WELCOME TO THE December 4, 2024 ISOAG MEETING

VIRGINIA
IT AGENCY

Information Security Officer's Advisory Group

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Kendra Burgess/VITA
TLS Transport Layer Security v1.0/v1.1 Encryption Remediation	John Del Grosso/VITA
Introduction to Cyber Vault Services (CVS)	John Del Grosso/VITA
Nationwide Cyber Security Review (NCSR)	Amy Braden/VITA
Products & Services Toolkit	Uma Seshakrishnan/VITA
End-of-Year Governance Reminder	Erica Bland/VITA
Announcements and Upcoming Events	Kendra Burgess/VITA
Adjourn	

VIRGINIA
IT AGENCY

TLS 1.0/1.1 Remediation

F5 and Non-F5 Firewall Balancer Devices - Enterprise Project

John Del Grosso, VITA service owner, SSDC

Encryption protocols have gone end-of-life

Release	Release date	End of life
TLS 1.3	March 2018	
TLS 1.2	August 2008	
TLS 1.1	April 2006	June 30, 2018
TLS 1.0	January 1999	June 30, 2018

- Transport layer security (TLS)1.0 and TLS1.1 are completely end-of-life
- There were several extensions due to COVID and other industry-related delays
- All TLSv1.0 and v1.1 must move to TLSv1.2 or TLSv1.3

TLS remediation for F5 devices

Background:

A project is underway to migrate server instances using deprecated encryption protocols (TLSv1.0 and TLSv1.1) that operate behind the F5 firewall load balancers.

Deprecated protocols are being migrated to use TLS 1.2+ versions

A communication was sent to affected agencies on Oct. 7

Progress:

Agencies that were affected by the F5 load balancer have **successfully** either deprecated from TLSv1.0/v1.1 or submitted security exceptions for those applications that cannot yet migrate.

This project will complete by the end of December 2024

Next: Deprecating all COV infrastructure in the data centers (enterprise)

The next step: Infrastructure deprecation of TLSv1.0/v1.1

Nearly every agency has some in-motion data that is using either TLSv1.0 and/or v1.1 within the data centers in the COV and going outside the COV.

Process to identify sources:

The Unisys and multi-sourcing service integrator (MSI) teams have used Atos 'Tenable' data and other sources to identify the servers, ports and TLS versions that have been detected as using v1.0 and v1.1.

Next steps:

The next step is for the team to determine the best and least intrusive method to limit all server ports to only using TLSv1.2. Those will incorporate direct means (specific to a server) or global means.

To ensure operations are not negatively impacted, no changes will be made globally without all agencies being notified through VITA communications about the impact of those updates.

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

1. Determine if the agency-owned application(s) on the servers are limited to use specific encryption protocols or can be either upgraded to use v1.2 exclusively or ‘locked’ to only use v1.2.
2. Check the operating system (OS) settings for security settings. If the OS settings on a server have been changed to allow ‘any’ TLSv1.x, to change those switches back to TLSv1.2+ only (or a similar switch).
3. If agency applications cannot be upgraded right away to use only TLS1.2+, then submit a security exception(s) in Archer to identify the server name and agency application, along with the remediation actions required.

More to come in 2025

Questions?

VIRGINIA
IT AGENCY

Cyber Vault Service (CVS)
New VITA Service

Server, storage, and data center (SSDC)

John Del Grosso, VITA service owner, SSDC

Agenda

- Overview
- How CVS works
- Compliance to standards

Overview

Cyber vault service (CVS) provides immutable data and application vault capabilities for critical application and sensitive Commonwealth data as a defense against Cyber threats including ransomware.

Anticipated release in quarter one (Q1) of 2025

How CVS works

- **Cyber threat detection:** Artificial intelligence (AI) is built in for automated early detection of cyber threats
- **Notification:** If a threat is detected – sends a notification to SSDC
- **Versioning:** CVS vaulted versions allow owner to recover from the last non-infected version of the data.

Compliance to standards

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 enterprise architecture (EA) 225 guideline DA-38.
- CVS qualifies as a cyber resilient backup service per EA 225 policy guidelines DA-43 through DA-53.

SEC530

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

- **Questions?**

VIRGINIA
IT AGENCY

NSCR MATURITY ASSESSMENT

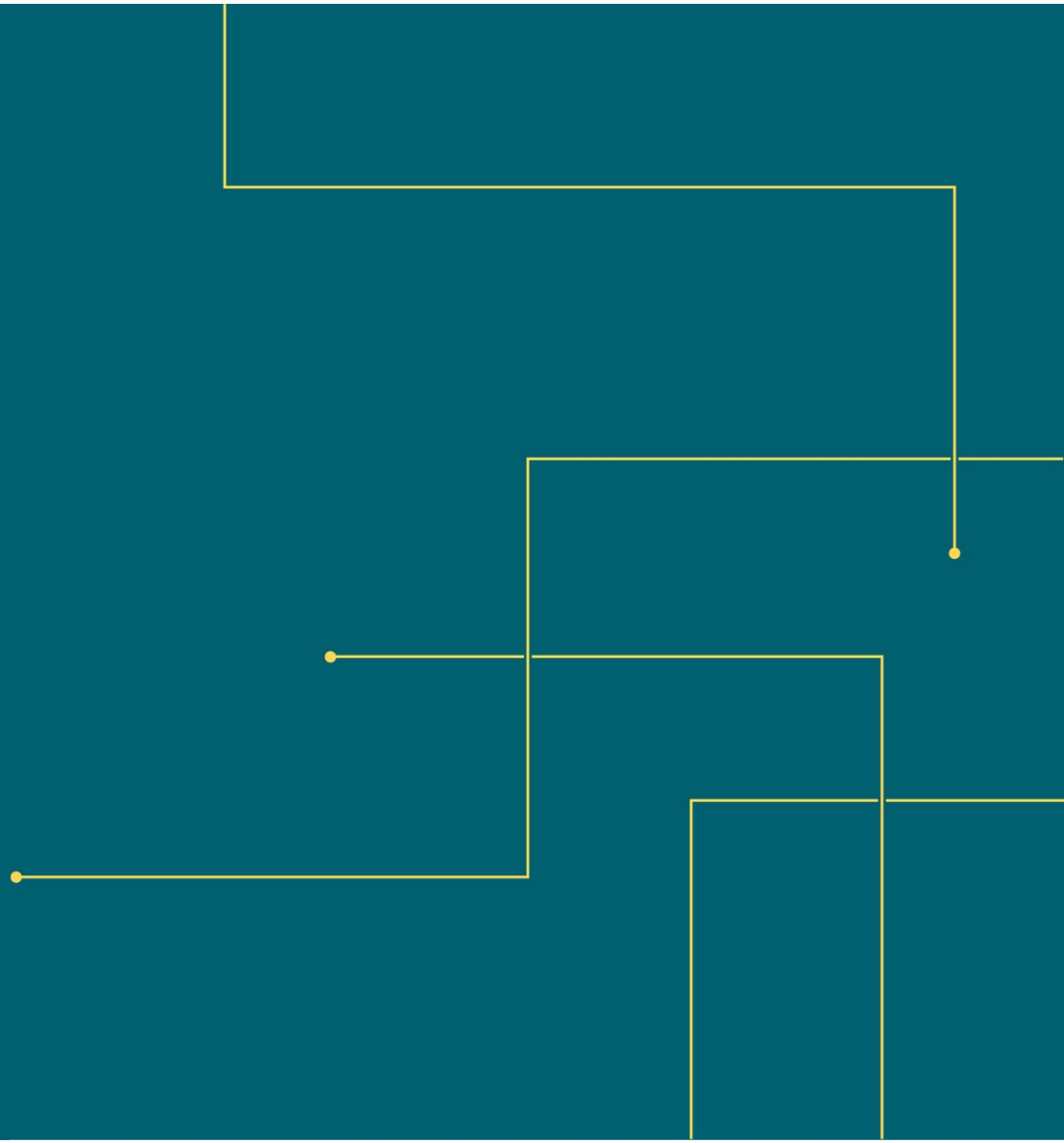
AMY BRADEN

DIRECTOR, IT SECURITY GOVERNANCE & COMPLIANCE

KEY NOTES

- Annual NCSR completion requirements are in IT Risk Management Standard (SEC520, Section 3) – Risk Management Methodology.
- Completion date January 31, 2025 for CY2024 annual reporting period. The assessment is lengthy, plan accordingly.
- CSRM completed an access review to ensure all agency ISOs currently listed in Archer have access in 11/2024.
- CSRM may include NCSR completion status as data point in CY2025 grades.
- Contact Matthew.Steinbach@VITA.Virginia.gov or CommonwealthSecurity@VITA.Virginia.gov with any questions regarding the assessment or questions with access to LogicManager.

QUESTIONS?



VIRGINIA
IT AGENCY

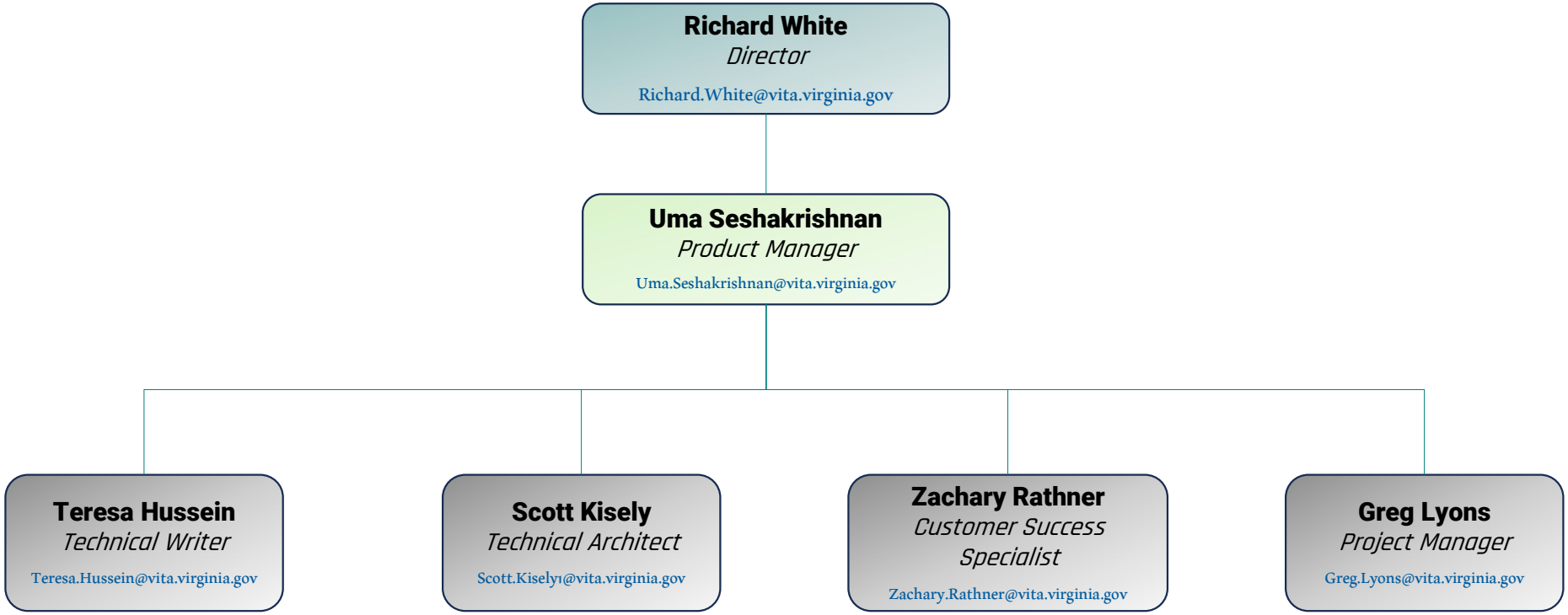
Introducing the Product Management Team

Uma Seshakrishnan
Manager, Security Services and Products

Our Mission

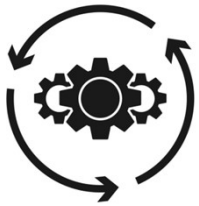
Streamline processes for onboarding, managing, and offboarding security products and services to align with the agency's vision and optimize customer satisfaction.

Meet the Team

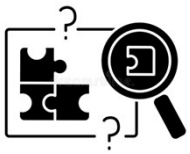


Team Objectives

Milestones (So Far)



Outline the current product onboarding process

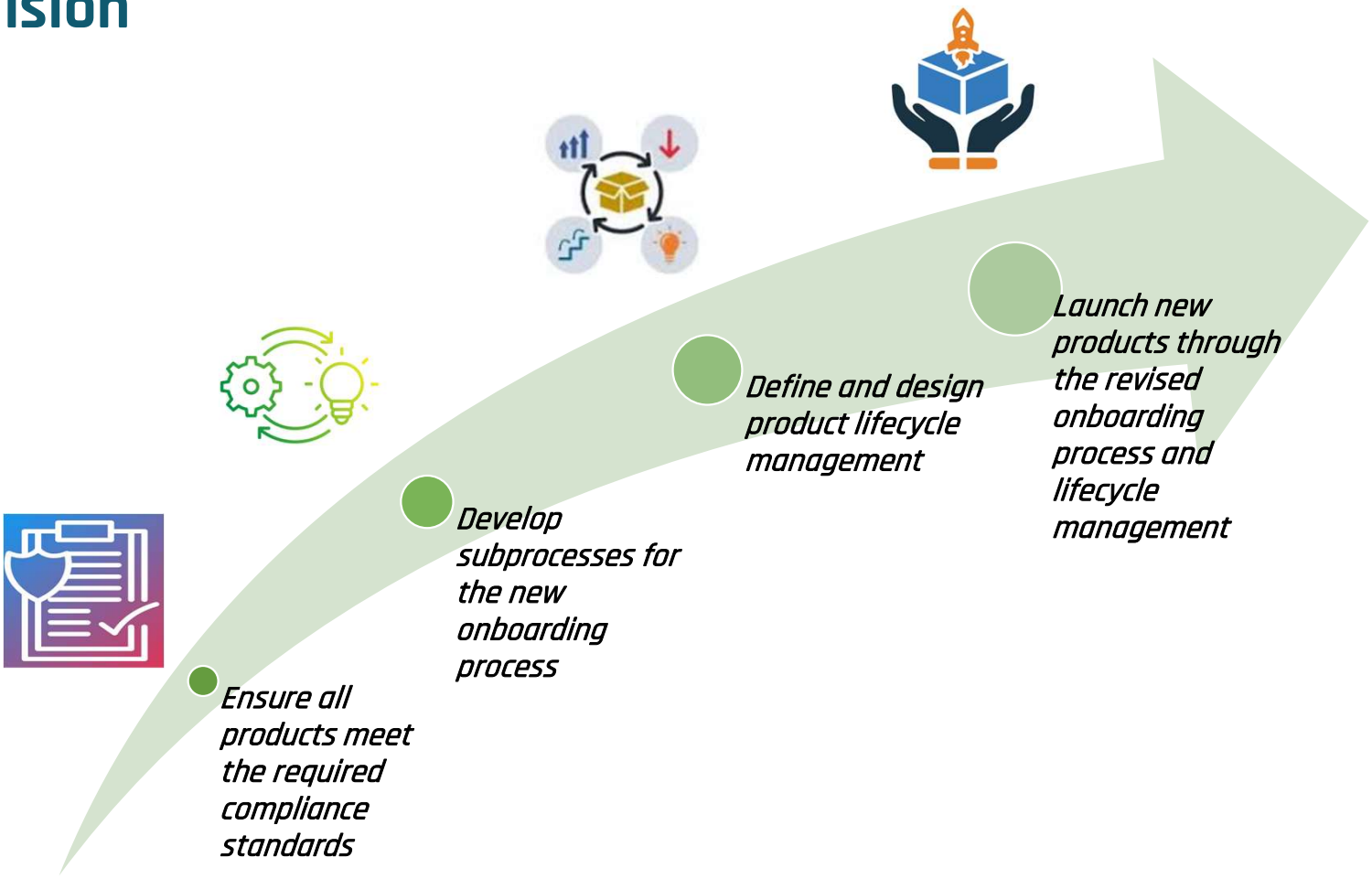


Assess gaps in relation to industry standards

Develop a new product onboarding process informed by gap analysis

Identify required product documents and design their templates

2025 Vision


Launch new products through the revised onboarding process and lifecycle management
Define and design product lifecycle management
Develop subprocesses for the new onboarding process
Ensure all products meet the required compliance standards

Conclusion

We will proactively identify customer needs and recommend suitable products.

By streamlining the onboarding process, you will receive clear user guides and informative training videos.

We will provide comprehensive support for the product throughout its lifecycle.

Questions?

Richard White
richard.white@vita.virginia.gov

Uma Seshakrishnan
uma.seshakrishnan@vita.virginia.gov

VIRGINIA
IT AGENCY

End of Year Governance Reminders

Erica Bland
Manager, IT Security Governance and Compliance

GOVERNANCE END-OF-YEAR REMINDERS

- Deliverables for calendar year 2024 will be accepted until January 31, 2025. Please submit them to your CSRM analyst or commonwealthsecurity@vita.virginia.gov
- The metrics listed below reset at the beginning of each calendar year in Archer:
  - ✓ Current year percentage of audit finding updates received;
  - ✓ Current year percentage of risk findings updates received;
  - ✓ ISO certification status.
- Annual Security Awareness Training must be completed by December 31, 2024. The Agency ISO must certify the completion of SAT by January 31, 2025.
- Access requests for Archer should be sent to commonwealthsecurity@vita.virginia.gov and not by entering a VCCC. Requests should have approval from the agency ISO.
- If your ISO certification status is N/C, please reach out to your analyst to determine if you are due to attend IS orientation by the end of the calendar year, we have not received your notification for CPE completion, and/or you did not attend the mandatory in-person October ISOAG meeting.
- Please review your agency datapoints to ensure accuracy prior to the end of year. If you have any questions about the scorecard, contact your CSRM analyst or Commonwealth Security.

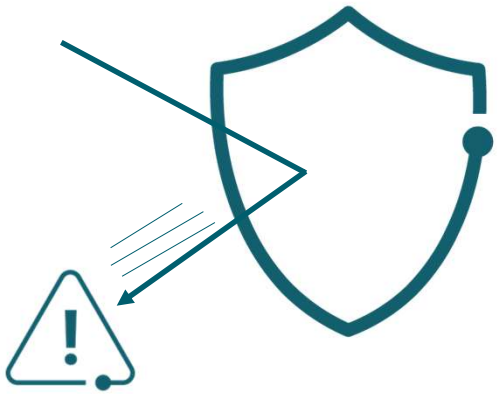
Announcements

ISOAG December 4, 2024

Top 5 Key Vulnerabilities

For the Month of December, the Top 5 Key Vulnerabilities are:

- **SSL Certificate Signed Using Weak Hashing Algorithm**
- **SNMP Default Community Name (public)**
- **SSL Medium Strength Cipher Suites Supported (SWEET32)**
- **Microsoft Windows SMBv1 Multiple Vulnerabilities**
- **KB5040430: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2024)**



- **SPLUNK Reminder**

WE WANT YOUR LOGS:

VITA is starting to work with agencies to ingest their application logs in to the VITA Splunk instance. We ask that all agencies start identifying what logs you would like to have ingested. We are always happy to schedule a call to review your options.

- **Security Awareness Training Deadline**

  - Please note that all 2024 Security Awareness Training must be completed by December 31, 2024.

  - The Annual Cybersecurity Awareness Training Verification Compliance Form must be submitted to CSRM on or before January 31, 2025. This form can be found in SEC527 and may be sent via email or completed online in Archer.

KnowBe4
Human error. Conquered.

Upcoming Events

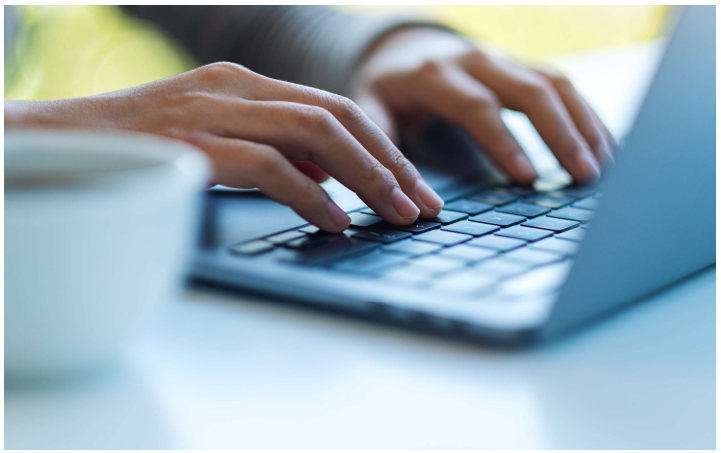
VIRGINIA
IT AGENCY
vita.virginia.gov

IS Orientation

The next IS Orientation is being held on December 11th

- It will be held virtually via Webex from 1pm-3pm
- Please register at the link below:

https://covaconf.webex.com/weblink/register/r95e66428081159841dc039e8b5d756d1



• SPLUNK Lunk and Learn

VITA will be hosting our fourth Splunk Lunch & Learn. This will be a continuation in the series. Investigating with Splunk pt.2 :

Investigating with Splunk is a modular, hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a question and answer format. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise.

• Next ISOAG Meeting

No January 2025 meeting.

We'll see you on February 5, 2025!

Enjoy the holidays!

MEETING ADJOURNED

VIRGINIA
IT AGENCY