WELCOME TO THE May ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

May 14, 2025

VIRGINIA
IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Kendra Burgess/VITA
Implementing CIS IG2: Tales from the Crypt	Randy Marchany/Virginia Tech
Introduction to Enterprise and Security Architecture	Chris Williams/VITA
Phishing Reporting and Phishing Simulation Update	Matthew Umphlet/VITA
TLS 1.0/1.1 Remediation	John Del Grosso/VITA
Upcoming Events and Announcements	Kendra Burgess/VITA
Adjourn	

Implementing CIS IG2: Tales from the Crypt

Randy Marchany

Virginia Tech IT Security Office and Lab

marchany@vt.edu

https://security.vt.edu

If we don't write the rules, our adversaries will write our future.*

VIRGINIA TECH BUSINESS PROCESS IT SECURITY MODELS

Administrative

- Process that runs the university
- Security: **CORPORATE**

Academic / Instructional

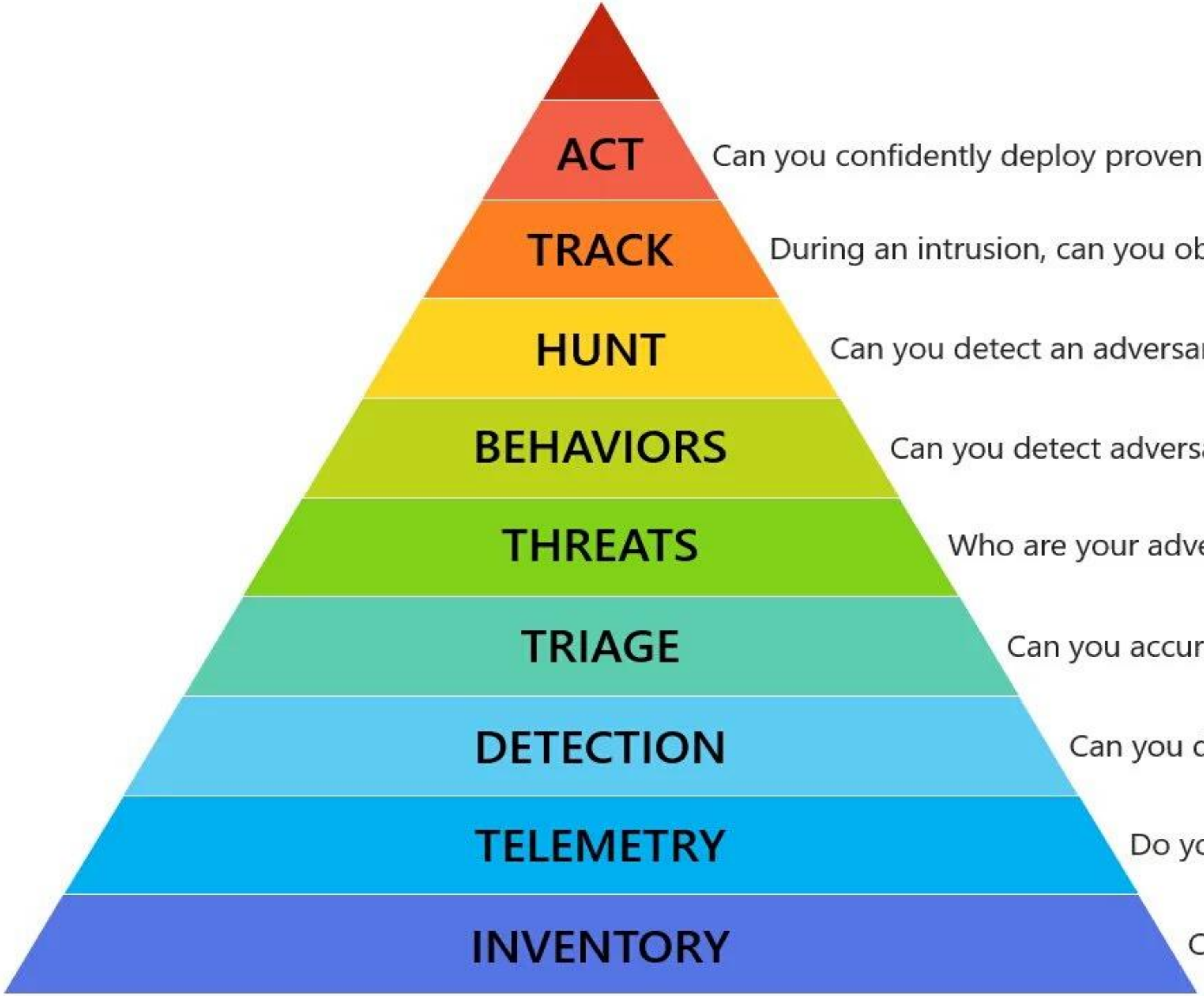
- Process that supports teaching/learning
- Security: **ISP***

*Internet Service Provider

Research

- Process that supports VT Research
- Security: **HYBRID**

Challenge: create overall security architecture blending these 3 business process IT security requirements



ACT Can you confidently deploy proven countermeasures to evict and recover?

TRACK During an intrusion, can you observe adversary activity in real-time?

HUNT Can you detect an adversary that is already embedded?

BEHAVIORS Can you detect adversary activity within your environment?

THREATS Who are your adversaries? What are their capabilities?

TRIAGE Can you accurately classify detection results?

DETECTION Can you detect unauthorized activity?

TELEMETRY Do you have visibility across your assets?

INVENTORY Can you name the assets you are defending?

Source: https://holisticinfosec.blogspot.com/2016/12/the-dfir-hierarchy-of-needs-critical.html
Figure source: https://github.com/swannman/ircapabilities

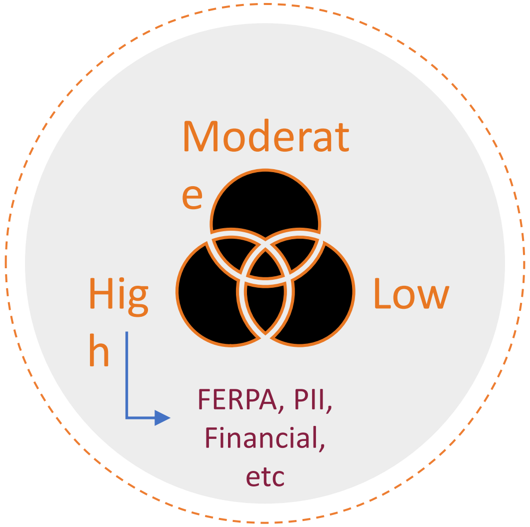
CONTROL 01	Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02	Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03	Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04	Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05	Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06	Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07	Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08	Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09	Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10	Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11	Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12	Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13	Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14	Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15	Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16	Application Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17	Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18	Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

Elevate VT to CIS v8 IG2

Goal:

Compliance with the Center for Internet Security (CIS) Critical Security Controls version 8, Implementation Group 2 (IG2) safeguards for units, systems, and applications that handle, process, or store sensitive (“high” and “moderate” risk) data across Virginia Tech.

Phase I - IT Risk Assessments



Asset Inventory

Inventory of unit's hosts and "in-house" developed applications

Risk Classification

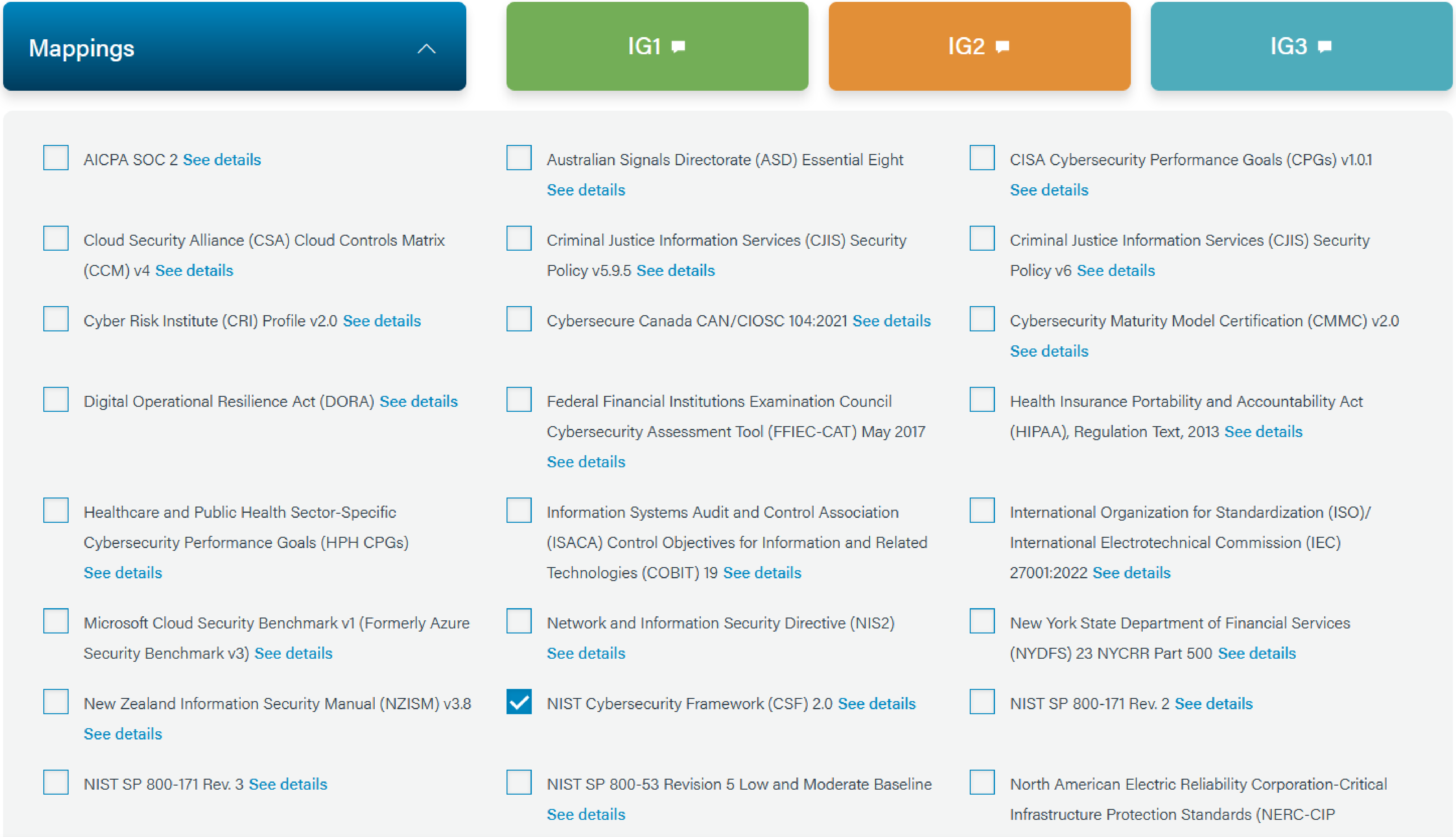
Determine data handled by assets and classify risk level accordingly

Assessment Survey

Complete questionnaire(s) based on CIS v8 IG2 controls

Due **6/30/2023**
3/1/2025

Due **10/31/2023**
6/1/2025



Mappings

IG1 IG2 IG3

□ AICPA SOC 2 See details

□ Australian Signals Directorate (ASD) Essential Eight See details

□ CISA Cybersecurity Performance Goals (CPGs) v1.0.1 See details

□ Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v4 See details

□ Criminal Justice Information Services (CJIS) Security Policy v5.9.5 See details

□ Criminal Justice Information Services (CJIS) Security Policy v6 See details

□ Cyber Risk Institute (CRI) Profile v2.0 See details

□ Cybersecure Canada CAN/CIOSC 104:2021 See details

□ Cybersecurity Maturity Model Certification (CMMC) v2.0 See details

□ Digital Operational Resilience Act (DORA) See details

□ Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC-CAT) May 2017 See details

□ Health Insurance Portability and Accountability Act (HIPAA), Regulation Text, 2013 See details

□ Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (HPH CPGs) See details

□ Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technologies (COBIT) 19 See details

□ International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001:2022 See details

□ Microsoft Cloud Security Benchmark v1 (Formerly Azure Security Benchmark v3) See details

□ Network and Information Security Directive (NIS2) See details

□ New York State Department of Financial Services (NYDFS) 23 NYCRR Part 500 See details

□ New Zealand Information Security Manual (NZISM) v3.8 See details

☑ NIST Cybersecurity Framework (CSF) 2.0 See details

□ NIST SP 800-171 Rev. 2 See details

□ NIST SP 800-171 Rev. 3 See details

□ NIST SP 800-53 Revision 5 Low and Moderate Baseline See details

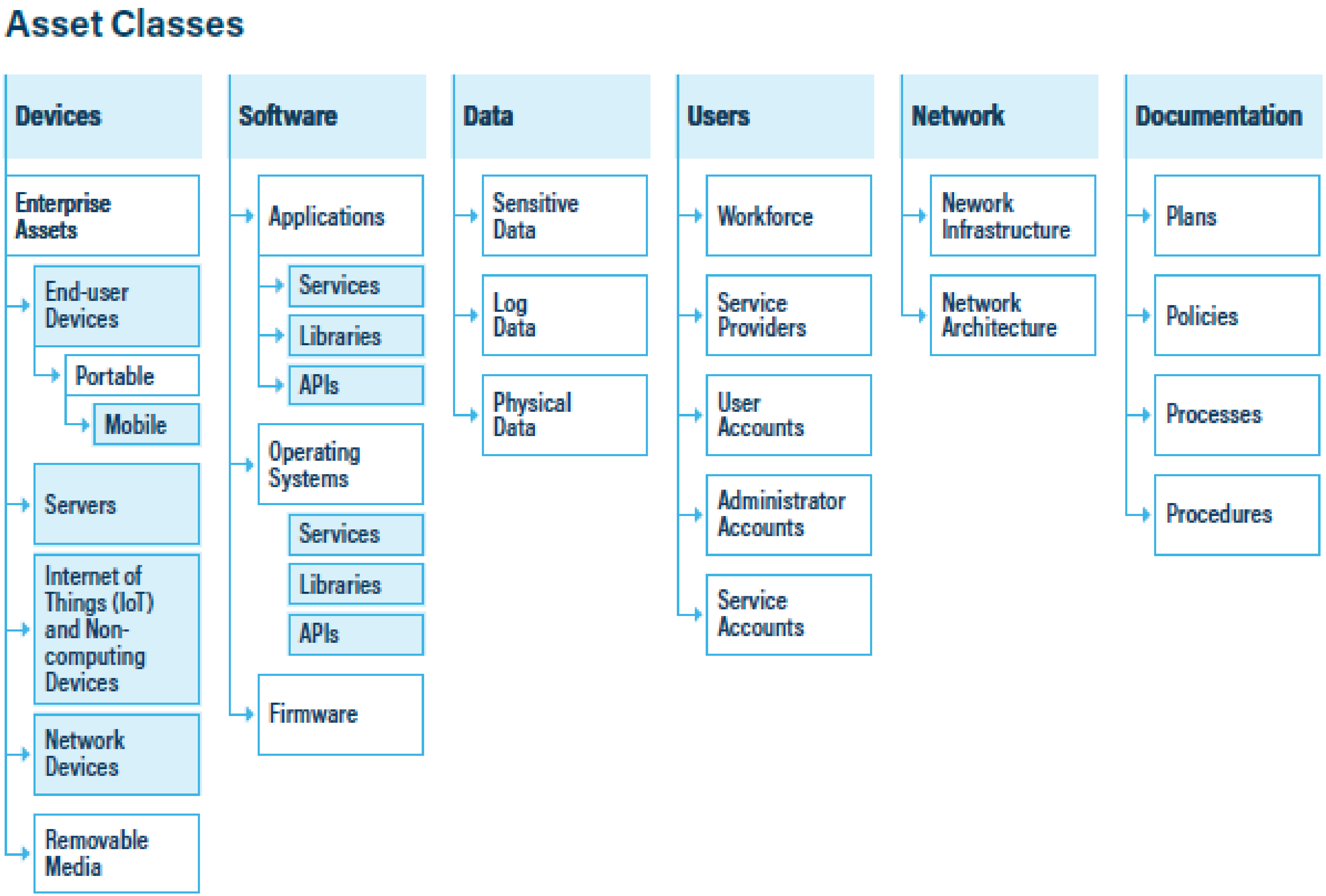
□ North American Electric Reliability Corporation-Critical Infrastructure Protection Standards (NERC-CIP

You have the answers already

- Inventory isn’t easy
- **Inventory of authorized and unauthorized devices**
  - Obtain from your network management team (maybe)
  - Who decides what’s unauthorized?
- **Inventory of authorized and unauthorized software**
  - Obtain from network infrastructure, software purchasing, fixed assets, local sysadmin, property mgt. teams, etc.
- **Inventory of Sensitive Data**
  - Obtain from business team, local IT staff
  - Risk classification standard determines data risk level

What Should Be in an Inventory Record?

- “Owner name”, hostname, description, location (on/off prem), inventory tag #, serial #, classification (low, mod, high), priority (non-essential, essential), system type (mobile, laptop, desktop, server, etc.), IT contact, user contact, valid users, managed? (Y/N, BigFix, InTune, JamF, osquery), MDE installed?, comments
- Tools: CMDB, Tanium, Axionius, GRC (Isora, SN-GRC), etc.
- Hardware, Software, **Data,** users, network, documentation

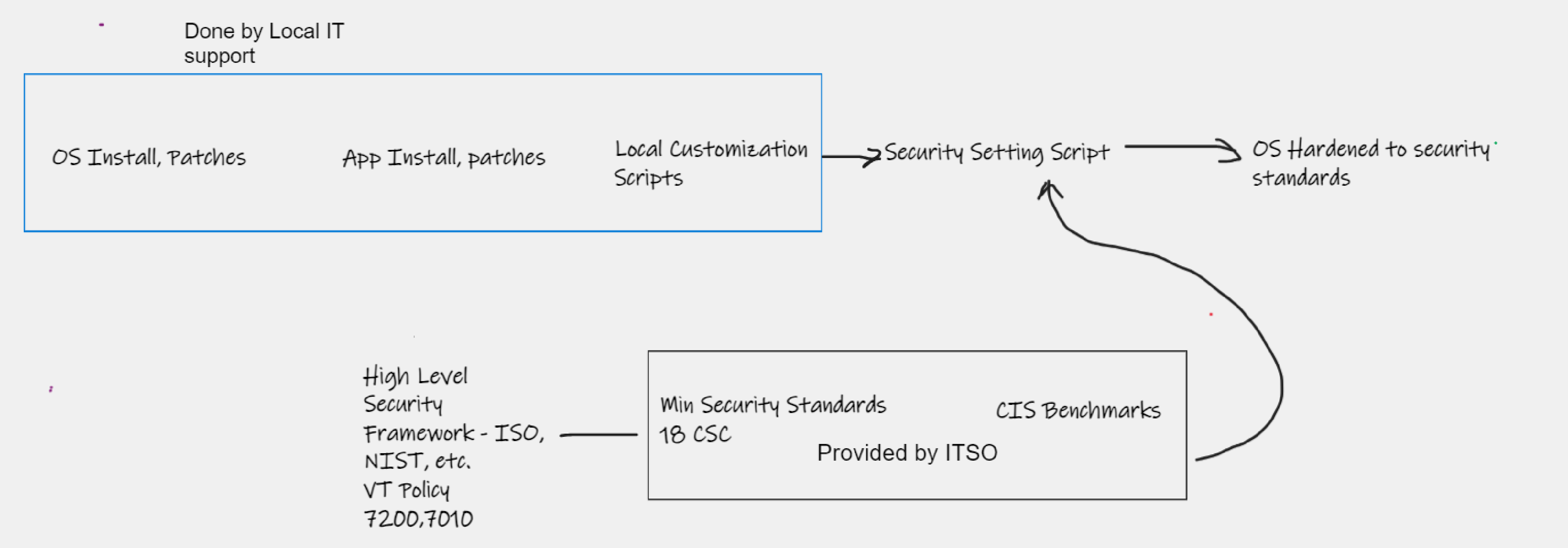


Asset Classes

- Devices
  - Enterprise Assets
    - End-user Devices
      - Portable
        - Mobile
    - Servers
    - Internet of Things (IoT) and Non-computing Devices
    - Network Devices
    - Removable Media
- Software
  - Applications
    - Services
    - Libraries
    - APIs
  - Operating Systems
    - Services
    - Libraries
    - APIs
  - Firmware
- Data
  - Sensitive Data
  - Log Data
  - Physical Data
- Users
  - Workforce
  - Service Providers
  - User Accounts
  - Administrator Accounts
  - Service Accounts
- Network
  - Nework Infrastructure
  - Network Architecture
- Documentation
  - Plans
  - Policies
  - Processes
  - Procedures

Source: CIS Controls v8.1

Secure Configuration Roadmap Example

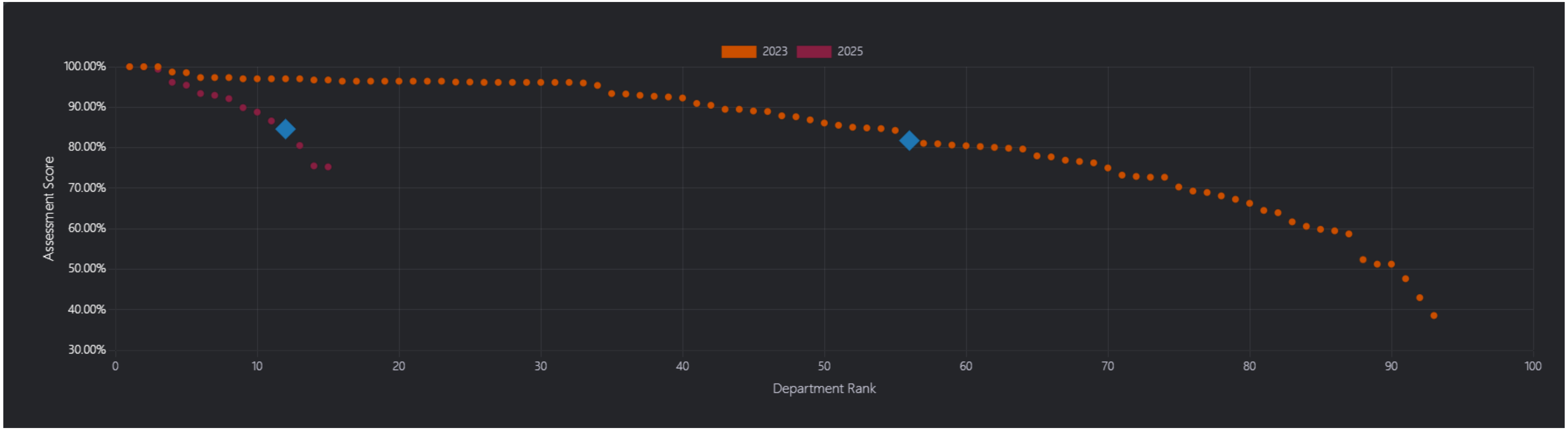


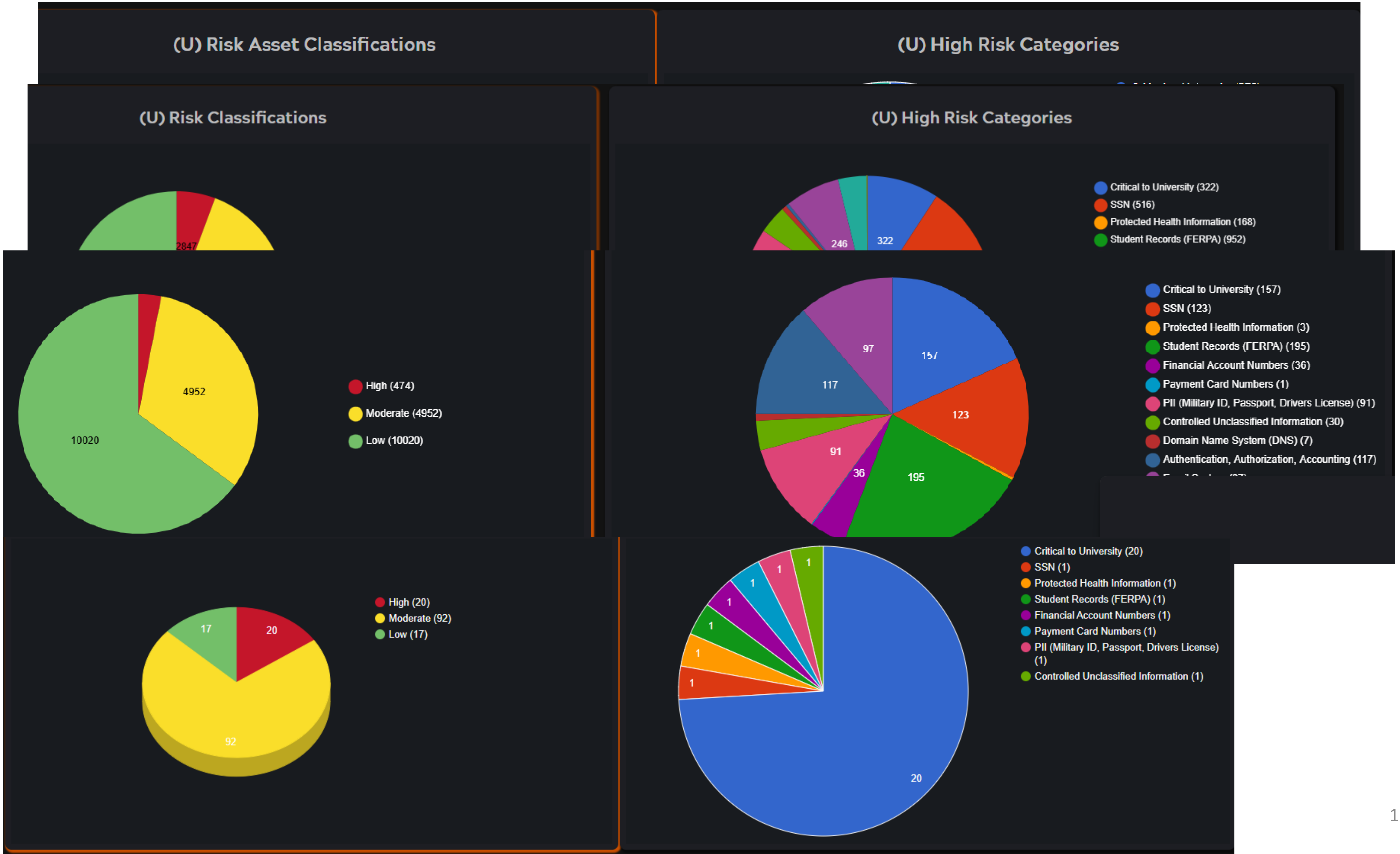
Since 2023

- Elevated to Microsoft A5 license
  - EDR, Phishing, DLP, robust toolset that runs in Windows, MacOs, Linux, MDE
- Requested funding for enterprise wide backup solution
- Expanding enterprise wide endpoint management
  - InTune, BigFix, Jamf, OSquery

Gap Analysis – Assessment Scores

- Incomplete, 2025 assessments due 6/1/25
- Lower? More realistic answers, clearer questions….



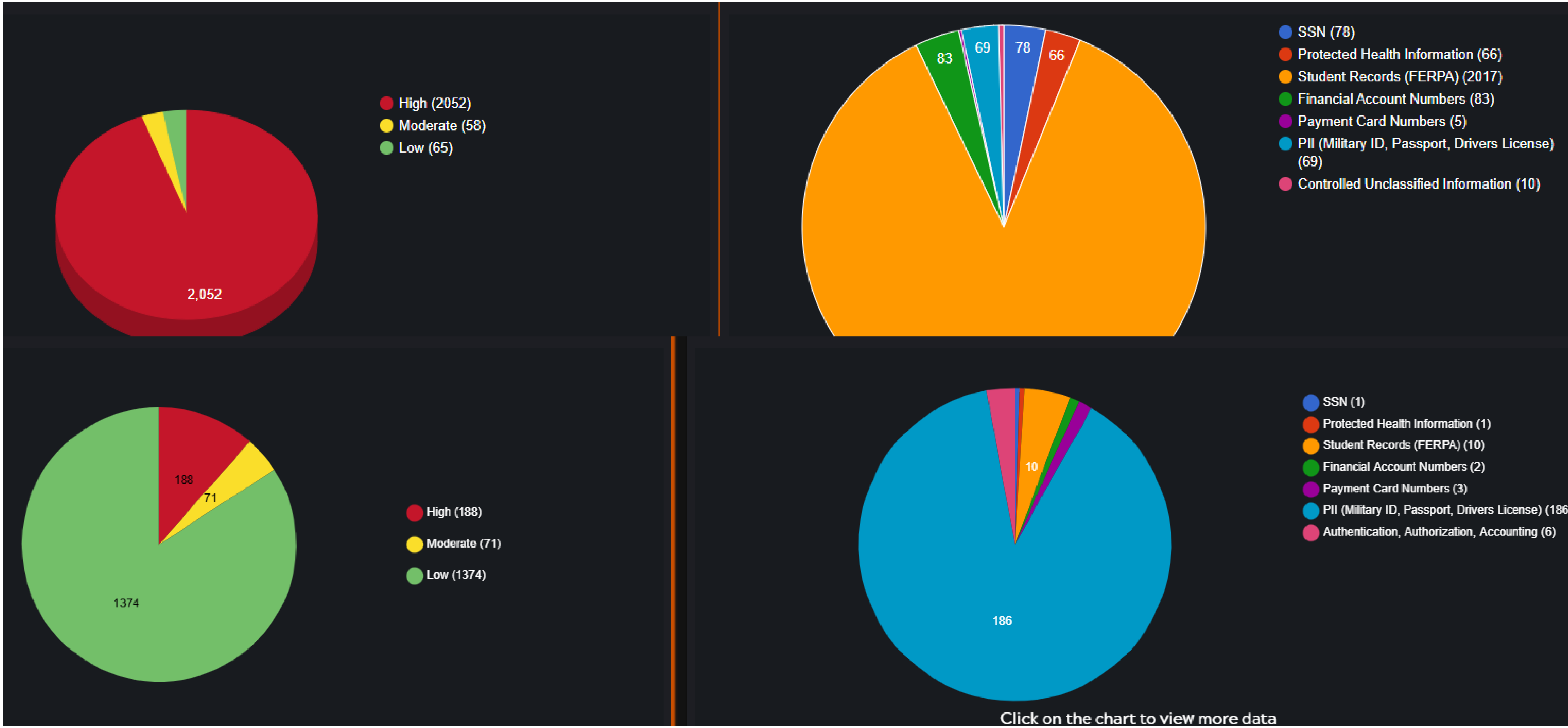

(U) Risk Asset Classifications

(U) High Risk Categories

(U) Risk Classifications

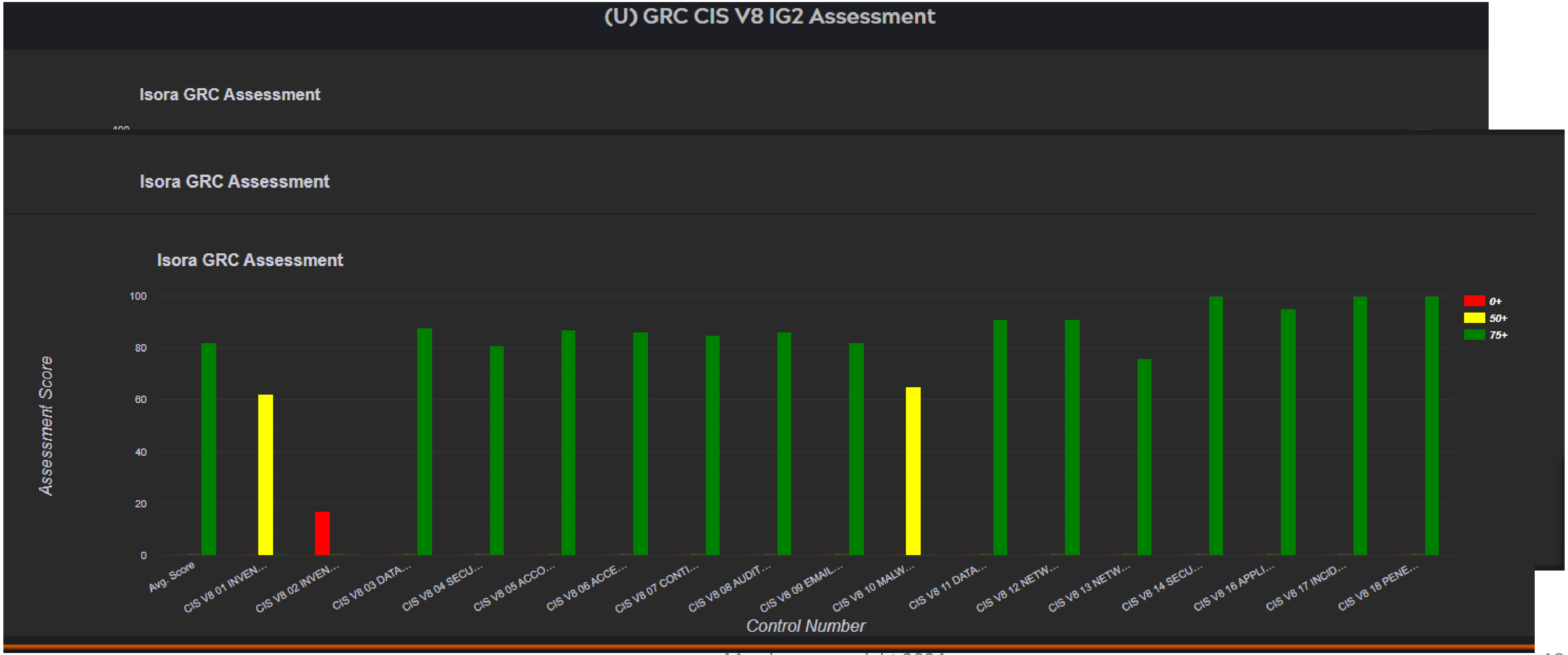
(U) High Risk Categories

2847
246
322
Critical to University (322)
SSN (516)
Protected Health Information (168)
Student Records (FERPA) (952)
4952
10020
High (474)
Moderate (4952)
Low (10020)
97
157
117
123
91
36
195
Critical to University (157)
SSN (123)
Protected Health Information (3)
Student Records (FERPA) (195)
Financial Account Numbers (36)
Payment Card Numbers (1)
PII (Military ID, Passport, Drivers License) (91)
Controlled Unclassified Information (30)
Domain Name System (DNS) (7)
Authentication, Authorization, Accounting (117)
17
20
92
High (20)
Moderate (92)
Low (17)
1
1
1
1
1
1
1
20
Critical to University (20)
SSN (1)
Protected Health Information (1)
Student Records (FERPA) (1)
Financial Account Numbers (1)
Payment Card Numbers (1)
PII (Military ID, Passport, Drivers License) (1)
Controlled Unclassified Information (1)



Click on the chart to view more data

2023 Gap Analysis – the Good, the Bad, the Ugly



(U) GRC CIS V8 IG2 Assessment

Isora GRC Assessment

Isora GRC Assessment

Isora GRC Assessment

Minimum Security Standard (MinSec)

- MinSec 4.0 went into effect 7/1/2024.
- Not a standard PDF, rather an “active” www page
- CIS IG2 has 130 items (“safeguards”) aka “subcontrols”
- https://securitystandards.iso.vt.edu

Summary

- Go to the CIS CSC V8 Landing Page
  - https://www.cisecurity.org/critical-controls
- Need an operational plan to implement a Security Framework? Use the CIS Navigator tool
- It’s auditable, strengthens your overall defensive posture

References

- “If we don't write the rules, our adversaries will write our future.” – Rob T. Lee, SANS Institute
- Virginia Tech Minimum Security Standards – https://securitystandards.iso.vt.edu
- CIS Controls: https://cisecurity.org/v8
- CIS Navigator tool: https://www.cisecurity.org/controls/cis-controls-navigator
- Virginia Tech Risk Assessment Standard: https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-IT-Risk-Assessment-Standard.pdf
- Virginia Tech Policy on Securing Technology Resources and Services: https://www.policies.vt.edu/7010.pdf

VIRGINIA
IT AGENCY

Security & Enterprise Architecture

ISOAG

Chris Williams, Director of SA/EA

May 14th, 2025

Agenda

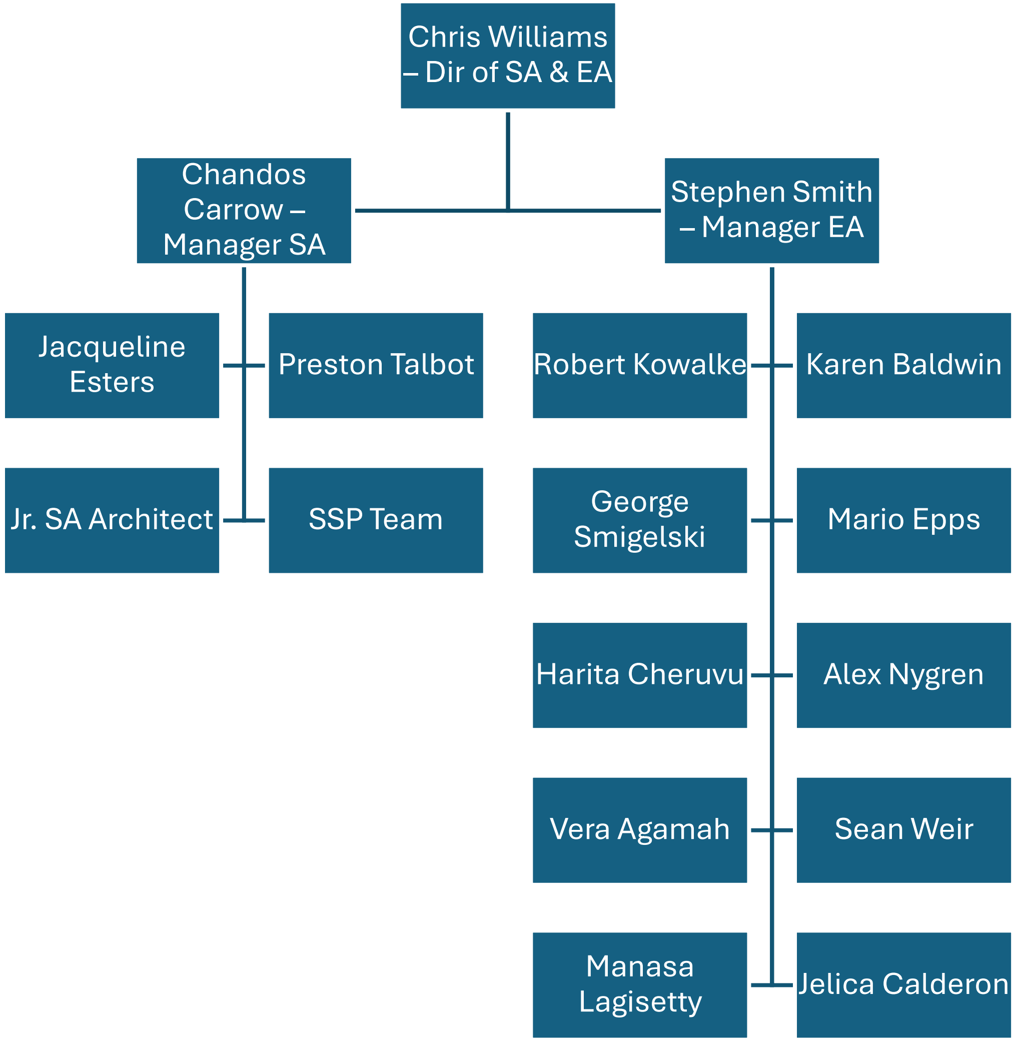
- Introduction from “new” EA/SA Director
- Who SA/EA is
- SA
- EA
- Engaging EA

“New” Director of Security & Enterprise Architecture

- Started role in Feb 2025
- Commonwealth Experience includes:
  - DIT (precursor to VITA) in 1999
    - Managed internal IT
  - VITA
    - Cloud Architect
    - Cloud Services Manager
  - DSS
    - Cloud Infrastructure Operations Director
- Other EA Experience includes:
  - Led EA Governance team at Capital One
  - EA with Federal Reserve/TWAI
- Additional IT roles with TEK Systems, Cognizant, Anthem, Markel in variety of Service Delivery roles

Chris Williams (no really, that is me)

SA & EA – Who we are



Chris Williams – Dir of SA & EA

Chandos Carrow – Manager SA

Stephen Smith – Manager EA

Jacqueline Esters

Preston Talbot

Jr. SA Architect

SSP Team

Robert Kowalke

Karen Baldwin

George Smigelski

Mario Epps

Harita Cheruvu

Alex Nygren

Vera Agamah

Sean Weir

Manasa Lagisetty

Jelica Calderon

SA & EA - What does SA Cover?

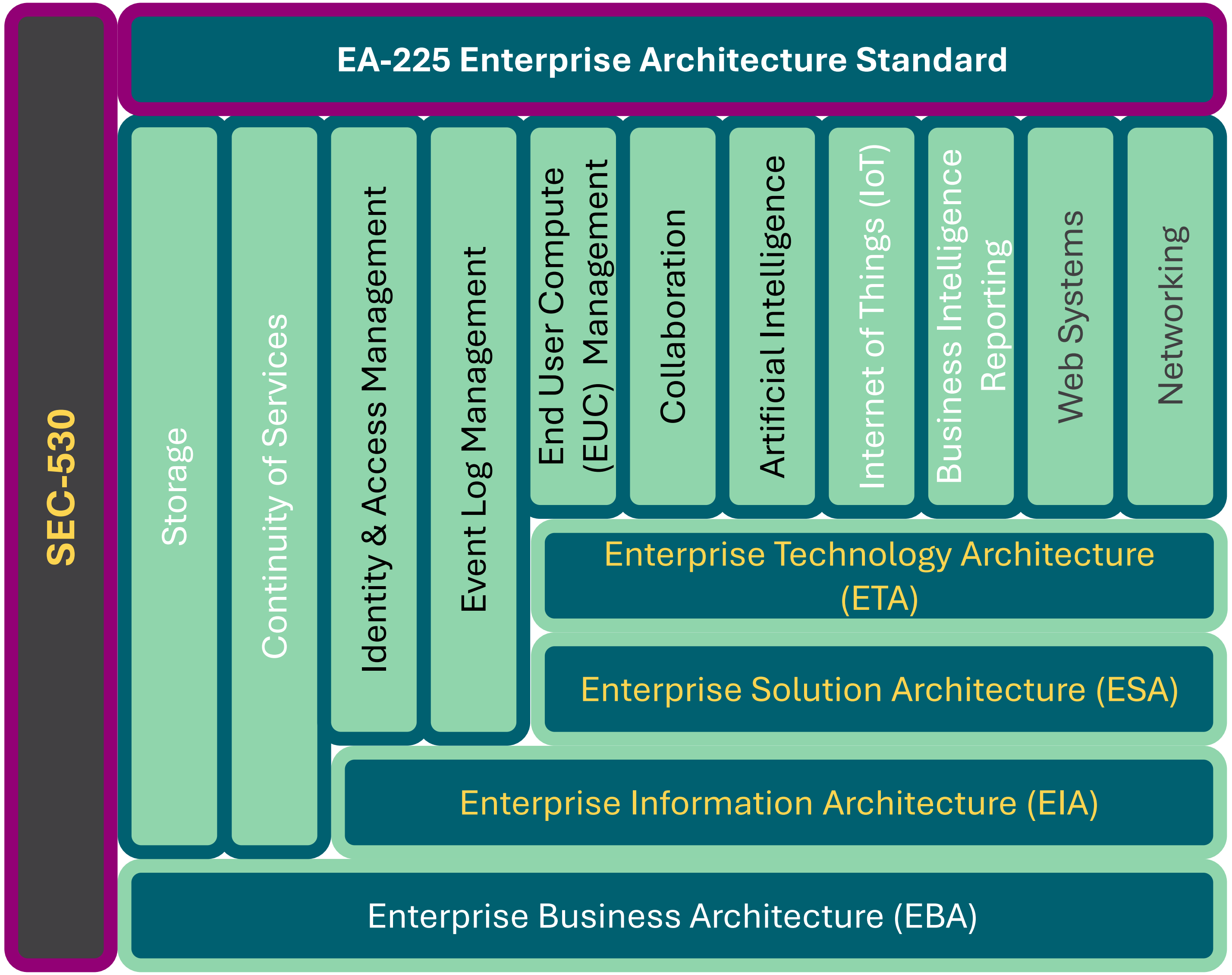
- SEC530 – Information Security Standard
- Security Exceptions
- SSP's – System Security Plans
  - Writing SSPs, process is owned by CSRM Governance & Compliance
- Baseline review
- Solution Support
  - RFS Guidance
  - Enterprise Procurement

SA & EA - What does EA cover?

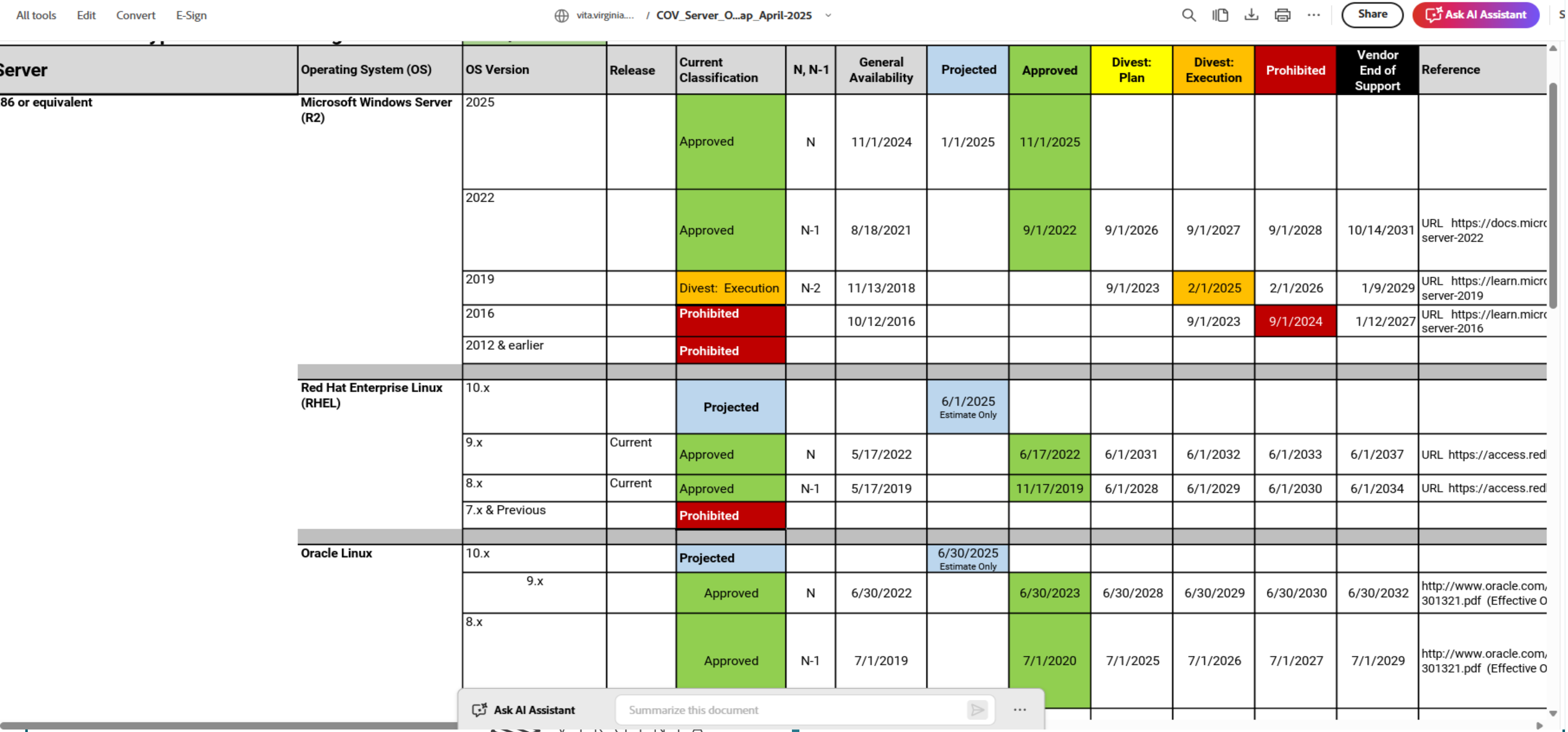
- EA 200 – Enterprise Architecture Policy
- EA 225 – Enterprise Architecture Standard
  - Individual EA standards
- EA Exceptions
- Enterprise Procurement Support
- AI
  - AI Registry
  - AI CoP (next meeting June 4th)

- Technology Roadmaps
  - Server OS/Hypervisor example
- EA "Tickets"
  - DNS
  - PGR
  - Etc.
- Ardoq
  - Enterprise Application Information
- EA Agency Assistance

Standards Map


SEC-530
EA-225 Enterprise Architecture Standard
Storage
Continuity of Services
Identity & Access Management
Event Log Management
End User Compute (EUC) Management
Collaboration
Artificial Intelligence
Internet of Things (IoT)
Business Intelligence Reporting
Web Systems
Networking
Enterprise Technology Architecture (ETA)
Enterprise Solution Architecture (ESA)
Enterprise Information Architecture (EIA)
Enterprise Business Architecture (EBA)

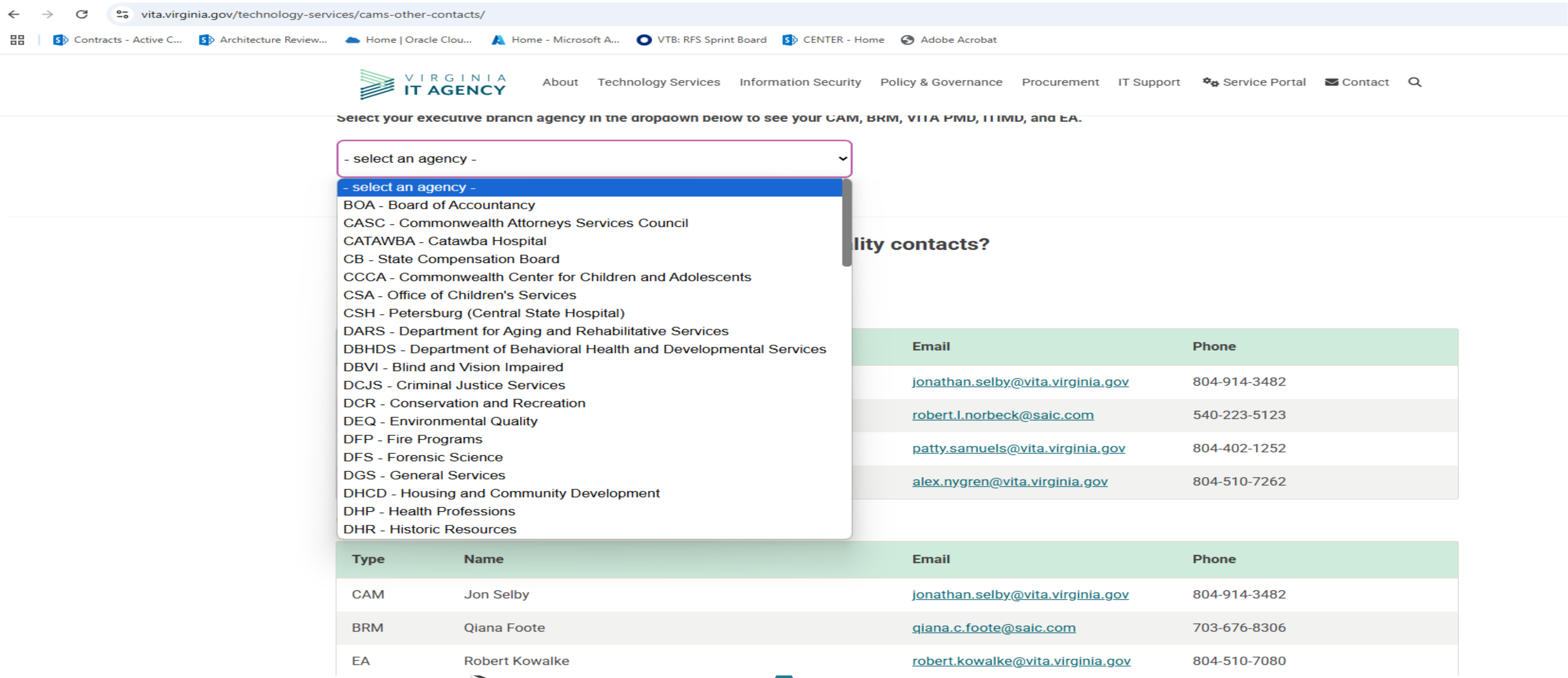
Tech Roadmap



Server	Operating System (OS)	OS Version	Release	Current Classification	N, N-1	General Availability	Projected	Approved	Divest: Plan	Divest: Execution	Prohibited	Vendor End of Support	Reference
86 or equivalent	Microsoft Windows Server (R2)	2025		Approved	N	11/1/2024	1/1/2025	11/1/2025					
		2022		Approved	N-1	8/18/2021		9/1/2022	9/1/2026	9/1/2027	9/1/2028	10/14/2031	URL https://docs.micro server-2022
		2019		Divest: Execution	N-2	11/13/2018			9/1/2023	2/1/2025	2/1/2026	1/9/2029	URL https://learn.micro server-2019
		2016		Prohibited		10/12/2016				9/1/2023	9/1/2024	1/12/2027	URL https://learn.micro server-2016
		2012 & earlier		Prohibited									
	Red Hat Enterprise Linux (RHEL)	10.x		Projected			6/1/2025 Estimate Only						
		9.x	Current	Approved	N	5/17/2022		6/17/2022	6/1/2031	6/1/2032	6/1/2033	6/1/2037	URL https://access.red
		8.x	Current	Approved	N-1	5/17/2019		11/17/2019	6/1/2028	6/1/2029	6/1/2030	6/1/2034	URL https://access.red
		7.x & Previous		Prohibited									
	Oracle Linux	10.x		Projected			6/30/2025 Estimate Only						
		9.x		Approved	N	6/30/2022		6/30/2023	6/30/2028	6/30/2029	6/30/2030	6/30/2032	http://www.oracle.com/ 301321.pdf (Effective O
		8.x		Approved	N-1	7/1/2019		7/1/2020	7/1/2025	7/1/2026	7/1/2027	7/1/2029	http://www.oracle.com/ 301321.pdf (Effective O

Assigned EA Resource

https://www.vita.virginia.gov/technology-services/cams-other-contacts/



Select your executive branch agency in the dropdown below to see your CAM, BRM, VITA PMD, ITIMD, and EA.

- select an agency -

- select an agency -
BOA - Board of Accountancy
CASC - Commonwealth Attorneys Services Council
CATAWBA - Catawba Hospital
CB - State Compensation Board
CCCA - Commonwealth Center for Children and Adolescents
CSA - Office of Children's Services
CSH - Petersburg (Central State Hospital)
DARS - Department for Aging and Rehabilitative Services
DBHDS - Department of Behavioral Health and Developmental Services
DBVI - Blind and Vision Impaired
DCJS - Criminal Justice Services
DCR - Conservation and Recreation
DEQ - Environmental Quality
DFP - Fire Programs
DFS - Forensic Science
DGS - General Services
DHCD - Housing and Community Development
DHP - Health Professions
DHR - Historic Resources

lity contacts?

Email	Phone
jonathan.selby@vita.virginia.gov	804-914-3482
robert.l.norbeck@saic.com	540-223-5123
patty.samuels@vita.virginia.gov	804-402-1252
alex.nygren@vita.virginia.gov	804-510-7262

Type	Name	Email	Phone
CAM	Jon Selby	jonathan.selby@vita.virginia.gov	804-914-3482
BRM	Qiana Foote	qiana.c.foote@saic.com	703-676-8306
EA	Robert Kowalke	robert.kowalke@vita.virginia.gov	804-510-7080

Reaching out to EA:

Initial step is to reach out to you CAM and/or BRM

- We want to ensure they are aware of anything impacting your agency

Reach out to the assigned EA resource (per previous slide)

Send an email to: ea@vita.virginia.gov

https://www.vita.virginia.gov/policy--governance/enterprise-architecture/

Questions?

Thank you!

VIRGINIA IT AGENCY

Phishing Reporting and Phishing Simulation Update

Matthew Umphlet, Threat Intelligence Analyst

KnowBe4 PAB and Phishing Simulation Discontinuation

- Change in the way that the KnowBe4 PAB is Authenticated in User Mailboxes
- On 5/1/25 Microsoft pushed a change that broke the current PAB implementation and requires an unsupported update in the COV M365 environment
- KnowBe4 PAB and Phishing Simulations will be discontinued effective immediately
- Annual Security Training is ***NOT*** affected at this time by this discontinuation and will be continued to be delivered in KnowBe4
- VITA CSRM is exploring replacement options, but has selected Microsoft as the Interim Solution Provider

Microsoft 365: Built in Report Phishing Button and Phishing Simulation

- **The Microsoft 365 Reproting Button allows end users to report Phishing and Spam across Workstations and Mobile Devices**
- **Supported on Web Client and Desktop Client**
- **All Reports will be analyzed by the appropriate VITA Service Tower**
- **Monthly Phishing Simulations will continue to be issued by VITA CSRM**
  - Agencies are not required to send additional Phishing Simulation

Changes and Limitations

- **Changes**
  - Agency ISOs will reach out to VITA to Schedule Agency specific campaigns, up to 6 months at a time
  - Agency ISOs will be able to build their own Templates, with enhanced features (New domains, techniques, attachments)
  - Agency ISOs will view results from a new dashboard
  - Can View and Generate Pass/Fail Reports and Remediation Training Status Reports

- **Limitations**
  - Agency ISOs cannot schedule and conduct local phishing campaigns
  - Reported Phishing emails cannot be forwarded to agency indicated mailboxes
  - Phishing templates cannot be shared before monthly campaigns

VIRGINIA IT AGENCY

TLS 1.0/1.1 Remediation

Enterprise Project

John C Del Grosso
VITA SSDC Service Owner

Overview: Transmission layer security (TLS) compliance

- TLS encrypts data that is transmitted over the internet. It is used with websites (https://), remote desktop protocol (RDP), email, etc.
- **TLS 1.0 and 1.1 are deprecated:** These versions have encryption ciphers that can expose systems to attacks such as downgrade attacks and weak cipher exploitation.
- **Compliance:** EA225 requires the Commonwealth of Virginia (COV) to use technologies that are not end-of-life (EOL).
- **Secure communication:** Enforcing modern TLS ensures data confidentiality and integrity during transit, protecting against eavesdropping or tampering.
- **Discovery:** Tenable scans show that TLS1.0/1.1 continue to be allowed on servers (<1,000) in the environment. Port 3389 accounts for majority of these detections.
  - **Port 3389** is the default transmission control protocol (TCP) port assigned to RDP
  - The intent is to force all RDP sessions to use TLSv1.2 only

Activities to block TLS1.0/1.1

Operating system (OS) level restriction

Process

1. **Establishment of security groups** for Windows Server 2012, 2016, 2019, 2022 and **required OS configuration changes** for Linux 6,7,8,9
2. **Restriction:** Security group policy restricts the change at the OS Level and does not allow for the use of TLS 1.0/1.1
3. **Reboot required:** Changing the setting at OS level requires a reboot to be enacted. Changes will take affect after the scheduled maintenance window reboot for patching.

Status

- **Testing:** Windows testing complete, Linux testing nearly complete
- **Review of 'security hardening' requirements** for OS (Windows and Linux) Security hardening restricts TLS 1.0/1.1 in more recent versions of OS (OS2016 and up, Linux 7 and up)

TLS support by operating system

All in-use COV operating systems are hardened do 'disallow' TLSv1.0/1.1 through policy and/or register changes

Windows OS Server	TLSv1.0/1.1	TLSv1.2	TLSv1.3
2008R2	Supported	Supports	Not supported
2012R2	Supported	Supports	Not supported
2016	Supported	Supports	Not supported
2019	Supported	Supports	Not supported
2022	Supports 1.1	Supports	Supports
2025	Supported for clients only	Supports	Supports

Linux OS Server	TLSv1.0/1.1	TLSv1.2	TLSv1.3
RHEL 5	Supported	Not supported	Not supported
RHEL 6	Supported	Supports	Not supported
RHEL 7	Supported	Supports	Supported w/updates
RHEL 8	Supports	Supports	Supports
RHEL 9	Not enabled	Supports	Supports
RHEL10	Not enabled	Supports	Supports

Process to change RDP Port to accept TLS1.2/1.3 only

01

VITA is identifying server ports using TLSv1.0/v1.1

02

Agencies will receive an impacted server list from their business relationship manager (BRM)

03

VITA will set a change date to prohibit TLSv1.0/1.1 on servers with detections for Port 3389 only

04

VITA will place the server OS in a security group to prohibit TLSv1.0/1.1

How agencies can help get ahead of the end-of-life deprecation

1. Work with your application developers to determine if your agency-owned **application(s) supports use of TLS v1.2 or v1.3**
2. System administrators should check the **operating system (OS) settings**. If the OS security settings on a server allow ‘any’ TLSv1.x, switches should be updated to **allow TLSv1.2+ only**
3. Agencies should review the server list to be provided by the BRM to identify potential changes or updates

If agency applications **cannot support TLS1.2+, then submit security exception(s)** in Archer to identify the servers' name, port, agency application(s), and action(s) required.

Next steps

- VITA will implement the restriction on servers with TLSv1.0/1.1 detected on Port 3389 only for Windows Servers only - expected quarter three (Q3) 2025.
- Look out for VITA communications announcing specific dates for Linux activity.
- **Agencies should advise their BRM if the change would be an issue for their agency**
- Further activity will be announced for those servers that show TLSv1.0/1.1 on other ports

Revised Patch Remediation Schedule

The recorded information sessions from March and April are available to watch:

- March 19 recording
- April 1 recording

The questions from the information sessions and ISOAG were collected and are available for review.

- Revised patch cycle frequently asked questions (FAQs) here

Questions?

Announcements

ISOAG May 14, 2025

Three New Types of User Guides!

There are three new types of user guides available on CSRM Connections:

- Hey ISOs! The Archer, Nucleus Acunetix user guides are now published on the CSRM Connections!
- View the guides today on CSRM Connections (Under the “ISO Resources” link on the right side)
- Strengthen your agency’s security with ease! 🔐

Learn how to:

✅ Access & analyze vulnerabilities
✅ Prioritize risks effectively
✅ Streamline workflows & boost security

ARCHER

acunetix

Nucleus

International Travel

As traveling season approaches us, lets make sure we all understand how to comply with COV guidelines regarding devices.

Before your trip, be sure to check out the knowledge base article on the VCCC site if you are travelling internationally.

If you're unsure about any compliance requirements, don't hesitate to ask!

Action Required: Archer User Access Audit

Who: Information Security Officers (ISOs)
What: Annual audit of Archer user access
When: Due by COB – May 30, 2025

Just a reminder if you received an email last week about the Archer user access audit, make sure it is completed

Important: If not completed by deadline, all Archer access, except ISOs, will be revoked

Issues accessing the link in the email? Contact Kendra Burgess

Questions? Contact CSRM

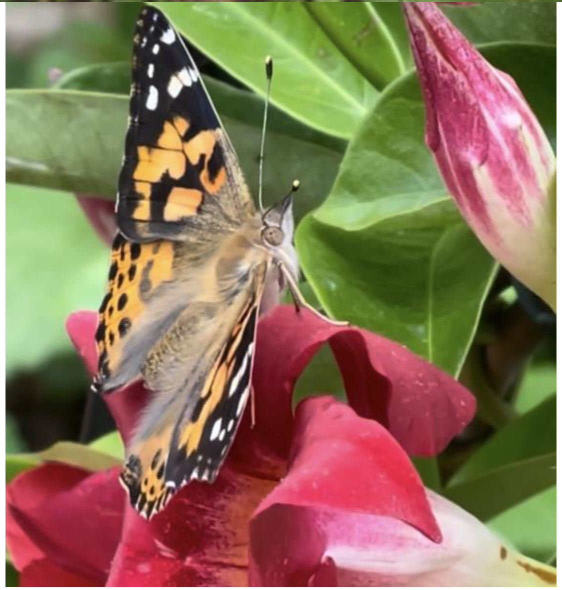
SPLUNK UPDATE – Spring Into Action: Get Your Logs Blooming!

Spring has sprung, so be sure to send in your logs, right into the VITA Splunk instance!

Just like pollen in the air (but way less annoying), your logs should be flowing freely. VITA is here to help bring your application logs into Splunk, giving you fresh insights and stronger security.

We’re always happy to hop on a call (no bunny suit required) to discuss your options and make sure everything is ready to grow.

Let’s make your logs blossom this spring – minus the allergies!



Top 5 Vulnerabilities

For the month of May, the Top 5 Key Vulnerabilities are:

- **Adobe ColdFusion < 2021.x < 2021u16 / 2023.x < 2023u10 Vulnerability (APSB24-71)**
- **KB5044293: Windows 10 Version 1607 / Windows Server 2016 Security Update (October 2024)**
- **Oracle WebLogic Server (October 2024 CPU)**
- **Tenable Nessus < 10.8.3 Multiple Vulnerabilities (TNS-2024-15 & TNS-2024-16)**
- **Google Chrome < 130.0.6723.92 Multiple Vulnerabilities**

NOTE Check CSRM Connections for more detailed information

Upcoming Events

VIRGINIA IT AGENCY

vita.virginia.gov

RVASEC 2025 Security Conference

The 14th annual RVASEC is coming up.

- Breakfast, lunch, coffee & snack breaks
- 30+ Speakers & keynotes
- Capture the flag
- Lock picking village and contest.

June 3rd 8am –
June 4th 6pm EDT

Richmond Marriott Downtown

500 E Broad St., Richmond, VA 23233

Registration Link!

Service Tower SOC Report Review Sessions

The upcoming SOC review session is June 11, 2025, and will be held remotely.

Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/r114f684dbdf1015aa82eaa3f39d24e67

Governance Office Hours – Now Monthly!

We're excited to announce the launch of monthly Governance Office Hours – a dedicated space for Agency ISOs and teams to bring their questions, concerns, or ideas directly to the Governance Team.

What to Expect:

- **Open discussion place**
- **Governance Updates**
- **Q&A and support for your needs**

Next Session:
June 18th 2025 | Microsoft Teams
[Click here to join the meeting]

Let's work together to strengthen governance across the Commonwealth!

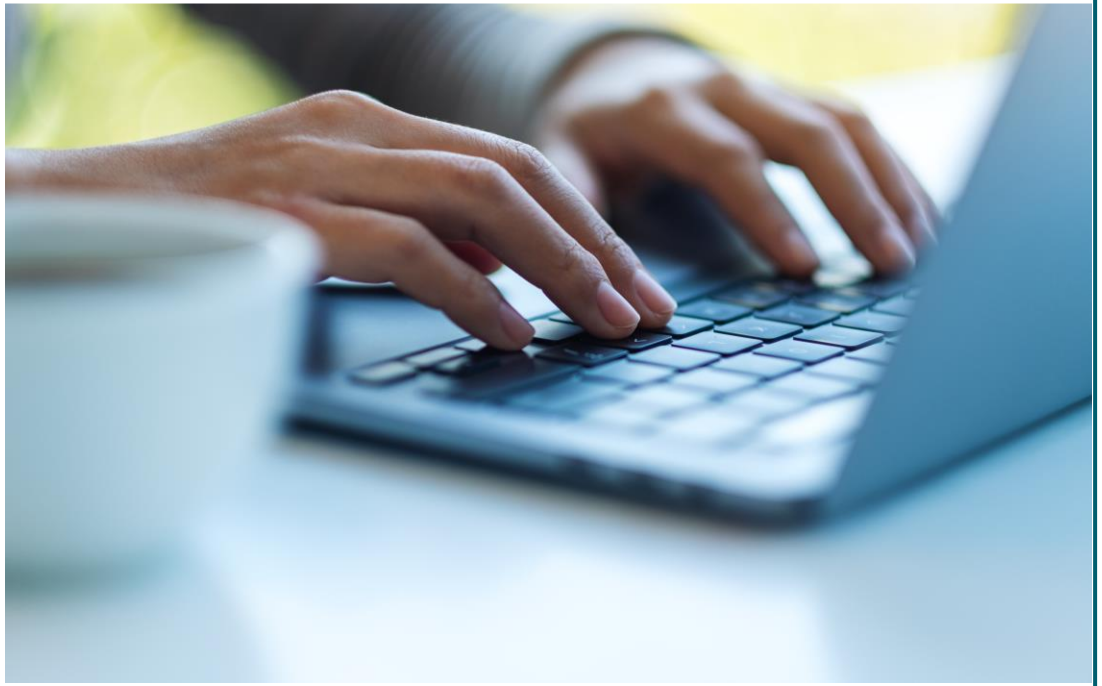
IS Orientation

The next IS Orientation is being held on June 25, 2025

- June 25, 2025, from 9am to 4pm, registration closes June 18th.
- It will be held in-person at the Boulders location:

  7325 Beaufont Springs Drive, Richmond, VA 23225

- Visit Commonwealth IS Orientation to register!



Commonwealth of Virginia Information Security Conference 2025
ISC:25

Future-Proofing Cybersecurity: *Next-Gen Strategies*

August 14, 2025

Hilton Richmond Hotel

12042 West Broad St.

Richmond, VA 23233

Registration will open soon!

[Security Conference | Virginia IT Agency]()

COV Information Security Conference 2025

ISC:25

Future-Proofing Cybersecurity: Next-Gen Strategies

Do you know of a potential speaker you'd would like to hear from at the upcoming COV ISC:25? Please let us know at ISConferenceCFP@virginia.gov

MEETING ADJOURNED

VIRGINIA
IT AGENCY