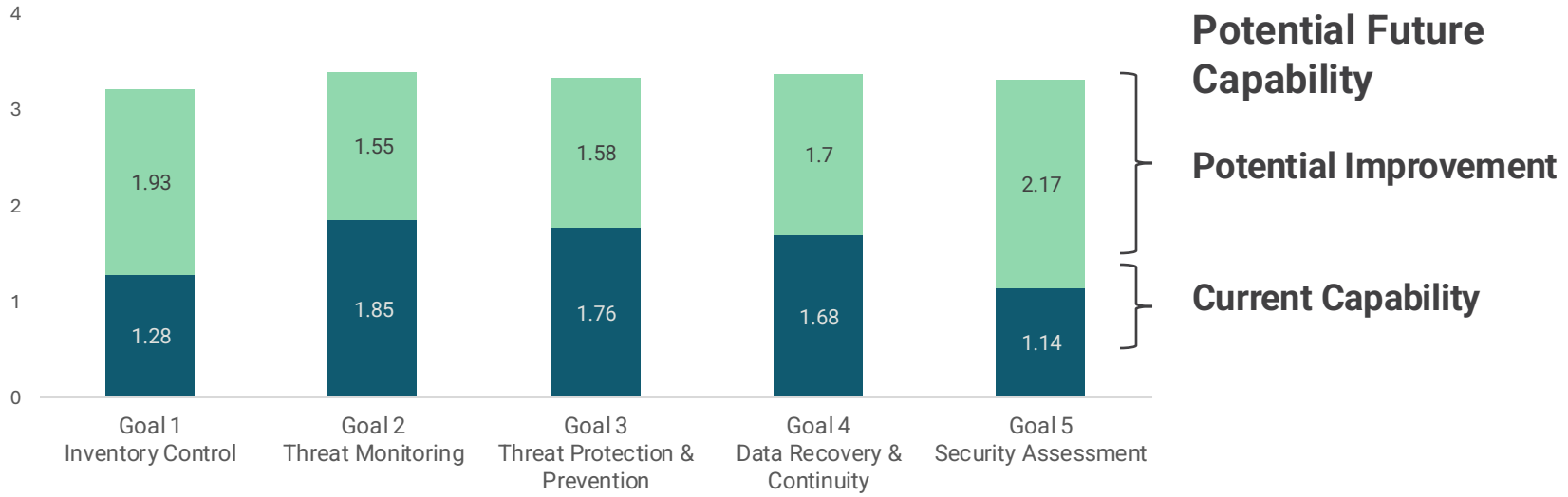
Cybersecurity Plan Capability Assessment



159 local government entity participants

- 42% local government (cities, counties, towns)
- 43% public school districts
- 15% other (tribal government, authorities, etc.)
- 62% rural participants

Analysis of capability improvements across participants identified focus areas for subsequent project funding



SLCGP Update – Locality Grants

Phase 2 Projects

Focus areas

- Vulnerability management
- Secure remote network access
- Asset inventory including hardware and software
- Data inventory including data sensitivity analysis
- Endpoint detection and response for all workstations and servers
- Firewalls for ingress/egress points, end point devices and web applications

Project execution options

- Designed to support a range of locality size and complexity
- Able to choose an option per focus area
- Ranges from purchase of additional licenses through full-service support

Application evaluation

- Must meet requirements associated with organization eligibility, capability assessment findings, alignment with focus areas
- Priority given to rural areas until 25% funding requirement met
- Focused on maximizing improvements across the state

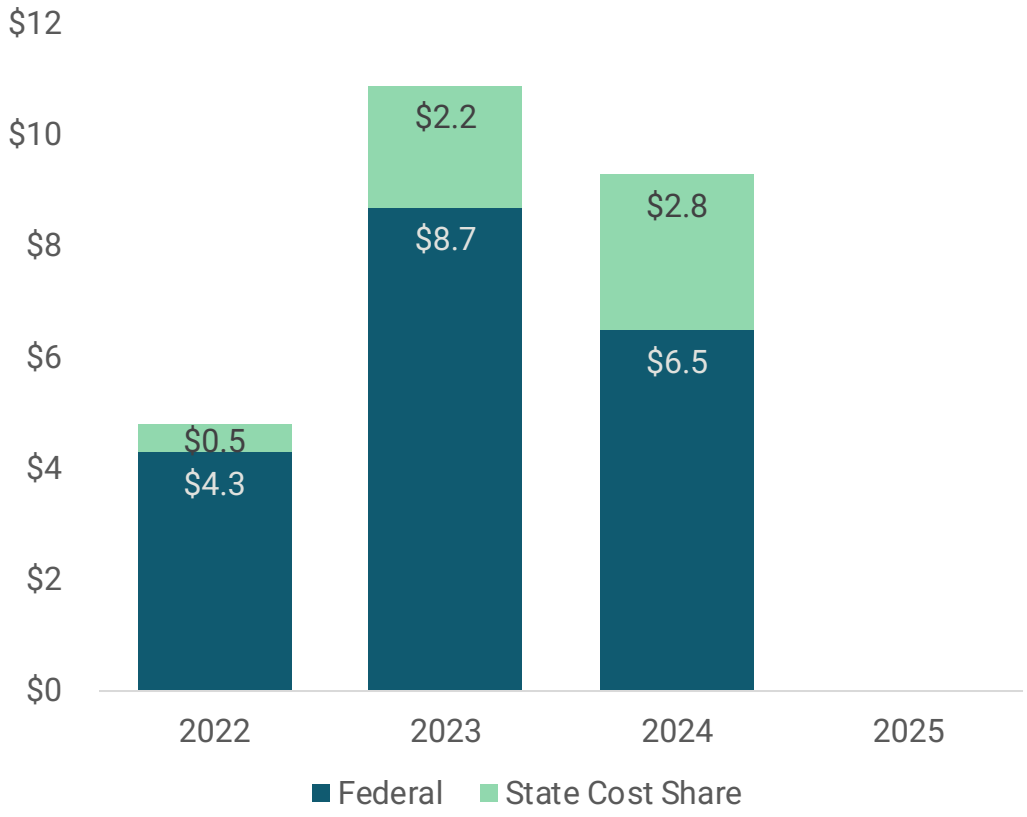
Status

- Locality applications – complete
- Solution selection, negotiation – underway
- Application approval – underway
- Local project execution – planned to begin September 2025

Funding and Allocations

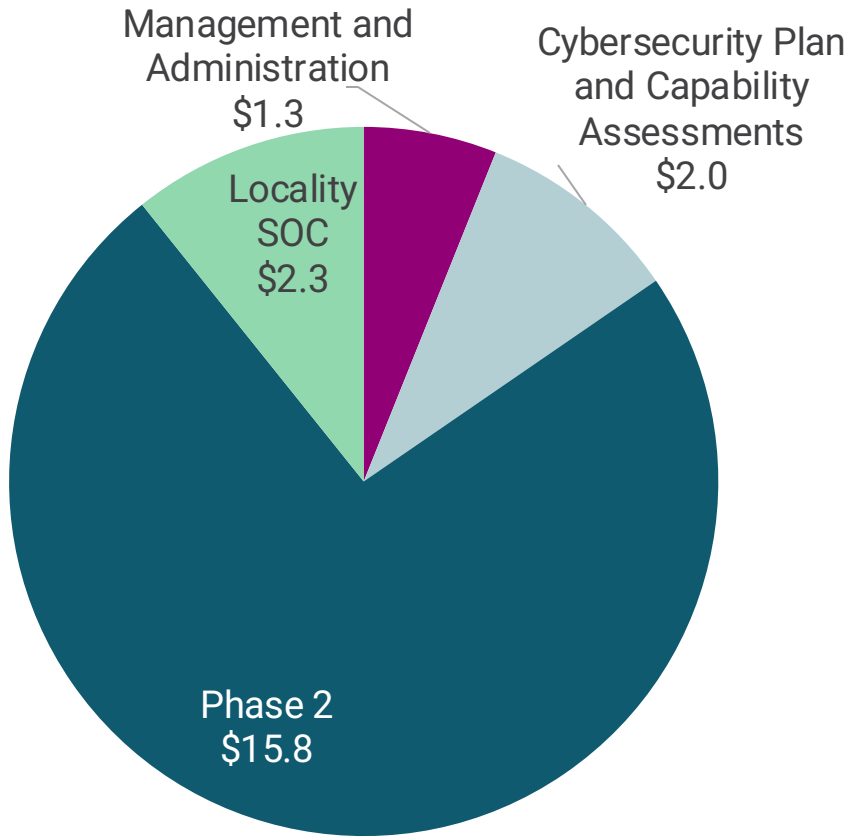
Total awarded to date: $25 million

State cost share **fully** covered through General Assembly appropriated funds



VCPC approved allocations as of 8/1/2025

In millions



Risks and migration

Current Risks

- Federal funding uncertainty may affect future rounds
- Execution delays possible due to vendor timelines and staffing constrains
- Varying local capability levels may impact project outcomes

Mitigation Strategies

- Prioritize high-impact, low-complexity projects
- Maintain flexibility with funding in response to federal guidance
- Provide technical assistance and oversight during execution
- Continual coordination with localities to monitor progress and adjust plans
- National organizations like NASCIO are lobbying Congress for continued funding and support

Discussion:

1. **What are some additional best practices that VITA can do to best enhance our cybersecurity program?**

2. **What information would be helpful for you to see from localities to inform future policymaking about the state and local cyber security relationship and services?**

3. **What can we do to encourage local entities to report their events?**

Agenda

✓ **Readoption of Remote Participation Policy**	Staff
✓ **Approval of minutes**	Staff
✓ **Application modernization and six-year plan update**	Richard Matthews Chief Customer Experience Officer
✓ **Cybersecurity risk management:** • Public briefing • Joint Subcommittee on Cyber Risk follow-up • State and Local Cybersecurity Grant Program update	Michael Watson Chief Information Security Officer
Officer Elections	Staff
Public Comment	
Other Business	Staff
Adjourn	

Thank You!