



WELCOME TO THE August 2, 2023

ISOAG MEETING



AGENDA	
Welcome/Opening Remarks	Tina Gaines/ VITA
SD WAN Overview	Thomas White/VITA
Website Modernization Update	Joshua Jones/VITA
New Threat Management Tools	Greg Lyons/VITA
Tabletop Incident Response Exercise	Zachary Wilton/SAIC
Iron Bow Update	John Sharp/Iron Bow
KnowBe4 Update	Tina Gaines/VITA
Upcoming Events	Tina Gaines/VITA
Adjourn	



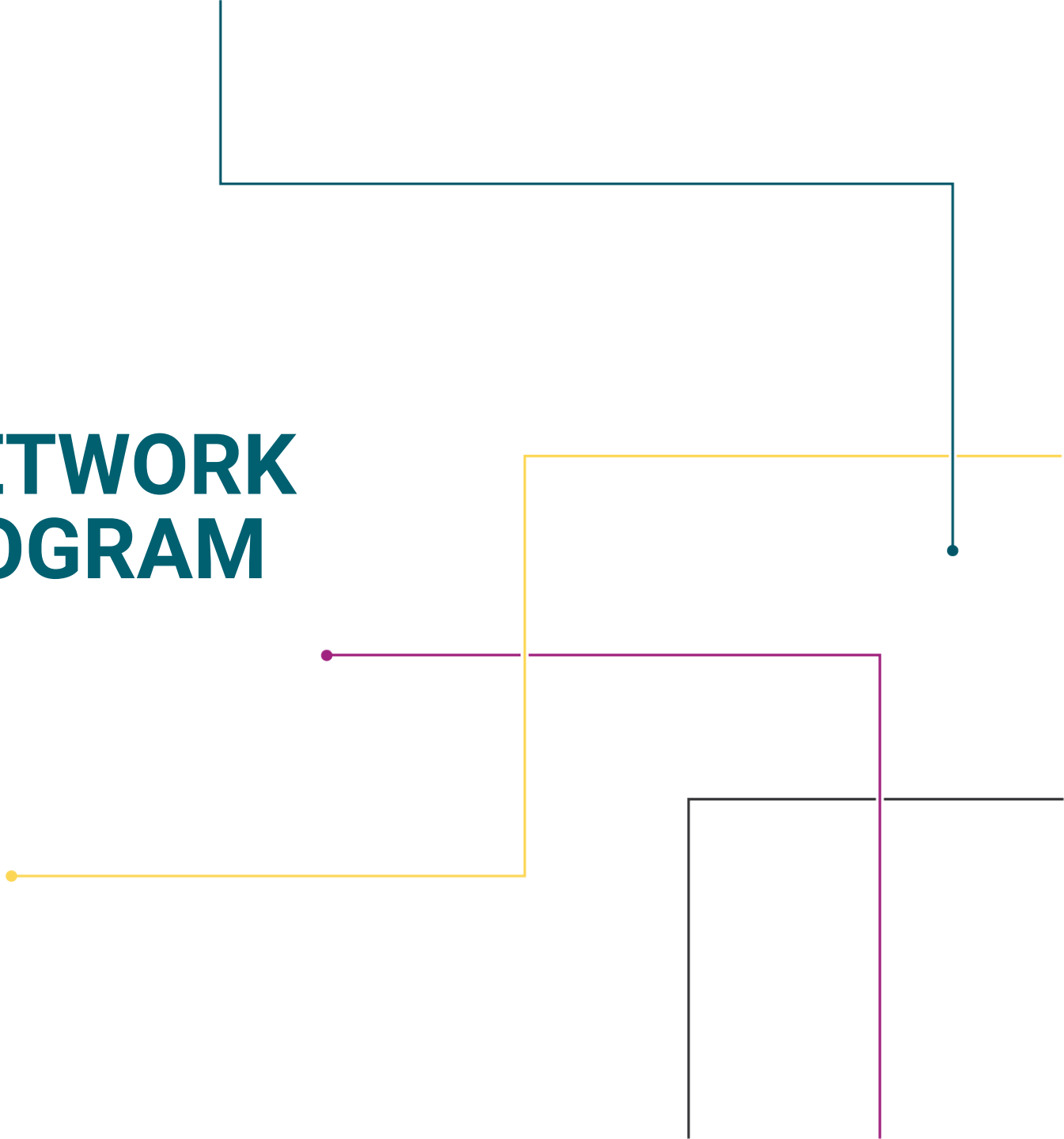
COMMONWEALTH NETWORK MODERNIZATION PROGRAM

TOM WHITE

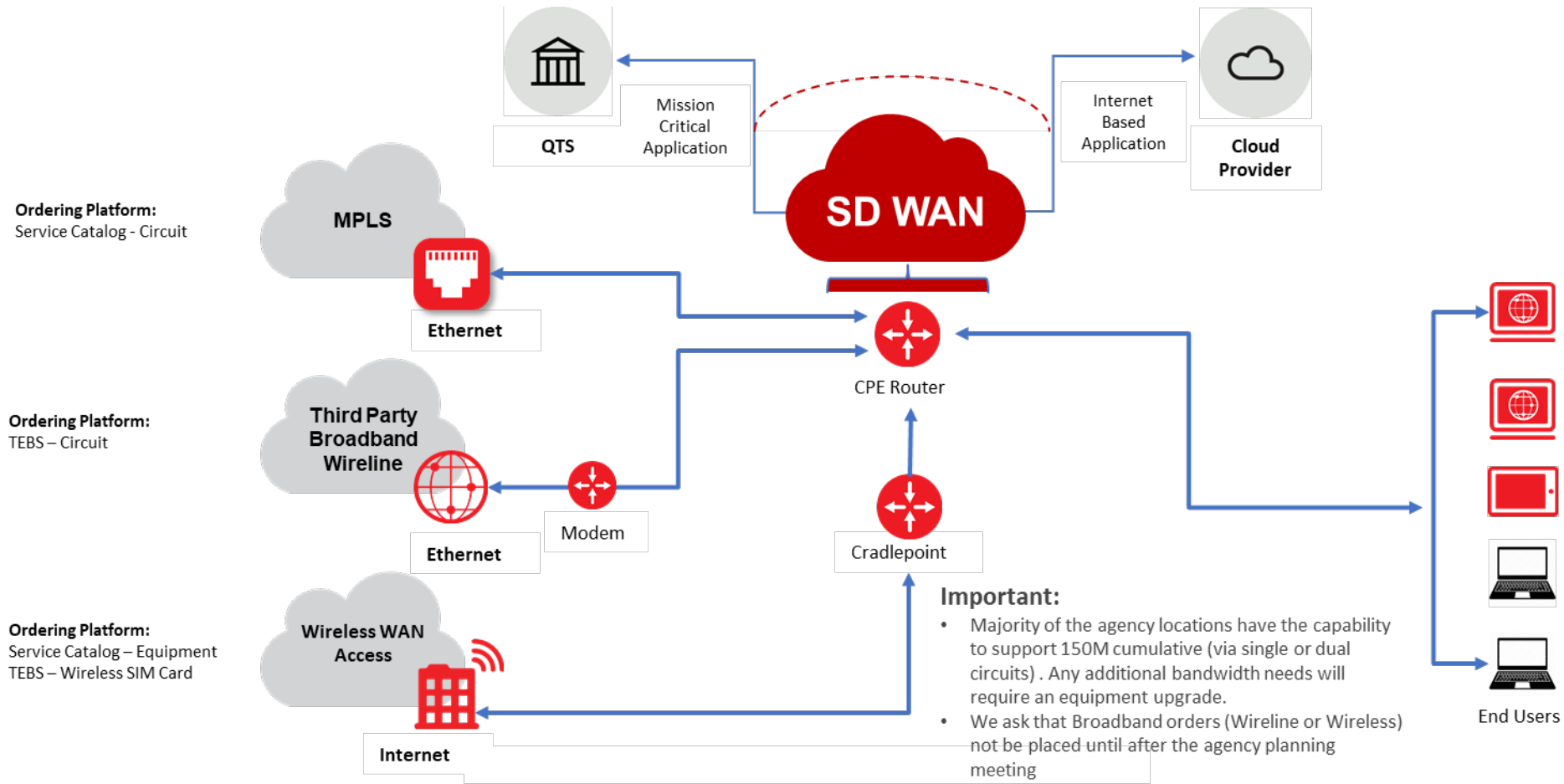
Program Manager, VITA SD-WAN/Broadband

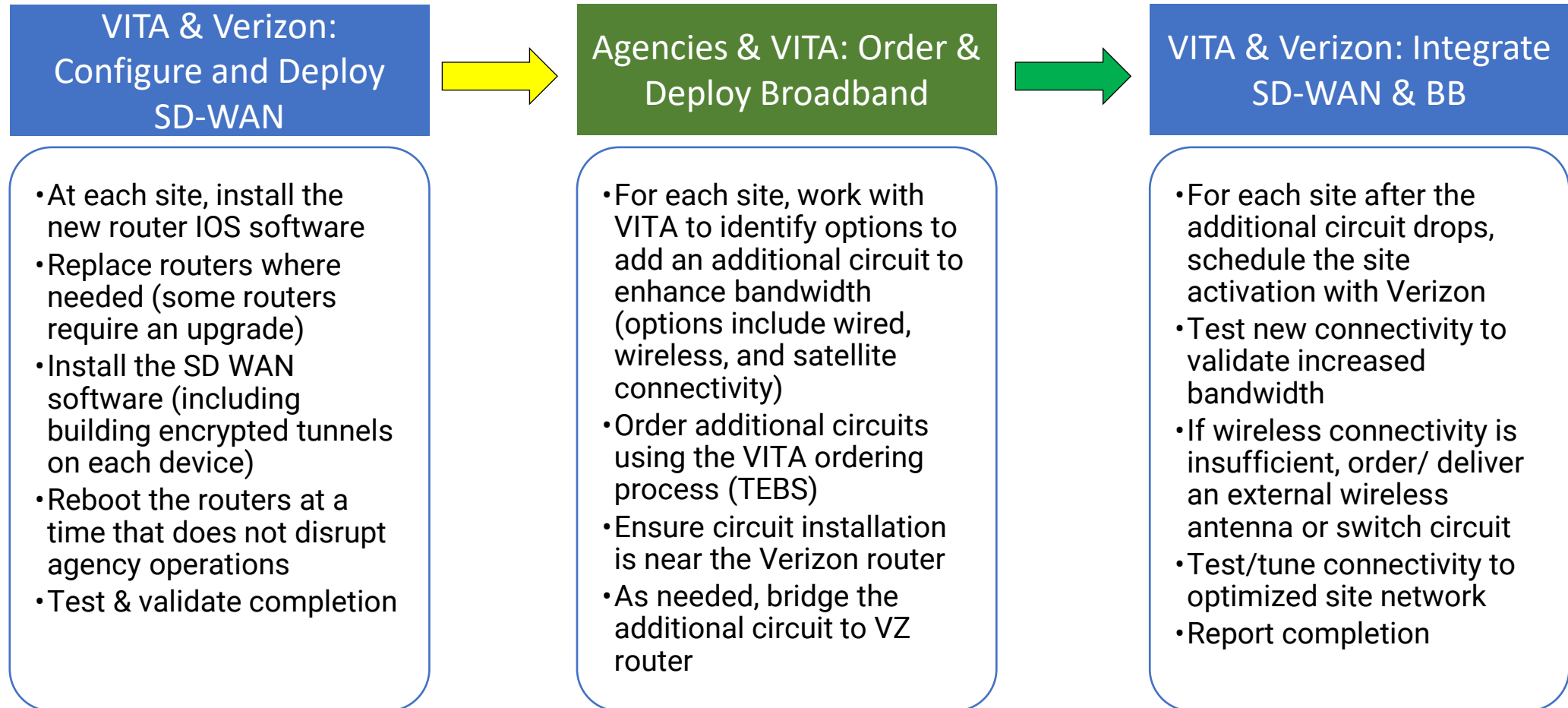
ISOAG MEETING

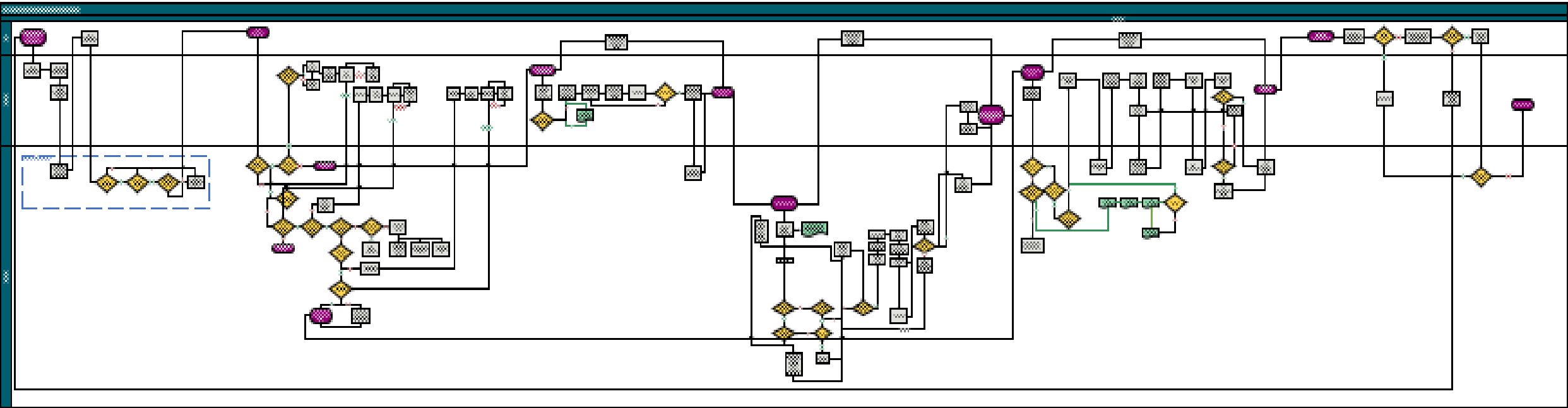
AUGUST 2, 2023



SD-WAN/BROADBAND









WHAT IS THE DEFINITION OF BROADBAND?







- “**Broadband**” is another term for high-speed internet access. In the United States, broadband is defined by the Federal Communications Commission (FCC) as a connection with **at least 25 Mbps download speed** and **3 Mbps upload speed**.
 - This definition is important because it’s the **benchmark for reliable internet access** in the United States and shapes the way we interpret population data and establish public policy.
- ***Virginia Telecommunication Initiative (VATI) in FY2024 targets 100 Mbps for circuits/agencies***

Status of SD-WAN and broadband:

Phase	Pending	Scheduled	Complete
Router IOS upgrade <small>IOS – Internetworking Operating System</small>	100 Router replacement or modem issue	174	890
SD-WAN conversion <small>SD-WAN – Software Defined Wide Area Network</small>	341	187	636
Broadband activation	770 770 need orders	229 19 scheduled 210 pending demarc/delivery	165

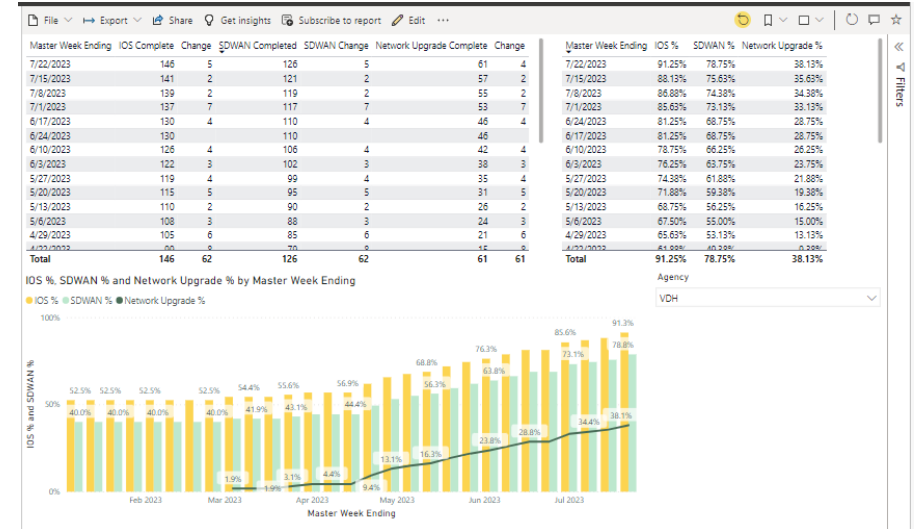
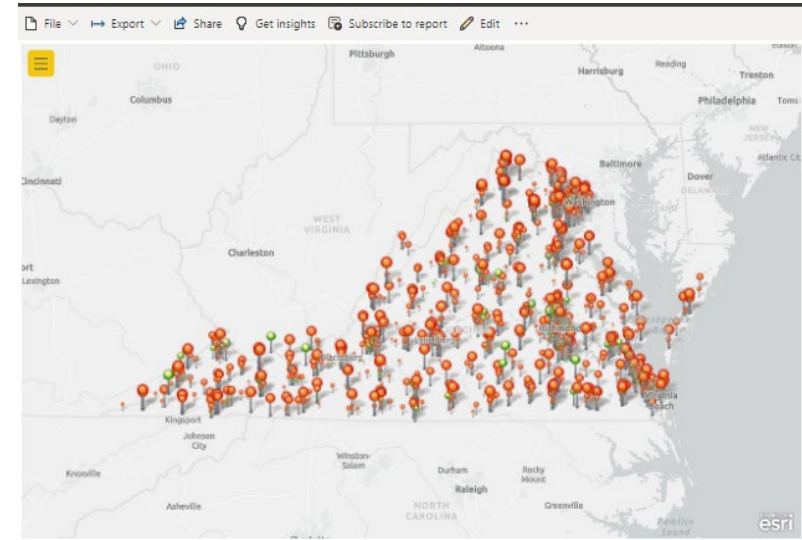
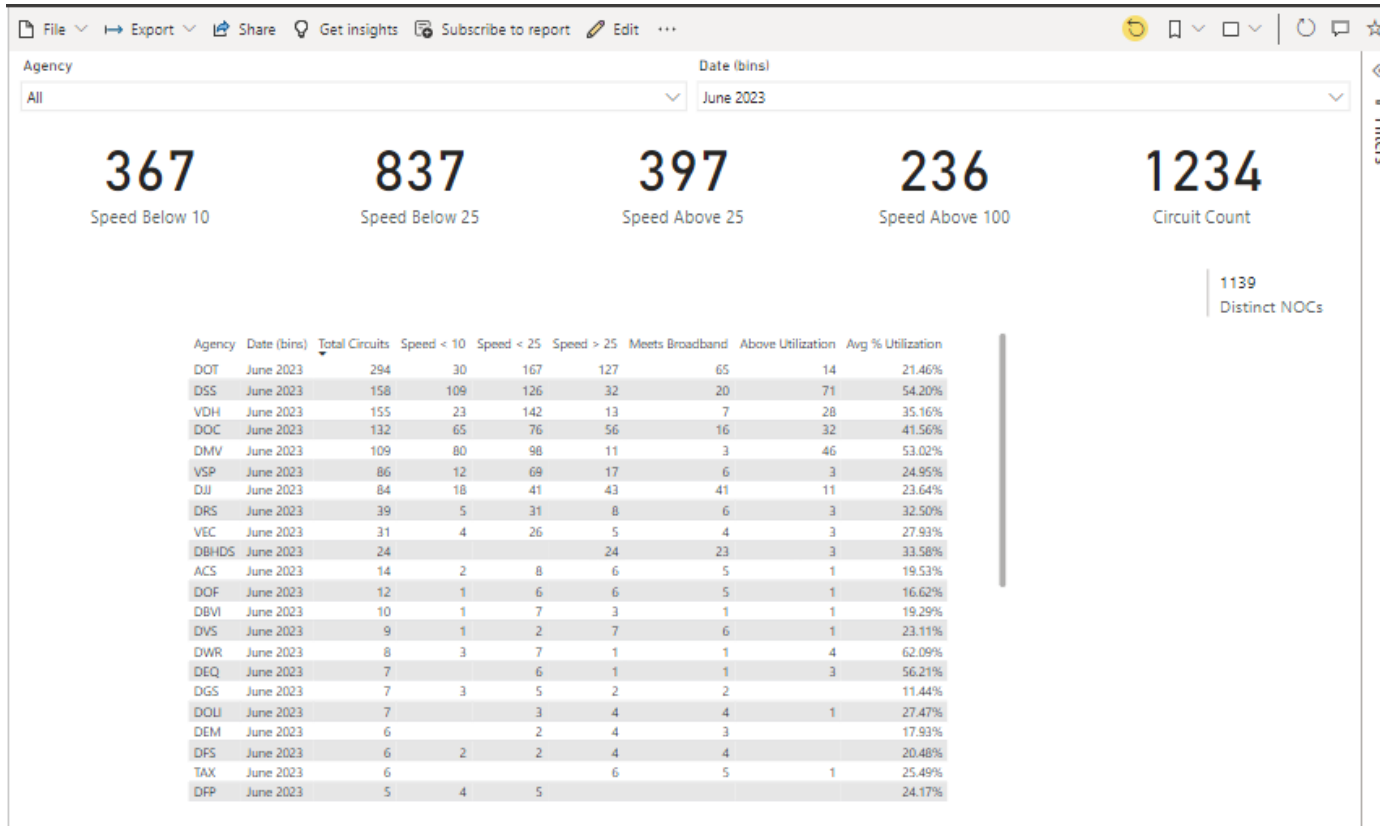
Total sites: 1,164

Current Challenges:

-  IOS upgrades
-  Scheduling
-  Demarcation and cabling
-  Circuit delivery
-  Site readiness
-  Overall communications

PROVIDE SINGLE SOURCE OF INFORMATION AND AGENCY-SPECIFIC REPORTING

- One source of truth
- Agency-specific reporting
- Roll up for executive level reporting



AGENCY COMPLETION REVIEW

Phase Status by Agency - SD-WAN Project								
Agency	Total Sites	IOS Complete	SDWAN Complete	Broadband Complete	IOS %	SDWAN %	Broadband %	Site %
VDOT	284	226	87	2	79.58%	30.63%	0.70%	Top 82%
VDH	159	144	130	62	90.57%	81.76%	38.99%	
DSS	143	131	104	33	91.61%	72.73%	23.08%	
DOC	119	97	58	3	81.51%	48.74%	2.52%	
DMV	91	87	85	27	95.60%	93.41%	29.67%	
DJJ	84	35	33	1	41.67%	39.29%	1.19%	
DARS	38	32	31	2	84.21%	81.58%	5.26%	
VEC	31	27	23	1	87.10%	74.19%	3.23%	
VSP	62	1	1	0	1.61%	1.61%	0.00%	
DVS	23	15	13	11	65.22%	56.52%	47.83%	
DBHDS	13	10	10	10	76.92%	76.92%	76.92%	
VDACS	14	8	8	0	57.14%	57.14%	0.00%	
DOF	12	8	7	0	66.67%	58.33%	0.00%	
DBVI	8	8	8	0	100.00%	100.00%	0.00%	
DWR	8	8	7	0	100.00%	87.50%	0.00%	
DEQ	7	6	6	6	85.71%	85.71%	85.71%	
DOLI	7	5	5	0	71.43%	71.43%	0.00%	
TAX	6	1	1	1	16.67%	16.67%	16.67%	
VITA	1	1	1	1	100.00%	100.00%	100.00%	
VDFP	5	5	1	1	100.00%	20.00%	20.00%	
DGS	4	0	0	0	0.00%	0.00%	0.00%	
VDEM	4	4	4	2	100.00%	100.00%	50.00%	
DFS	4	4	4	0	100.00%	100.00%	0.00%	
JYF	3	2	1	0	66.67%	33.33%	0.00%	
MRC	2	1	1	0	50.00%	50.00%	0.00%	
DHR	2	1	1	0	50.00%	50.00%	0.00%	
								Remaining 18%

Phase Status by Agency - SD-WAN Project								
Agency	Total Sites	IOS Complete	SDWAN Complete	Broadband Complete	IOS %	SDWAN %	Broadband %	Site %
DOA	1	1	0	0	100.00%	0.00%	0.00%	Remaining 18%
DPOR	1	1	1	1	100.00%	100.00%	100.00%	
DOAV	1	1	1	0	100.00%	100.00%	0.00%	
DRPT	1	1	1	0	100.00%	100.00%	0.00%	
VIPC	1	1	1	0	100.00%	100.00%	0.00%	
VMFA	1	1	1	0	100.00%	100.00%	0.00%	
DHCD	1	1	0	0	100.00%	0.00%	0.00%	
DHP	1	1	1	1	100.00%	100.00%	100.00%	
DMAS	1	1	0	0	100.00%	0.00%	0.00%	
ENERGY	1	1	0	0	100.00%	0.00%	0.00%	
LVA	1	1	0	0	100.00%	0.00%	0.00%	
VASAP	1	1	0	0	100.00%	0.00%	0.00%	
VRC	1	1	0	0	100.00%	0.00%	0.00%	
VSDB	1	1	0	0	100.00%	0.00%	0.00%	
GH	1	0	0	0	0.00%	0.00%	0.00%	
GOV	1	0	0	0	0.00%	0.00%	0.00%	
VBPD	0	0	0	0	0.00%	0.00%	0.00%	
VMNH	1	0	0	0	0.00%	0.00%	0.00%	

Completed Agencies		
VITA		
DPOR		
DHP		

Legend	
Total Sites	Total # Project Sites
IOS Complete	Project Sites where IOS Upgrade is Complete and approved by Agency
SDWAN Complete	Project Sites where SDWAN Upgrade is Complete and approved by Agency
Broadband Complete	Project Sites where Broadband Upgrade is Complete and approved by Agency

Data valid as of 7/21/2023.
 Data Source: Smartsheets Master Tracker
 COM-### Sites are not included in this data as it skew individual Agency information
 Broadband completion numbers are not inclusive of all broadband upgrades, they represent those sites that have been upgraded during the execution of this project.

IDENTIFYING SD-WAN ORDERS

When using TEBS to order broadband services

1. Order circuits using standard TEBS ordering options
2. In the **Service Order Number** field enter, SDWAN
3. Project name has also been used, **Service Order Number** is preferred

The use of this field will enable the VITA and Verizon teams to track SD-WAN-related orders to their associated NOCs

The screenshot displays the 'Work Order Search' interface. The top navigation bar includes 'Work Order Search' and 'Summarize By'. The main area is divided into several sections of search criteria:

- Work Order Search Criteria:** Work Order Number, Status, Cost Center, Job, Switch, Requesting User, Contact Email, Priority, Tasks For User, Notes, Technician Group.
- Project Information:** Project Name, Project Number, Site Contact Number, NSP Number/ACK, Vendor, Service Request Type, Internal Remarks 2, Internal Remarks 4, Ship To (Name).
- Personnel and Location:** Technician, Service Location, User Phone, Vendor Ticket, Vendor, Contact Phone, User Email, Entered By.
- Advanced Search:** START, Date, To.
- Additional Fields:** Work Order Batch ID, Site Contact Name, Service Request Number (SR#), Service Order Number (highlighted in yellow), Expedite Order? Charges Apply, Internal Remarks 1, Internal Remarks 3, Internal Remarks 5.

At the bottom, there is a 'Page Size' dropdown set to 20 and a 'Show Closed?' checkbox. A 'Search' button is located at the bottom right.



Process improvements to help accelerate the initiative:

- CradlePoint wireless WAN option for the most critical sites encountering broadband delivery or network issues

[Frequently Asked Questions - Wireless Wide-Area Network Access \(WWA\) FAQ \(virginia.gov\)](#)

- Site-specific project checklist and demarcation with site inspection validation, either remote or in-person
- Hot swap of routers, reducing downtime for agency
- Operating between hours of 7 a.m. and 7 p.m. for site scheduling flexibility



- [CradlePoint](#) is a router that provides flexible, reliable connectivity and provides security control
- Available CradlePoint routers - IPSec compatible
 - Small office or remote office (SORO): A router equipped with 5 x 1 GB LAN/WAN ports. Single power supply.
 - Branch office (BO): A router is equipped with 10 x 1 GB LAN/WAN ports. Single power supply.
- Features and benefits
 - Available for existing and new SD-WAN customers updating or adding a new location to their network
 - Managed WAN service with a WWA router accelerates site turn-up by providing cellular wireless connectivity
 - Fast site service speeds without the special construction costs often found to bring ethernet service feeds
 - It allows access to mission-critical business applications, even during dedicated wireline circuit provisioning
- Requirements
 - SD-WAN or ~~Secure Gateway~~ [New Orders will be handled with SD-WAN]
 - SIM card
- Ordering
 - Cradlepoint requests are placed through the [VITA service portal](#)
 - Tactical teams will assist agencies with Cradlepoint ordering in conjunction with their sites SD-WAN upgrades

PROJECT OVERVIEW – SD-WAN/BROADBAND



Service item	Supplier	Why needed?	When to order?	Ordering platform
SD-WAN	Verizon	<ul style="list-style-type: none"> Included in transformation 	<ul style="list-style-type: none"> n/a 	<ul style="list-style-type: none"> n/a
Direct internet access (DIA)	ATOS	<ul style="list-style-type: none"> Required for locations with secondary or standalone broadband connection 	<ul style="list-style-type: none"> Once location has been migrated to SD-WAN 	<ul style="list-style-type: none"> Service catalog – SCTask
CPE (Router)	Verizon	<ul style="list-style-type: none"> If agency location cumulative bandwidth exceeds 150M (via single circuit or dual circuit combined); or if project team determines upgrade is required 	<ul style="list-style-type: none"> Once location has been migrated to SD-WAN 	<ul style="list-style-type: none"> Service catalog – SCTask
MPLS	Verizon	<ul style="list-style-type: none"> Secondary dedicated access with SLA. DIA will not apply here, and all traffic will route through QTS 	<ul style="list-style-type: none"> Once location has been migrated to SD-WAN 	<ul style="list-style-type: none"> Service catalog – SCTask
Wireless WAN access and SIM card/data plan AKA Cradlepoint	Verizon and third-party	<ul style="list-style-type: none"> Secondary wireless access with SLA 	<ul style="list-style-type: none"> Once location has been migrated to SD-WAN 	<ul style="list-style-type: none"> Service catalog - SCTask TEBS - SIM card/data plan
Broadband circuit	Third-party	<ul style="list-style-type: none"> Secondary dedicated access without SLA 	<ul style="list-style-type: none"> Once location has been migrated to SD-WAN 	<ul style="list-style-type: none"> TEBS – multiple providers available

QUESTIONS

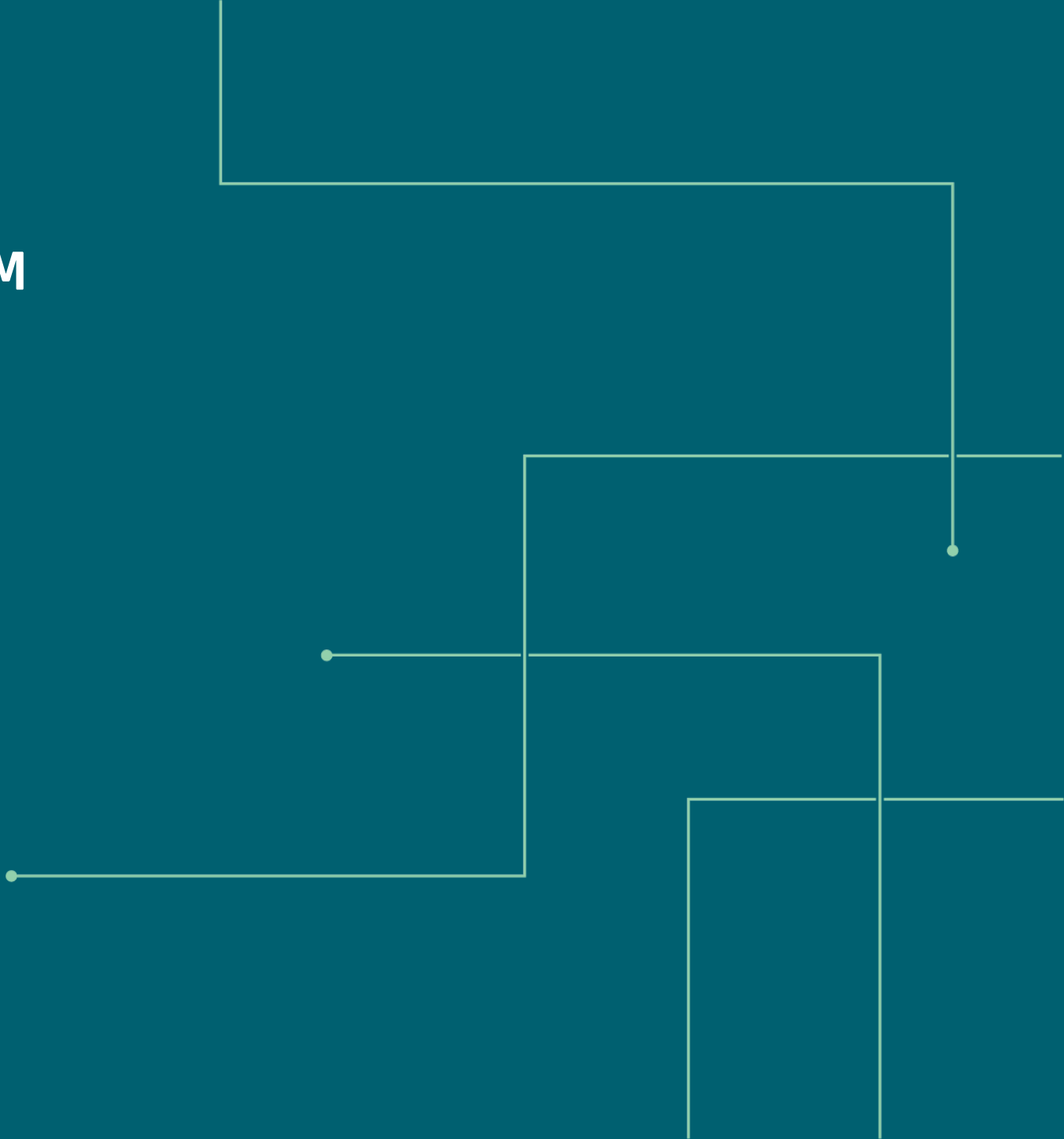




WEBSITE MODERNIZATION PROGRAM ISOAG MEETING

JOSHUA JONES
Program Manager

AUGUST 2, 2023





- Program vision and goals
- Updates
- Tools and services
- Next steps

Vision

- Improve citizen trust and engagement with Virginia government websites by providing modern, consistently-branded Commonwealth websites that are secure, Section 508 accessible and digitally responsive





Nucleus

Global Dashboard

Vulnerability Overview

Single High Risk	Unique CVEs	Unique Exploits	Total High Risk	Total CVEs	Total Exploits
2.3k	3.6k	776	87.5k	20.0k	9.6k

Projects

Project Name	Project Type	High Risk	Medium Risk	Low Risk	Score	Severity	Age	Exploits
Project A	Web	100	50	20	8.5	Critical	10	5
Project B	Mobile	750	300	100	7.2	High	20	10
Project C	Network	150	80	30	9.1	Critical	5	2
Project D	Cloud	500	250	100	6.8	High	15	8

Most Vulnerable Projects

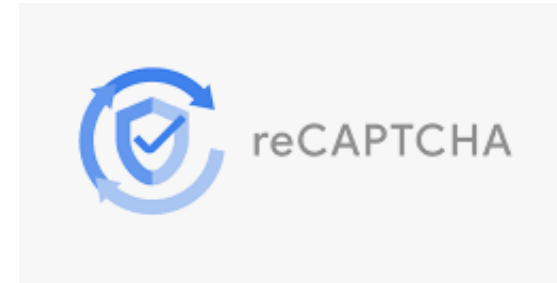
Project Name	Score	# Assets	Severity	Age
Project A	8.5	100	Critical	10
Project B	7.2	750	High	20
Project C	9.1	150	Critical	5
Project D	6.8	500	High	15

Latest Scans

Scan ID	Source	# Assets	Severity	Age
SCAN-01	192.168.1.1	1	Critical	10
SCAN-02	192.168.1.1	1	High	20
SCAN-03	192.168.1.1	1	Critical	5

Nucleus

VULNERABILITY & RISK MANAGEMENT PLATFORM



2007

2012

2018

2020

```
<script src="https://www.google.com/recaptcha/api.js" async defer></script>  
<script>  
  grecaptcha.ready(function() {  
    grecaptcha.execute('reCAPTCHA_site_key', {  
      action: 'homepage' }).then(function(token) {  
      // ...  
    });  
  });  
</script>
```

2020





Questions

???



CSRM THREAT MANAGEMENT TOOLS/UPDATE

GREG LYONS

CSRM/IT Project Manager

**INFORMATION SECURITY OFFICERS
ADVISORY GROUP**

AUGUST 2ND, 2023



ACCUNETIX A360 VULNERABILITY SCANNER

- **Challenge**: Vulnerability scanning was manual, slow, and generated large reports that were difficult to interpret. Agencies had no ability to manage or view their own information without a request to VITA. Remediation took several back-and-forth conversations between the agency and VITA to resolve, slowing our response.
- **Solution**: Acunetix 360 SaaS solution.
- **Benefit**: A360 enables agencies to view all of their web app vulnerabilities, run their own full scans at will, run remediation scans, and provide access to their web/sec teams to ensure vulnerabilities can be remediated in a timely fashion. PDF reports are replaced by dashboard views of agency vulnerabilities. Threat Management time has been freed by A360 automation so they can focus on providing more SME advice and remediation help to agencies.

Deployed in June – live in production now

SPLUNK SIEM

- **Challenge**: Providing agencies enterprise log data for their agency was difficult at best. Agencies had no ability to manage or view their own information without a request to VITA.
- **Solution**: Splunk SIEM setup for Multi-Tenant
- **Benefit**: Splunk will give agency ISOs access to dashboards and raw logs tailored only to their agencies data. This will allow them to see and manage their logs in real time. They now have instant access to clear, concise log reporting in place of a slow, manual request process.

Initial access and dashboards to be deployed Sept/Oct
(M365/Crowdstrike)

NUCLEUS VULNERABILITY MANAGEMENT SOFTWARE

- **Challenge:** Currently our process to track vulnerabilities and their remediation is manual, challenging, and inaccurate. Tenable and Acunetix vulns are tracked in separately in respective software. ISO's cannot easily see their agency level vulnerabilities and have trouble knowing which ones they are responsible to remediate.
- **Solution:** Nucleus Sec Vulnerability Management SaaS solution
- **Benefit:** Agency ISOs will receive access to Nucleus which will provide them a single pane of glass view of vulnerabilities for their agency. Initial data inputs are Tenable Nessus and Acunetix 360. It will clearly tell them which vulnerabilities are unresolved, if the tower or agency is responsible, and allow ISOs to directly track resolution.

Initial access and dashboards to be deployed later this
year



Questions



COV Tabletop Exercise 2023

Zachary D. Wilton
SAIC MSI Security Incident Response

Agenda

- Overview
- Objectives
- Expected Outcomes
- Event Information



Overview

The COV Annual Tabletop Exercise is an unclassified, adaptable exercise developed by the MSI/MSS for the Commonwealth of Virginia. The main purpose is to evaluate performance of the multisupplier model, promote dialogue around opportunities for continuous improvement, and identify recommendations for improvement for the COV Cybersecurity Incident Response process.



Objectives

- The main objective for this exercise is to uncover strengths within the COV IR process:
 - Evaluate the Service Delivery capability for detecting, responding to, and recovering from simulated, realistic events
 - Evaluate Service Delivery communication and responsiveness
 - **Run the event through the Service Delivery and State Agency Incident Response plans, identify opportunities for alignment, and any gaps in Service Delivery execution**
 - Provide recommendations for corrective action to VITA-CSRMM



Expected Outcomes

- Expected outcome from this event is to conduct a tabletop event where coordination of multiple Suppliers and Service Delivery ensures COV information systems will successfully operate in support of the exercise scenario, and when the managed environment is under attack.
 - Demonstrate successful coordination of multiple Supplier Service Delivery
 - Ensure COV information systems will successfully operate in support of the exercise scenario
 - Enhance awareness, readiness and coordination
 - Test capability to determine operational impacts of a cyberattack
 - Test participant's exercise playbooks, incident analysis, incident response plans and procedures, and incident reporting
 - Demonstrate compliance with MSI Security Incident Management Process SMM 4.1.5.7 and VITA Playbooks
 - Identify Enterprise-wide opportunities for improvement
 - Further integration of multi sourcing program between MSI, VITA-CSR, Service Towers, and the Agencies



Event Information

- **When:**
 - Exercise is Thursday, Oct 26th, 2023, Time is TBD*
 - Hotwash is Friday, Oct 27th, 2023, Time is TBD*
- **Who:**
 - Hosted by MSI SIRT team, ATOS Security, and VITA CSRM
 - Participants include representatives from each agency and service tower (Last year had over 50)
- **Where:**
 - Virtual option will be available for all participants, link will be provided in invitation
 - Physical option still TBD*

Additional information will be provided

Event Information

- How to join:

- An email will be sent out weekly to all ISO's (expect this to start within 1-2 weeks) requesting a response to sign-up, if your agency/tower has not done so already.
- You are also always welcome to send an email to MSI-Security-Operations@saic.com stating that your agency/tower would like to participate in this year's event

Cut-off date: Friday, Oct 14th, 2023

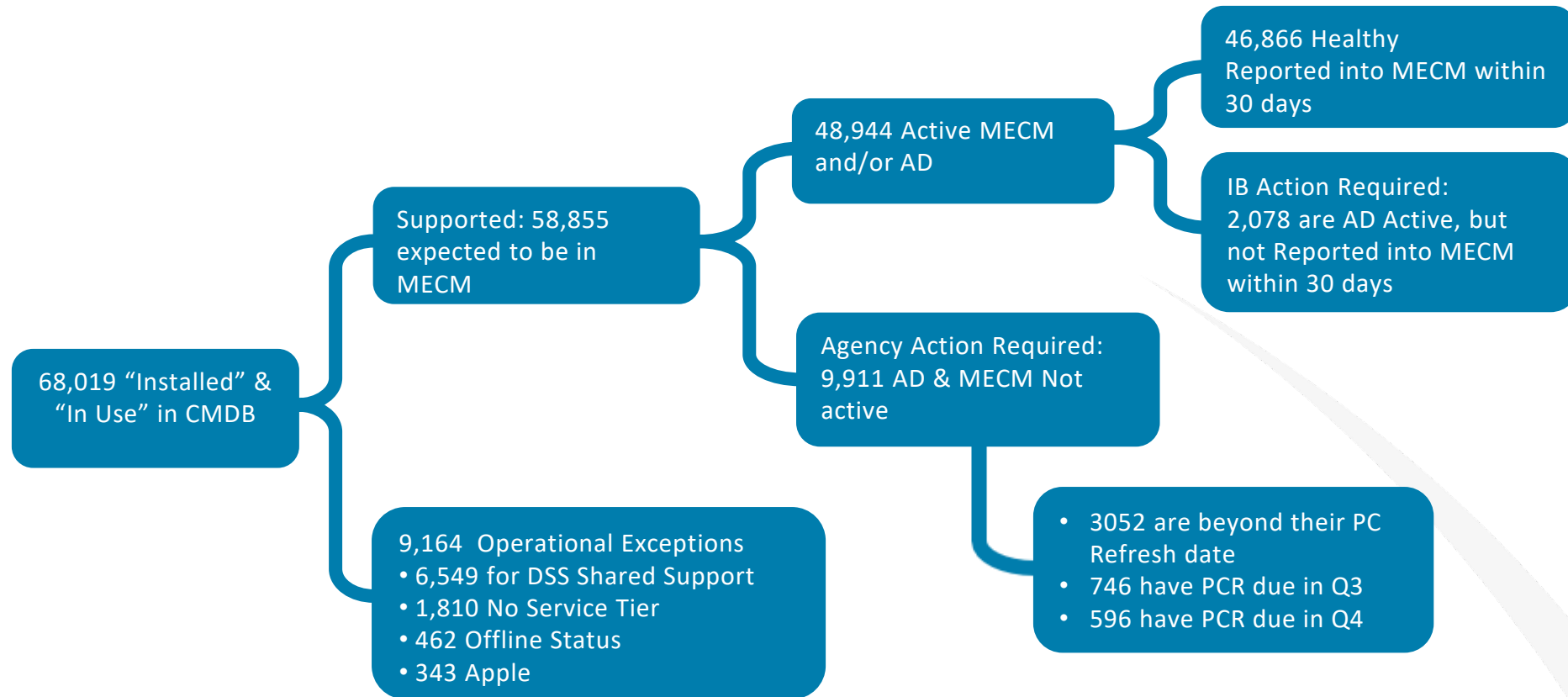
**Please direct all questions about the exercise to
MSI-Security-Operations@saic.com**





End User Computing Patching Report June 2023

MECM Agent Health Metrics



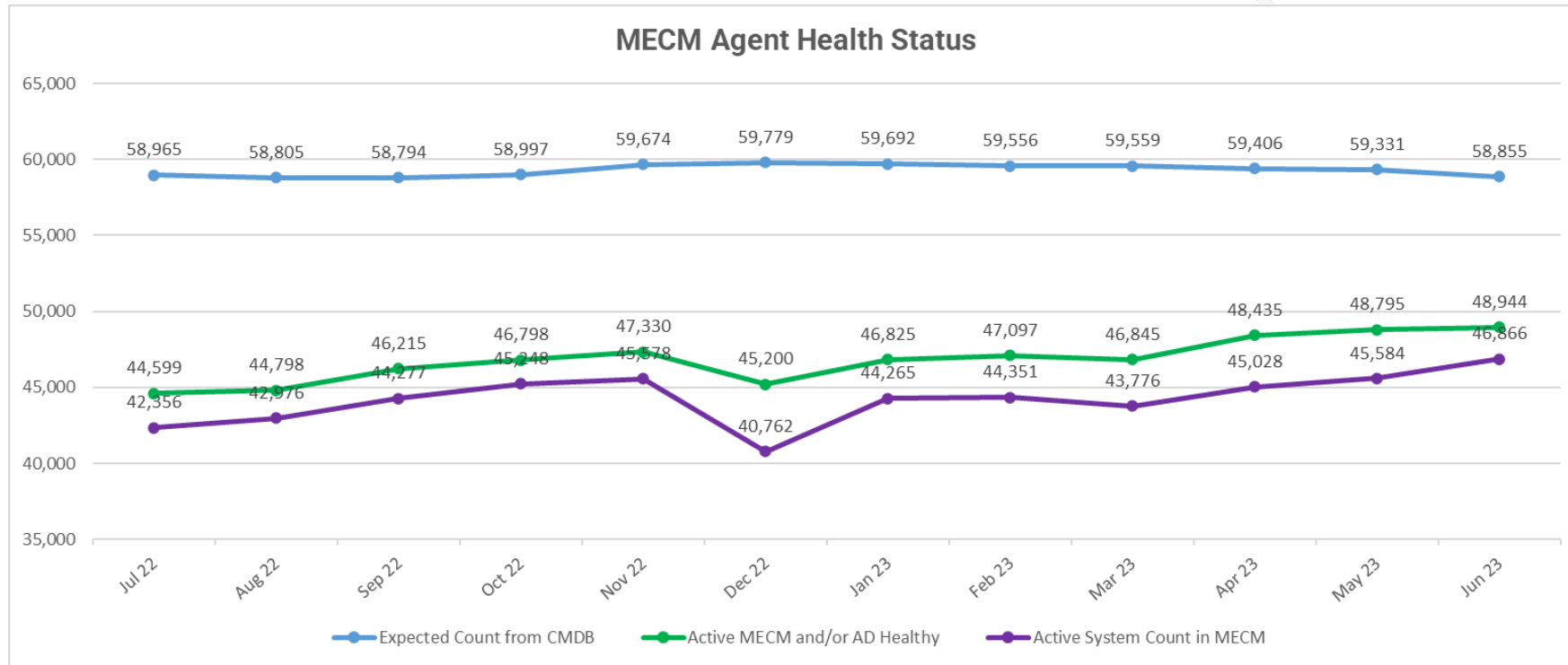
Operational view of KM 2.3.8 is that 95.75% of devices have checked in electronically

- These numbers represent an operational view and calculation of the KM metric. They do not represent the final KM metrics.

MECM Agent Health Status

MECM Agent Health Status						
Date	Expected Count from CMDB *	Active MECM and/or AD Healthy	Active System Count in MECM **	IB Action Required: AD Active but MECM not active	Agency Action Required: AD & MECM not active	Active Systems
Apr 23	59,406	48,435	45,028	3,407	10,971	92.97%
May 23	59,331	48,795	45,584	3,211	10,536	93.42%
Jun 23	58,855	48,944	46,866	2,078	9,911	95.75%

*Expected Count = Does not include DSS shared support
**Active = Have reported vulnerability scan data into MECM within 30 days



June 2023 - Data as of 07/03/2023



Workstation Patching

Patches 60 days and older

Workstation Patching - Patches 60 days and older

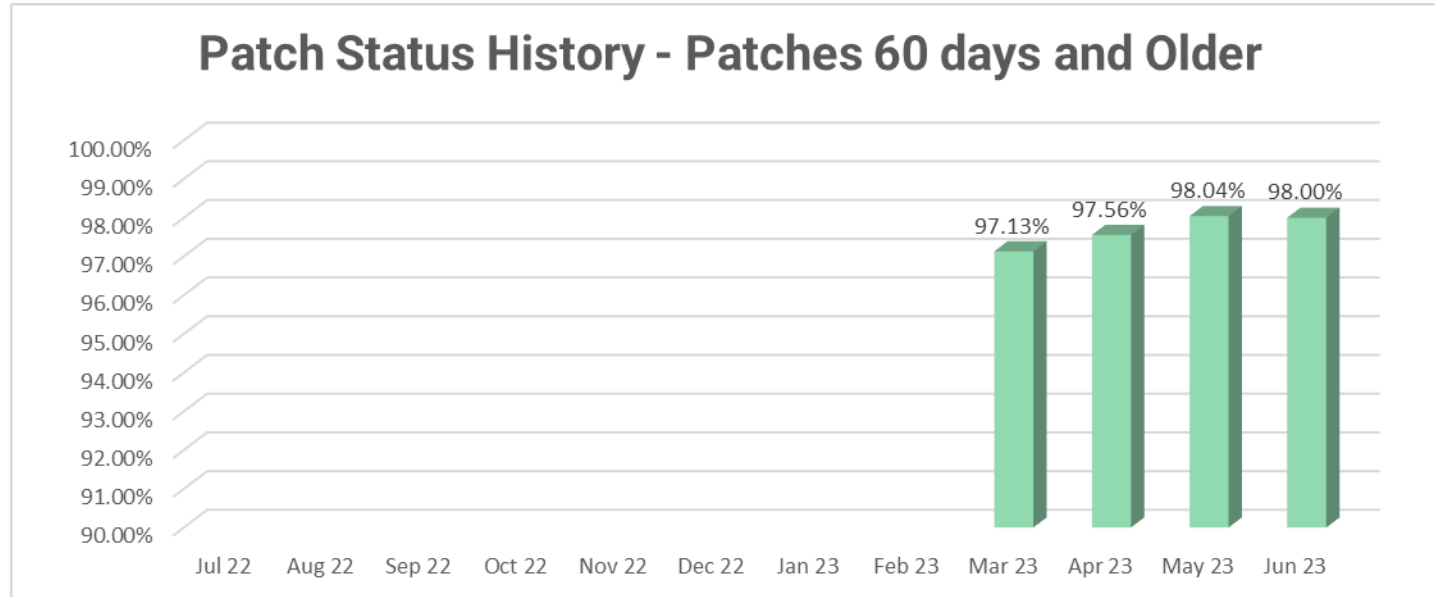
Patches 60 days an older

In Scope Workstations		
Eligible for Security Patching *Have reported vulnerability scan data into Nessus & MECM within 30 days *Have reported vulnerability for a patch that is 60 days or older	46,134	99.09%
Operational Exceptions	423	0.91%
Total Systems *All Systems that are Installed - In Use in KSE (Excluding DSS Shared Support)	46,557	

Security and Vulnerability Patching Compliance		
Fully Patched Systems (Current Systems)	45,211	98.00%
Missing Patches (Current Systems)	923	2.00%

Operational Exceptions	Count
OE II - 1809 Out of support	19
OE II - 1909 Out of support	139
OE II -Win7 Out of support	1
OE III - Install less than 30 days	56
OE III - No AD Logon in 30 days	78
OE III - Offline Service Tier	2
OE III - Pending Reboot	128

Patch Status History



These numbers represent an operational view and calculation of the KM metrics. They do not represent the final KM metrics.

Patch Status By Agency (Over 60 days)

AGENCY Cost Centers	Compliant + exceptions	Patching compliant, operational exceptions, or noncompliant			Total	Compliant %	Exception %	Noncompliant %
		97.11% Yes	0.91% OE	1.98% No				
ATS - 8801	95.83%	23		1	24	95.83%	0.00%	4.17%
BOA - 0226	100.00%	11			11	100.00%	0.00%	0.00%
CASC - 0957	100.00%	6			6	100.00%	0.00%	0.00%
CCCA - 0708	98.80%	82		1	83	98.80%	0.00%	1.20%
CH - 0724	100.00%	194			194	100.00%	0.00%	0.00%
CSA - 0200	100.00%	8			8	100.00%	0.00%	0.00%
CSH - 0703	99.06%	526	2	5	533	98.69%	0.38%	0.94%
CVTC - 0707	100.00%	1			1	100.00%	0.00%	0.00%
DARS - 0262	92.07%	453	23	41	517	87.62%	4.45%	7.93%
DBHDS - 0720	98.92%	546	3	6	555	98.38%	0.54%	1.08%
DBVI - 0702	84.57%	140	8	27	175	80.00%	4.57%	15.43%
DCJS - 0140	98.29%	172		3	175	98.29%	0.00%	1.71%
DCR - 0199	99.42%	510	1	3	514	99.22%	0.19%	0.58%
DEQ - 0440	99.45%	726	1	4	731	99.32%	0.14%	0.55%
DFS - 0778	100.00%	364			364	100.00%	0.00%	0.00%
DGS - 0194	93.26%	630	6	46	682	92.38%	0.88%	6.74%
DHCD - 0165	100.00%	155			155	100.00%	0.00%	0.00%
DHP - 0223	97.66%	331	3	8	342	96.78%	0.88%	2.34%
DHR - 0423	100.00%	57			57	100.00%	0.00%	0.00%
DHRM - 0129	98.13%	105		2	107	98.13%	0.00%	1.87%
DJJ - 0777	98.61%	1400	16	20	1436	97.49%	1.11%	1.39%
DMAS - 0602	99.50%	595	1	3	599	99.33%	0.17%	0.50%
DMV - 0154	100.00%	2023			2023	100.00%	0.00%	0.00%
DOA - 0151	96.82%	274		9	283	96.82%	0.00%	3.18%
DOAV - 0841	100.00%	30			30	100.00%	0.00%	0.00%
DOC - 0701	98.80%	6973	11	85	7069	98.64%	0.16%	1.20%
DOE - 0201	98.81%	581	2	7	590	98.47%	0.34%	1.19%

Patch Status By Agency (Over 60 days) cont.

AGENCY Cost Centers	Compliant + exceptions	Patching compliant, operational exceptions, or noncompliant			Total	Compliant %	Exception %	Noncompliant %
		97.11% Yes	0.91% OE	1.98% No				
DOF - 0411	96.22%	170	8	7	185	91.89%	4.32%	3.78%
DOLI - 0181	99.44%	176	2	1	179	98.32%	1.12%	0.56%
DPB - 0122	100.00%	21			21	100.00%	0.00%	0.00%
DPOR - 0222	95.04%	227	3	12	242	93.80%	1.24%	4.96%
DRPT - 0505	100.00%	54			54	100.00%	0.00%	0.00%
DSBSD - 0350	100.00%	59			59	100.00%	0.00%	0.00%
DSS - 0765	94.90%	5,653	149	312	6,114	92.46%	2.44%	5.10%
DVS - 0912	98.53%	466	4	7	477	97.69%	0.84%	1.47%
DWR - 0403	99.68%	315		1	316	99.68%	0.00%	0.32%
ELECT - 0132	100.00%	84			84	100.00%	0.00%	0.00%
ENERGY - 0409	96.97%	223	1	7	231	96.54%	0.43%	3.03%
ESH - 0704	99.56%	454		2	456	99.56%	0.00%	0.44%
FCMV - 0239	100.00%	4			4	100.00%	0.00%	0.00%
GH - 0417	92.31%	12		1	13	92.31%	0.00%	7.69%
GOV - 0121	100.00%	273			273	100.00%	0.00%	0.00%
HDMC - 0748	99.09%	109		1	110	99.09%	0.00%	0.91%
IBT - 8800	100.00%	95			95	100.00%	0.00%	0.00%
JYF - 0425	100.00%	172			172	100.00%	0.00%	0.00%
LVA - 0202	96.84%	92		3	95	96.84%	0.00%	3.16%
MRC - 0402	100.00%	78			78	100.00%	0.00%	0.00%
MVDB - 0506	100.00%	15			15	100.00%	0.00%	0.00%
NTT - 8808	100.00%	4			4	100.00%	0.00%	0.00%
NVMHI - 0728	98.61%	213		3	216	98.61%	0.00%	1.39%
ODGA - 0167	100.00%	17			17	100.00%	0.00%	0.00%
OSIG - 0147	97.78%	44		1	45	97.78%	0.00%	2.22%
PGH - 0729	100.00%	246			246	100.00%	0.00%	0.00%
SAIC - 8803	100.00%	14			14	100.00%	0.00%	0.00%
SBVCC - 0922	93.88%	46		3	49	93.88%	0.00%	6.12%
SCB - 0157	100.00%	21			21	100.00%	0.00%	0.00%
SCHEV - 0245	94.67%	70	1	4	75	93.33%	1.33%	5.33%

Patch Status By Agency (Over 60 days) cont.

AGENCY Cost Centers	Compliant + exceptions	Patching compliant, operational exceptions, or noncompliant			Total	Compliant %	Exception %	Noncompliant %
		97.11% Yes	0.91% OE	1.98% No				
SEVTC - 0723	94.92%	186	1	10	197	94.42%	0.51%	5.08%
SVMHI - 0739	100.00%	133			133	100.00%	0.00%	0.00%
SWMHI - 0705	99.36%	309	1	2	312	99.04%	0.32%	0.64%
TAX - 0161	96.00%	1192	7	50	1249	95.44%	0.56%	4.00%
TRS - 0152	99.23%	129		1	130	99.23%	0.00%	0.77%
UNYS - 8805	100.00%	29			29	100.00%	0.00%	0.00%
VASAP - 0413	100.00%	2			2	100.00%	0.00%	0.00%
VBPD - 0606	100.00%	10			10	100.00%	0.00%	0.00%
VCA - 0148	100.00%	5			5	100.00%	0.00%	0.00%
VCBR - 0794	99.56%	225		1	226	99.56%	0.00%	0.44%
VDACS - 0301	87.82%	308	2	43	353	87.25%	0.57%	12.18%
VDDHH - 0751	100.00%	11			11	100.00%	0.00%	0.00%
VDEM - 0127	90.75%	157		16	173	90.75%	0.00%	9.25%
VDFP - 0960	96.55%	83	1	3	87	95.40%	1.15%	3.45%
VDH - 0601	98.73%	5641	29	73	5743	98.22%	0.50%	1.27%
VDOT - 0501	98.89%	6685	17	75	6777	98.64%	0.25%	1.11%
VEC - 0182	100.00%	1171	61		1232	95.05%	4.95%	0.00%
VIPC - 0309	100.00%	18			18	100.00%	0.00%	0.00%
VITA - 0136	100.00%	251			251	100.00%	0.00%	0.00%
VMFA - 0238	99.66%	291		1	292	99.66%	0.00%	0.34%
VMNH - 0942	100.00%	7			7	100.00%	0.00%	0.00%
VRC - 0405	100.00%	8			8	100.00%	0.00%	0.00%
VRCBVI - 0263	57.14%	4		3	7	57.14%	0.00%	42.86%
VSDB - 0218	83.33%	10		2	12	83.33%	0.00%	16.67%
VSP - 0156	100.00%	1338	20		1358	98.53%	1.47%	0.00%
VVCC - 0128	100.00%	30			30	100.00%	0.00%	0.00%
VZN - 8806	100.00%	41			41	100.00%	0.00%	0.00%
WSH - 0706	99.33%	442		3	445	99.33%	0.00%	0.67%
WWRC - 0203	97.95%	152	39	4	195	77.95%	20.00%	2.05%
Grand Total	98.02%	45211	423	923	46557	97.11%	0.91%	1.98%



CYBERSECURITY AWARENESS TRAINING FOR THE COMMONWEALTH

Tina Gaines
KnowBe4 Team Lead
CSRM





- KnowBe4 Training
 - a. Agencies should have started uploading their users and creating training campaigns
 - b. Agencies should have participated in the KB4/OKTA testing
 - c. All agencies should have training programs up and running by September 31, 2023

Note: We are halfway through the calendar year, if your agency has not participated in any of the above, Please contact CSRM to get started.



What VITA Is Working on:

- Providing continuing KB4 Support to agencies
- Working on the issue of not being able to add non domain users to the KB4 platform
- Working on the issue of how to provide training to agency localities
- Activating the PAB (Phish Alert Button) enterprise wide.
- Enterprise KB4/Okta integration.
VITA has completed testing the KnowBe4/Okta integration. The following phases have been completed.
 - Phase One - June 28th
 - Phase Two - July 10th.
 - Phase Three – July 17th
 - Phase Four – July 24th





UPCOMING EVENTS



COMMONWEALTH OF VIRGINIA INFORMATION SECURITY (IS) CONFERENCE 2023



Revolutionizing IS through Advanced Thinking:
Unleashing the Power of Human Ingenuity and AI

Save the date for the most innovative Commonwealth of Virginia Information Security conference, yet!

Date: August 17, 2022

Time: 8a – 3p

Cost \$125

<https://www.vita.virginia.gov/information-security/security-conference/>

Location: Hilton Richmond Hotel and Spa/Short Pump at 12042 West Broad Street, Richmond, VA 23233.

Join us for a day of thought - provoking discussions and networking opportunities with industry experts.

Keynotes:

Paul Chin Jr., Serverless Developer (Chat GPT)

Elham Tabassi, NIST (NIST AI Framework)





Any conference related questions may be sent to:

commonwealthsecurity@vita.virginia.gov

COMMONWEALTH OF VIRGINIA
INFORMATION SECURITY (IS)
CONFERENCE 2023

**Revolutionizing IS through Advanced Thinking:
Unleashing the Power of Human Ingenuity and AI**



Elham Tabassi is a Senior Research Scientist at the National Institute of Standards and Technology (NIST) and the Associate Director for Emerging Technologies in the Information Technology Laboratory (ITL). She leads the NIST Trustworthy and Responsible AI program that aims to cultivate trust in the design, development and use of AI technologies.

She has been working on various machine learning and computer vision research projects with applications in biometrics evaluation and standards since she joined NIST in 1999.

She is a member of the National AI Resource Research Task Force, vice-chair of Organization for Economic Cooperation and Development (OCED) working party on AI Governance, Associate Editor of Institute of Electrical and Electronics Engineers (IEEE) Transaction on Information Forensics and Security and a fellow of Washington Academy of Sciences.



Paul is a curious human. He is passionate about exploring technology, art, and business. He advocates for making technology accessible and growing communities to help one another. He has created new markets, guided start-up validations, and architected enterprise platforms. The future is amazing, and he can't wait to help you build it.



- Jenny Heflin, Managing Director at Accenture
- Dr. Andrea M. Matwyshyn, Associate Dean for Innovation and Technology, Penn State Law
- Glenn Schmitz, Chief Information Security Officer, Virginia Department of Behavioral Health and Developmental Services
- Beth Burgin Waller, Chair, Cybersecurity and Data Privacy at Woods Rogers Vandeventer Black
- Michael Watson, Chief Information Security Officer, Virginia Information Technologies Agency
- Wendy Wickens, Cisco



- Cory Bannerman – FCTO Public Sector
 - Angus Chen – Cybersecurity Professional, Kerberos
 - Nick Popovich – Principal, Rotas Security LLC
 - Dr. Matthew McFadden, General Dynamics IT
-
- <https://www.vita.virginia.gov/information-security/security-conference/conference-program/#acc-sconfscedule>



COVITS 2023
Wednesday, September 13, 2023
Open to Public Sector only.

Registration — \$45

<https://events.govtech.com/covits.html>

September ISOAG MEETING

September 6, 2023

TIME 1 P.M. - 3 P.M.

Arnold Webster / Benjamin Gilbert - Cybersecurity and Infrastructure Security Agency
Greg Lyons - VITA/CSRM IT Project Manager
Sonya Shearon Hefferan - Tenable Security Specialist

The next scheduled IS Orientation:

September 27, 2023

12 p.m. - 1 p.m. (virtual)

Presenters: Erica Bland
Renea Dickerson
Tina Gaines

<https://covaconf.webex.com/weblink/register/rdc14adee106e50193fac4c9f549ba925>

The next scheduled meeting for the IS Council:

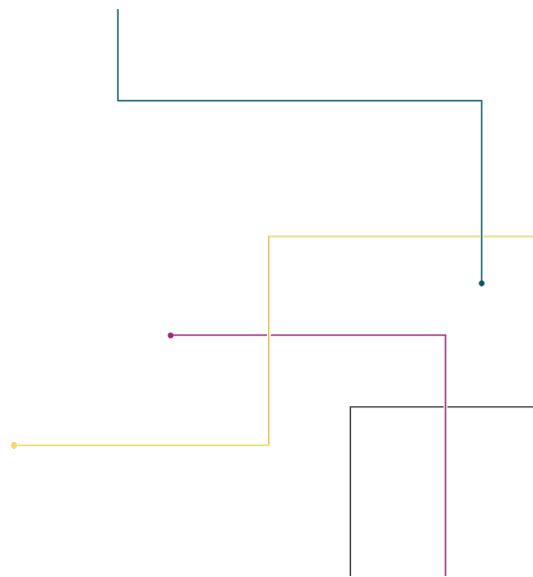
September 20, 2023

12 p.m. - 1 p.m. (virtual)

If you would like an invite to the meeting, contact:

Johanna.Opolski@vita.virginia.gov

**MEETING
ADJOURNED**



**VIRGINIA
IT AGENCY**