WELCOME TO THE April ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

April 2, 2025

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Kendra Burgess/VITA
VFC Cyber Program	Chris Cruz/VSP, VFC and Scott Brinkley/ VITA
Server Vulnerability Compliant Patching Schedule	John Del Grosso/VITA
Cyber Vault Service (CVS)	John Del Grosso/VITA
Announcements & Upcoming Events	Kendra Burgess/VITA
Adjourn	

VFC Cyber Program

Program Overview

UNCLASSIFIED // FOR OFFICIAL USE ONLY

SCIENTIA EST POTENTIA

SCIENTIA EST POTENTIA

Cyber Program History

2013

Cyber Coverage

0.5 (FTE) CIKR Analyst assigned to cyber

2014-2015

Cyber Support

1 Senior Analyst

1 Special Agent

2016-2022

Cyber Team

1 Lead Analyst

3 Senior Analysts

Required Reporting

Virginia Code § 2.2-5514 – Required cyber incident reporting to VFC

2022

Cyber Program

1 Program Manager

1 Lead Analyst

3 Senior Analysts

2023

VFC Cyber

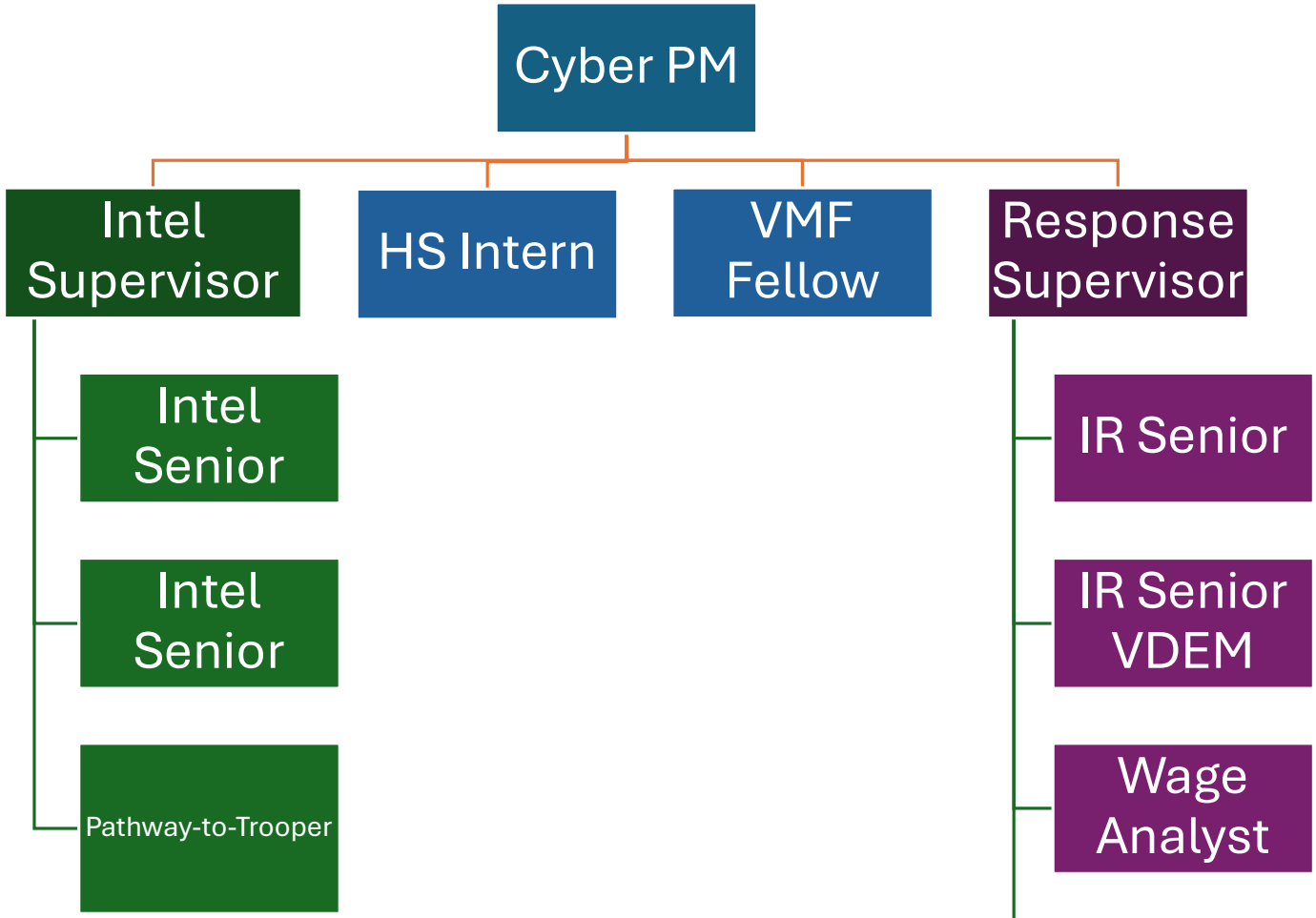
1 Program Manager

2 Supervisors (IR & Intel)

6 Analysts / 1 Fellow

Current Staffing

SCIENTIA EST POTENTIA



SCIENTIA EST POTENTIA

Current Cyber Capabilities

Threat Intelligence & Info Sharing

Prioritize, collect, and analyze reports and data on cyber risks and threats with a nexus to Virginia. Produce and distribute products to need-to-know partners.

Incident Response & Coordination

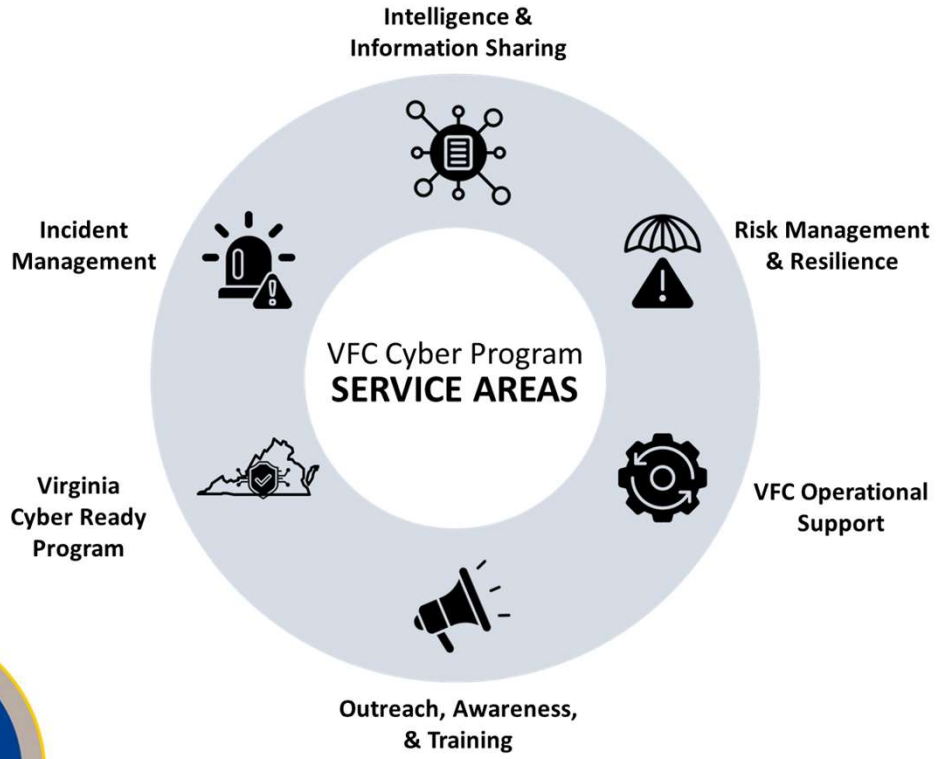
Virginia § 2.2-5514, cyber incidents are reported to VFC within 24 hours. When requested, VFC coordinates response and supporting partners. May activate Cyber Response Task Force (CRTF).

Stakeholder Engagement

Support and participate in exercises. Provide sector-specific threat briefings when requested. Engage with multiple associations. Assist SLTT partners in locating resources.

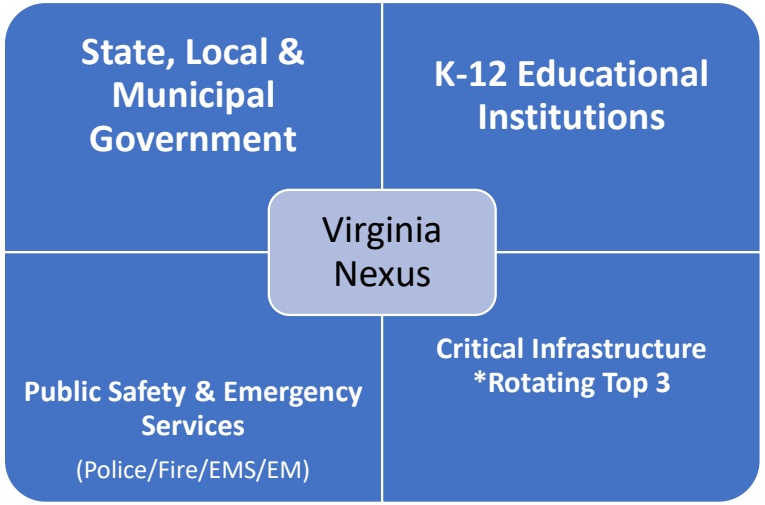
SCIENTIA EST POTENTIA

VFC Cyber Program



Critical Stakeholders

Critical Stakeholders represent priority areas for partnership, outreach, intelligence collection, & delivering products & services.



- Drive intelligence collection for these groups
- Prioritize engagements with these groups
- New ideas/projects should favor these groups

Risk Management & Resilience: Special Project - VAST

- **Description:** Review public-facing infrastructure for SLTT entities and notify them of high risk issues/vulnerabilities – proactive work to reduce the likelihood of successful attacks.
- **Project Goal:** Double stakeholders onboarded.

Working to better formalize this capability during pilot:

- Documenting internal procedures [complete]
- Standardizing notifications [complete]
- Establish improved baseline for alert thresholds [in progress]

Intelligence & Information Sharing
Special Project: PISCES

- **Project Description:** Platform for Intelligence Sharing and Cybersecurity Engagement Services (PISCES) – HSIN Community of Interest for Cyber
  - Re-building / re-branding HSIN Cyber COI (formerly SHIELD) [in progress]
  - Act as primary cyber product library for Virginia [in progress]
    - Aggregates intel products from multiple entities/sectors
    - Searchable
    - Increases engagement opportunities
  - Ability to virtually interface with VFC Cyber [complete]
    - Request assistance, submit RFI's, ask questions, etc.
    - Develop into a "Virtual Fusion Center" concept for cyber

SCIENTIA EST POTENTIA

Risk Management & Resilience: Special Project – CIRP-in-a-Box

- **Description:** Cyber Incident Response Plan-in-a-Box offers guidance, templates, and checklists for SLTT entities needing to develop an incident response plan from scratch or
- **Project Goal**: Version 1.0 [complete] – tested with several local and state agencies. Workshopped at APCO/NENA conference.

Future work will include growth into a Cyber Annex (CAnnex) option:

VIRGINIA FUSION CENTER

Quarterly Cyber Meeting

INTELLIGENCE BRIEFING

03/27/25

U//FOUO

Today's Topics

Incident Reporting Statistics
Recent Events
Q1 Cyber Intelligence Products

July 1,2022:
VA Code§2.2-5514

Every public body shall report all (i) known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data protected by federal or state laws and (ii) other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies. Such reports shall be made to the Virginia Fusion Intelligence Center within 24 hours from when the incident was discovered. The Virginia Fusion Intelligence Center shall share such reports with the Chief Information Officer, as described in § 2.2-2005, or his designee at the Virginia Information Technologies Agency, promptly upon receipt.

Recent Events

Oracle Cloud Breach

Fog Ransomware

Trump Winery DDoS Attacks

Questions?

VIRGINIA IT AGENCY

Server Vulnerability Compliant Patching Schedule

SEC530 30-Day ‘High’ and ‘Critical’ Compliance

John C Del Grosso
VITA SSDC Service Owner

Agenda

- Server Patching Process
- Server Patching Window assignments
- SEC530 Compliance Requirements
- Prior Patch Schedule
- New Patch Schedule

SEC520 Risk Management Requirement & SEC530 Information Security Standard Requirement

SEC520

4.7.2 Requirements

a. Fix vulnerabilities within 30 days of a fix becoming available that are either:
   1. Rated as critical or high (CVSS V3 Score of 7-10) according to the National Vulnerability Database (VND)
   2. Otherwise identified by CSRM

b. Remediate all other vulnerabilities within 90 days of a fix becoming available.

c. Acquire an approved security exception for the vulnerability should it not be remediated within the timeframes identified. Mitigating controls will be expected as part of this process.

SEC530

SI-2 FLAW REMEDIATION

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within at least 30 days or within a timeframe approved by Commonwealth Security and Risk Management of the release of the updates; and

d. Incorporate flaw remediation into the organizational configuration management process.

Patching Processes

Patching Processes

- Patching is a continual activity which is done weekly, even to some degree, daily, depending on application ownership and VITA/Supplier responsibility.
- Most patching by Unisys is automated using the Ivanti Management System with no manual intervention. The Ivanti system reports the patch results, any issues or failures are investigated by the SSDC patch team and rectified either manually or a re-patch from Ivanti is completed until successful.
- Manual patching is accomplished for Oracle-based Operating Systems and Applications or other situations where servers did not ‘take’ the patch from Ivanti.
- Suppliers have support responsibility for applications, as listed in the ESSP (Enterprise Software Security Patching List.

Patching Window Assignments

- Unisys schedules “Patch Windows” initially when servers are placed into production
  - A specific patching window can be requested when a server is requested (Service Catalog) or
  - Patching window can be assigned/modified via Service Request (indicate servername and preferred patch cycle)
  - Push & Stage: Agency can request that patches are staged (pushed) on the server but not initiated automatically. The Agency can either reboot the server themselves to start and complete the patching –or- request that Unisys initiate the reboot via Service Request
  - Push & Reboot: Server will be rebooted when patches are applied, as necessary,
- Patch cycles are based on Microsoft Patch Tuesday, when all Microsoft, Adobe and other patches are released.
  - Linux/RHEL patches are released through the month – generally every one or two weeks based on patch type
  - In most months, patching occurs in the middle or second half of the month as Patch Tuesday occurs between the 8th and 14th, nearly halfway into the month.

VITA/Unisys Patch Window Details (Current State)

Patch Window (in CMBD)	Server Count	Day and Time of Patch Window	Comments
Window A: Pilot Group	192	1st Sunday after MS Patch Tuesday. 3AM to 9AM. Success and operational impact of patch(es) assessed over the week.	Prod, Test, and Dev servers. A one-week observation and verification before the next Patch Window.
Window B: Dev & Test	846	2nd Sunday after MS Patch Tuesday. 3AM to 9AM	Test and Dev are done first, then Prod. Provides for final check before releasing to entire environment.
Window C: Storage & Backup	15	2nd Tuesday after MS Patch Tuesday. 10AM to 3PM	Nearly all of these are Unisys production Storage and Backup servers that are done during the day (backups happen at night).
Window D: Dev & Test	65	2nd Wednesday after MS Patch Tuesday. 7PM to Midnight	Nearly all Prod belong to Agencies.
Window E: Production Servers	1871	3rd Sunday after MS Patch Tuesday. 3AM to 1PM	This is the full patching for 50% of the population, three weeks after all patches have been tested, verified considered safe for release.
Window X: Storage and Back-up Production	29	3rd Tuesday after MS Patch Tuesday. 10AM to 3PM	This date is scheduled for AIX servers and Unisys servers. Reserved as a catch-up from Windows B, C, and D.
Window F: Production	68	3rd Wednesday after MS Patch Tuesday. 7PM to Midnight	Also reserved as a catch-up from Windows B, C, and D
No Patch Window indicated	527	These are done throughout the month independent of the MS Patch Tuesday schedule.	Generally, Agencies/Suppliers who opt to self-patch or to Stage and self-restart or devices that must be manually patched (e.g. Oracle).

Patch Calendar – Current State (Example: March)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
25	26 Patch “X”	27 Patch “F”	28	29	30	1
2	3	4	5	6	7	8
9	10 Microsoft Patch Tuesday	11	12	13	14	15 Patch “A”
16	17	18	19	20	21	22 Patch “B”
23	24 Patch “C”	25 Patch “D”	26	27	28	29 Patch “E”
30	31 Patch “X”	1 Patch “F”	2 April	3 April	4 April	5 April

Future State of Patching

Revised patch schedule – starts April 2025

Patching schedules will be as follows:

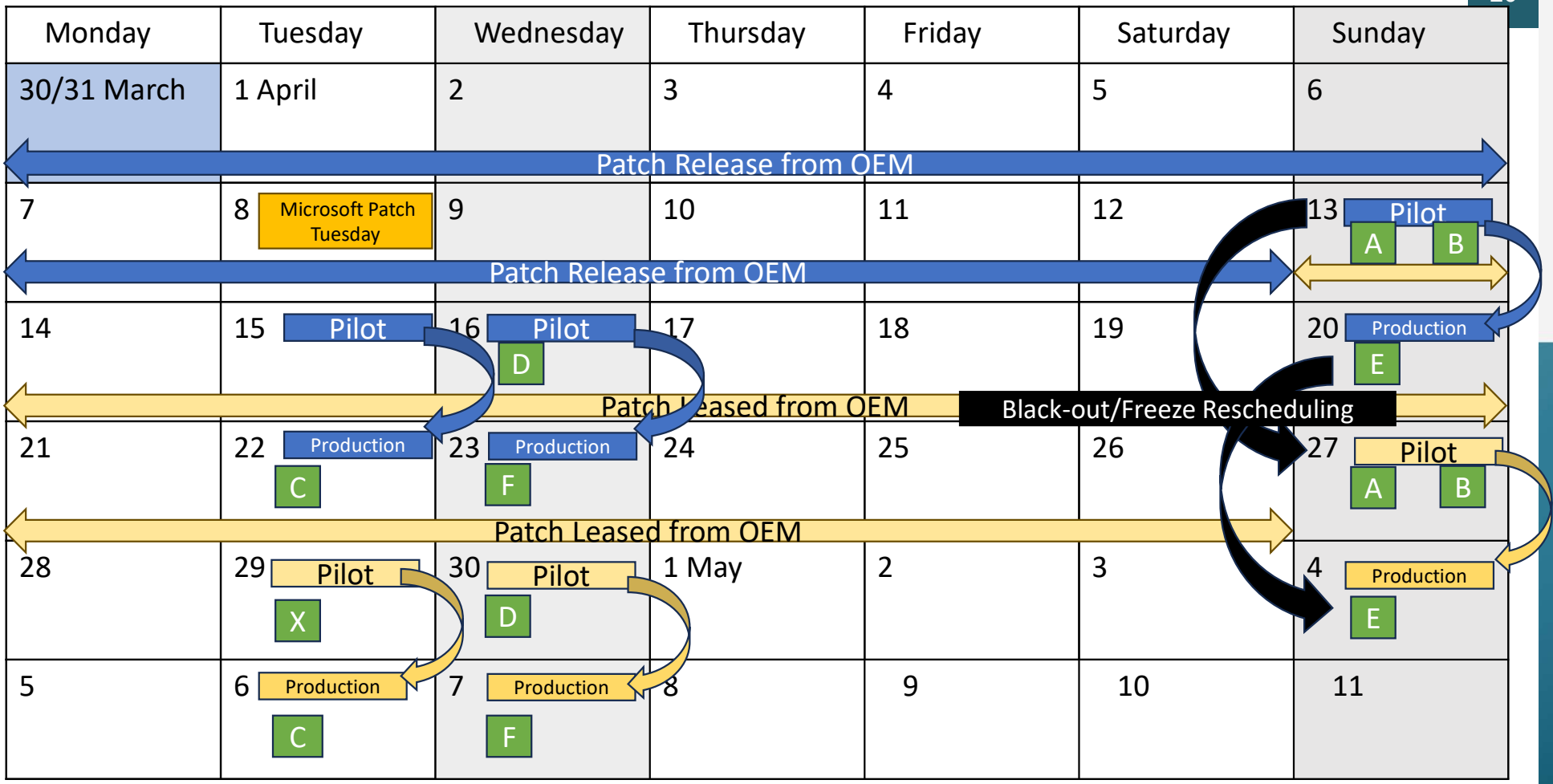
	Sundays	Tuesdays	Wednesdays
Pilot patching	3:00 am – 9:00 am	10:00 am – 3:00 pm	7:00pm – Midnight
Production patching	3:00 am – 1:00 pm	10:00 am – 3:00 pm	7:00pm - Midnight

- Days A and B will be combined into the Sunday pilot window
- Day D will be moved to the Wednesday pilot window
- Day E will be Production Sunday window
- Day F will be Production Wednesday
- Days C and X will remain at their current times

Patch schedule beginning in April

Patch released between	Pilot windows	Production windows
March 30 – April 12	Sunday, April 13	Sunday, April 20
	Tuesday, April 15	Tuesday, April 22
	Wednesday, April 16	Wednesday, April 23
April 13- April 26	Sunday, April 27	Sunday, May 4
	Tuesday, April 29	Tuesday, May 6
	Wednesday, April 30	Wednesday, May 7
April 27 – May 17	Sunday, May 18	Sunday, May 25
	Tuesday, May 20	Tuesday, May 27
	Wednesday, May 21	Wednesday, May 28

Patch Calendar – Future State (Start: April 2025)



Primary Differences from Past to Future Patching Cycles

- Monthly Patching Cycles
  - Past: Patch Cycles planning over a month (30-day period)
  - Future: Patch Cycles planned over a 2-week period, with two patch cycles per month
- Reduction of time duration between Pilot (Dev/Test) and Production
  - Past: a two-week patch checkout and test cycle before applying to Production
  - Future: a one-week patch checkout and test cycle before applying to Production
- Blackout / Change Freeze re-scheduling
  - Past: In general, if the affected patch window fell on a freeze date, the patch would be pushed to the next month
  - Future: Servers affected by freeze are pushed to next patch cycle within the same month or the next months first cycle
- Security Exceptions for patch outside the 30-day window
  - Past: Generally, with a 60 or 90-day requirement, the patch was applied within the time requirement, negated need for Exception
  - Future: Agencies that push or delay patching beyond 30-day cycle must submit a Security Exception for the specific servers

Common Questions with Answers

How can agencies adjust the window their servers are patched in?

Agencies can view their server patch window through the **Pilot & patching** tab of the AITR dashboard. Submit a general service request to adjust a server patching window. Indicate the server, the current patch window and the desired patch window.

How can agencies ensure servers are only patched during a specific time window, such as Sunday's patch day?

Specified with Ivanti and noted in the CMDB – patching outside of the specified window should not be happening unless the agency specifically requests for a patch window adjustment.

When does my agency require a security exception for vulnerability patching?

If the high or critical patch cannot be applied within the 30-day requirement.

In a patch change freeze or blackout, how does my server get re-scheduled?

The server(s) will be pushed to the next patch cycle within the same month or the first patch cycle in the following month (ensuring 30-day compliance)

Questions?
Thank you!

VIRGINIA
IT AGENCY

Cyber Vault Service (CVS)

John Del Grosso
Service Owner

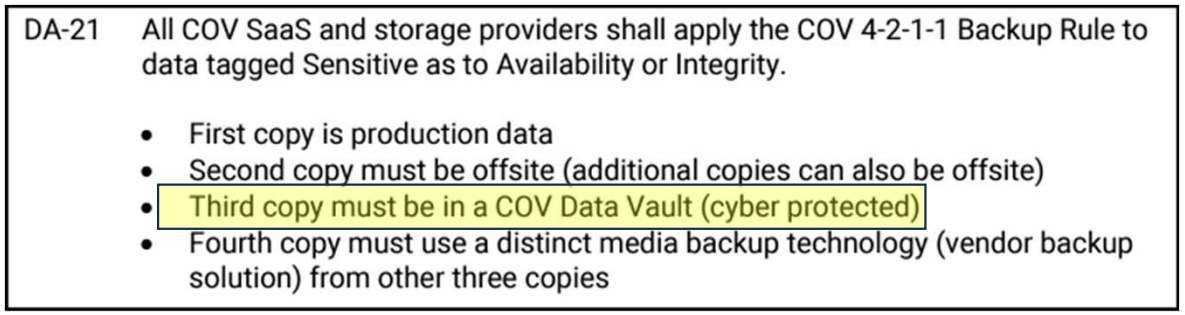
Agenda

- Compliance to Commonwealth of Virginia (COV) standards
- Overview
  - Use of a vault
  - The air gap
  - Threat detection and notification
- Availability

Compliance to standards

Enterprise architecture (EA) 225

- All data assets tagged with “sensitive as to availability or integrity” in the system of record shall be protected by a COV data vault per EA 225 guideline DA-38
- Cyber vault service (CVS) qualifies as a cyber resilient backup service per EA 225 policy guidelines DA-43 through DA-53
- CVS is the third leg of the COV 4-2-1-1 backup rule for sensitive data



DA-21 All COV SaaS and storage providers shall apply the COV 4-2-1-1 Backup Rule to data tagged Sensitive as to Availability or Integrity.

- First copy is production data
- Second copy must be offsite (additional copies can also be offsite)
- Third copy must be in a COV Data Vault (cyber protected)
- Fourth copy must use a distinct media backup technology (vendor backup solution) from other three copies

SEC530

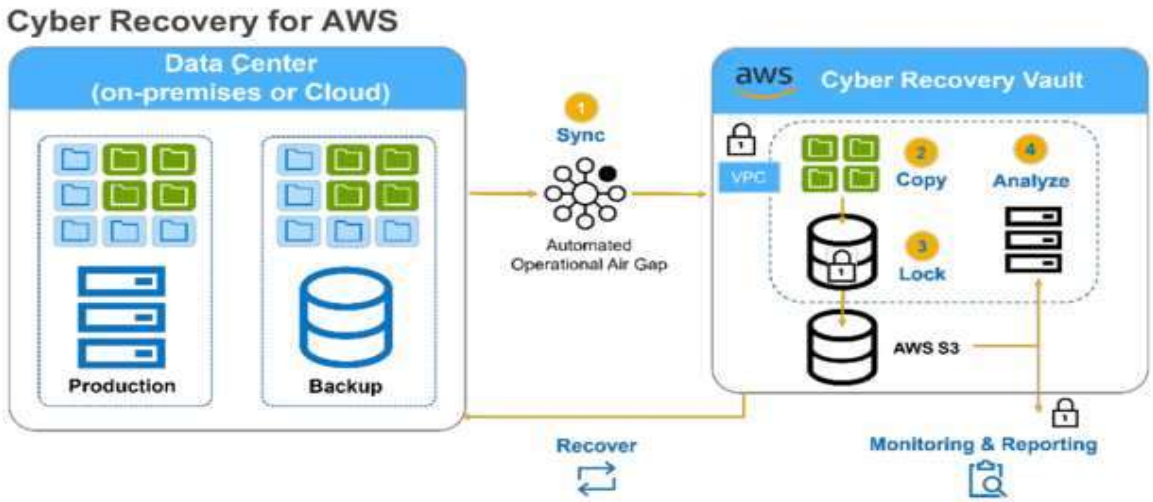
- CVS can be used for contingency planning and adheres to SEC530 CP-2

Benefits and use cases

Cyber vault service (CVS) will allow agencies to maintain mission-critical business data and technology configurations in a secure, air gapped vault that can be used for data recovery from the last non-infected dataset saved

- Enable long-term archiving of sensitive information for business continuity
- Isolates essential systems from potential cyber threats
- Safeguard citizen data, including personal identification details
- Data recovery from ransomware and cyber attack(s)

How it works



Air gap: The air gap is a logical separation between the QTS data center and Amazon Web Services (AWS) to ensure their isolation from each other where ports are de-activated to prevent unauthorized access.

Vaulting cadence: Data sets are retained up to 14 days in CVS and can be refreshed by the agency after the daily backup. The vaulting cadence is determined by the agency during implementation.

Notification: Subscribing agencies will be notified for various syslog (system logging) activity within the vault via email. Logs are stored by security information and event management (SEIM) in Splunk.

Questions about vaulting

Question	Answer
Does the vault support database backups? If so, does it back up just the data or the entire server?	The cyber recovery vault captures database backups as file system dumps, which are then included in the nightly full server backup. This ensures that the entire server is backed up, not just the database.
What level of access does the agency have to the vault? Can they retrieve their data?	Agencies do not have direct access to the vault, as it serves as a secure, immutable backup environment. However, reports can be generated to view the vaulted data and servers.
Can the vault be used for server recovery?	No, the cyber recovery vault is not designed for direct server recovery. Instead, recovery must be performed using Dell's Avamar services.
Is the data stored in the vault a full or partial backup?	The vault retains full backups, incorporating all prior incremental backups from nightly snapshots.

Ordering and costs

Now available in the VITA service catalog

Chargeback costs:

Chargeback RU name	Chargeback rate	Unit of measure
Agency implementation	$1,232.00	One-time
Application protection	$456.00	Per protected application, one-time
Server protection	$236.00	Per protected server, one-time
Agency cyber vault support	$736.75	Per month
Application cyber vault support	$64.00	Per protected application
Server cyber vault support	$45.95	Per protected server

Note: There may be additional one-time labor costs for vaulting

Questions?

Announcements

ISOAG April 2, 2025

Two New Types of User Guides!

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

- **Hey ISOs! The Archer and Nucleus 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!** 🔐

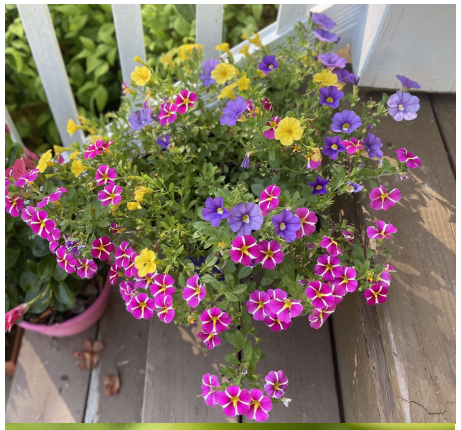
Learn how to:

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

ARCHER

Nucleus

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

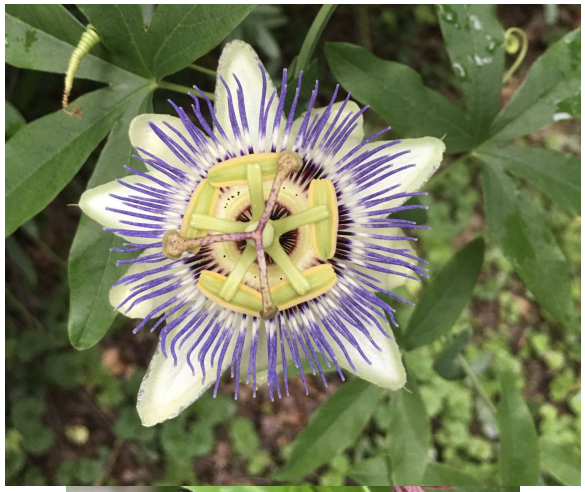


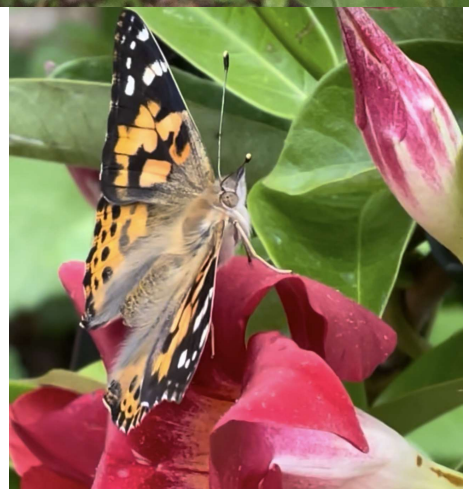
Spring has sprung, so be sure to send in your logs, right into the VITA Splunk instance!

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 April, the Top 5 Key Vulnerabilities are:

- **IBM HTTP Server 8.5.0.0<8.5.5.26/9.0.0.0<9.0.5.18 DoS (7129933)**
- **KB4025339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update**
- **Splunk Enterprise 9.0.0<9.0.9, 9.1.0<9.1.4, 9.2.0<9.2.1 (SVD-2024-0718)**
- **SSL RC4 Cipher Suites Supported (Bar Mitzvah)**
- **Jenkins LTS<2.452.4/Jenkins weekly<2.471 Multiple Vulnerabilities**

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

Service Tower SOC Report Review Sessions

The upcoming SOC review session is June 12, 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

IS Orientation

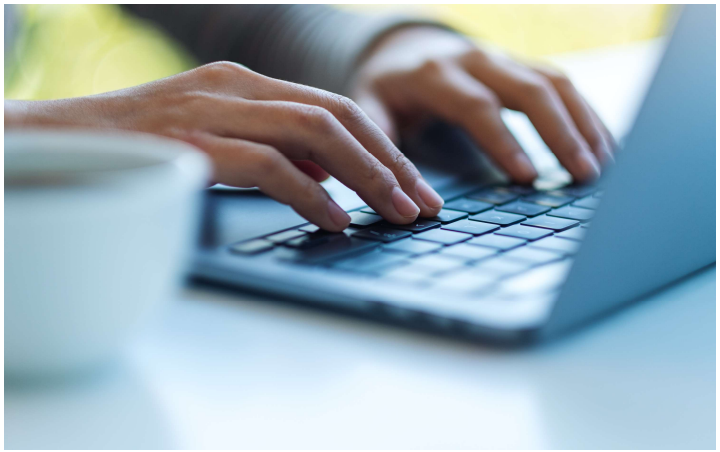
The next IS Orientation is being held on June 25, 2025

- 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!

  https://www.vita.virginia.gov/about/events-conferences/is-orientation/



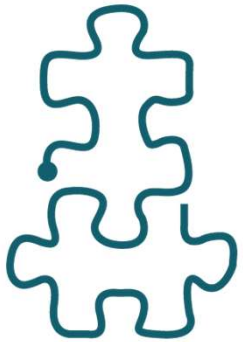
Government Cybersecurity Showcase Virginia
Elevating Virginia's Digital Defense

Public Sector Network is presenting: Government Cybersecurity Showcase Virginia

Held on Wednesday, April 9, 2025, at the **Downtown Richmond Marriott**

- The registration link is below:

  Public Sector Network » Event - Government Cybersecurity Showcase Virginia



Future-Proofing Cybersecurity:

Next-Gen Strategies

August 14, 2025

Hilton Richmond Hotel, 12042 West

Broad St., Richmond, VA 23233

Registration will open soon!

MEETING ADJOURNED

VIRGINIA
IT AGENCY