



ISOAG Meeting March 2, 2016

Welcome to CESC!





ISOAG March 2, 2016 Agenda

I. Welcome & Opening Remarks

Mike Watson, VITA

**II. Social Media and How
Government Agents are
Targeted.**

Cyber Special Agent - Richmond FBI

**III. Legislative Update on Centralized
ISO and Centralized IT Security
Audit Services**

Ed Miller, VITA

IV. Upcoming Events

Bob Baskette/Mike Watson, VITA

V. Partnership Update

NG



Welcome and Opening Remarks

Michael Watson

March 2, 2016



Virginia Information Technologies Agency

Cyber Special Agent Richmond FBI

There will be no slides
available on the web for
this part of the presentation
due to security reasons



Legislative Update

(Centralized ISO & Security Audit Services)

Ed Miller
IT Security Governance





General Assembly Session 2016

- HB30 was introduced to support the Governor's budget related to state agency cyber security.
- The bill B.1: "(VITA) shall operate an **information technology security service center** to support the information technology security needs of agencies "
- "Support for participating agencies shall include, but not be limited to, **vulnerability scans**, information technology **security audits**, and **Information Security Officer services**."



General Assembly Session 2016

3. Agencies electing to participate **in the information technology security service center** shall enter into a **memorandum of understanding** with (VITA). Such memorandums shall outline the services to be provided by the Virginia Information Technologies Agency and the costs to provide those services.



General Assembly Session 2016

“4. **Non-participating agencies *shall*** be required by July 1 each year to ***notify*** the Chief Information Officer of the Commonwealth ***that the agency has met the requirements*** of the Commonwealth's **information security standards**. If the ***agency has not met the requirements*** of the Commonwealth's information security standards, the agency ***shall report*** to the Chief Information Officer of the Commonwealth ***the steps and procedures*** the agency is implementing in order to satisfy the requirements.”



So What Does This Mean?

If passed as proposed, and starting July 1 2016, VITA will be provided with funds and personnel to perform 3 critical IT security services:

- Vulnerability Scanning Services
- Centralized IT Security Auditing Services
- Centralized Information Security Services



So What Does This Mean?

Vulnerability Scanning Services

We are anticipating that we will hire 2 full-time personnel and purchase related software tools to conduct vulnerability scanning of ***all*** publicly facing websites and systems that are operated by state agencies.



So What Does This Mean?

Centralized IT Security Audit Services

We are anticipating that we will hire 6 to 8 FT employees to conduct IT security audits of sensitive IT systems.

We may also out-source some IT security audit work to auditing firms.

We will use a risk-based approach to prioritize and schedule these audits based on agency needs.



So What Does This Mean?

Centralized IT Security Services

We are anticipating that we will also hire 5-6 FT employees to work directly with agencies to bring agency IT security programs into compliance with SEC501. The services provided by this unit may include:

- IT Security Consulting
- Risk Assessments (identifying threats, risks, vulnerabilities)
- Business Impact Analysis
- DR Consulting
- IT Compliance & Remediation
- Policies & Procedures Development
- Review of agency projects & initiatives for IT security risk mitigation provisions
- IT Security Training & Awareness Activities



What will it cost?

- We are still working out pricing for specific services.
- Agencies may elect to use as little or as much of the centralized services as they need.
- However, agencies must either use the centralized services or adequately provide their own resources.
- These services are available to all Executive branch agencies.



Small Agency ISO Services

- 2 years ago, VITA established a Small Agency ISO Service with funding for 1 person. This service has been used to provide IT Security & ISO assistance to “small” agencies.
- The new Centralized IT Security Services, whether approved or not, does not affect the Small Agency ISO Service.
- Agencies currently being serviced by the Small Agency ISO Service will continue to be serviced as always.
- Note: the Small Agency ISO Service has never been staffed to perform IT Security Audits, so use of the Centralized IT Security Audit Services by small agencies is an extra service.

Any Questions?



Sensitive System Conflicts



making all the pieces fit



Sensitive System Conflicts

- Any system that can be noted as **HIGH** for any of the security attributes of **Confidentiality, Integrity or Availability** is a **SENSITIVE** system.



Sensitive System Conflicts

- In the last few years, you have routinely submitted to CSRM your agency's BIA to identify the business processes that your agency performs. These business processes were then associated with systems where applicable.
- In September/October 2015, as part of ED#6, you also submitted to CSRM an inventory of the different datasets that your agency stores, processes or transmits. These datasets were also associated with systems.



Sensitive System Conflicts

- We have a lot of systems that we are tracking that are not marked as SENSITIVE, but the system is associated with a Business Process or a Dataset that is SENSITIVE.



Sensitive System Conflicts from BIAs

- Any system that performs, supports or is otherwise a resource for a **business process** that is also noted as **High** for **Confidentiality, Integrity** or **Availability** must also be noted as a **SENSITIVE** system.



Sensitive System Conflicts from Datasets

- Any system that stores, processes or transmits any **dataset** that is also noted as **HIGH** for **Confidentiality**, **Integrity** or **Availability** must be noted as a **SENSITIVE** system.



Sensitive System Conflicts

- Your Homework
- Go to Archer
 - Go to the **Agency Workspace** TAB
 - Go to the **Actionable Application Information** Dashboard
 - Review the **Reports** that are in there. The 1st 3 reports will be a good start.
- We need to get these conflicts fixed. Let us know what is wrong, if anything.
- If, after reviewing the business processes and/or datasets that are in conflict, the system will be noted as SENSITIVE if that's what those items support.



Sensitive System Conflicts

Other common issues we are seeing

- Some systems are not associated with a Business Process
- Some systems are not associated with a Dataset
- Some sensitive datasets have not had a risk control questionnaire completed
- Some systems are not associated with Devices

Please take some time to clean up as much of this as you can. CSRM analysts can assist you and will be reaching out to you in the coming weeks to get this organized.



Sensitive System Conflicts

The screenshot shows a web browser window with the URL <https://itgrcs.vita.virginia.gov/foundation/Workspa>. The page title is "Enterprise Governance Risk" and the VITA logo is visible. The navigation menu includes "Threat Management", "Issue Management", "COV Incident Management", and "Agency Workspace". Below the navigation menu, there are several tabs: "Add/Change Datasets (Information)", "Add/Change Devices", "Change Applications", "Device Reports", and "Dataset Reports". The "Actionable Application Information" section is expanded, showing a dropdown menu with the text "COV: Applications Marked as Vital Business Function". Below the dropdown is a table with the following columns: Application Name, Agency Number, Agency, Description, Criticality Rating, Sensitive System, Status, and Vital Business Function.

Application Name	Agency Number	Agency	Description	Criticality Rating	Sensitive System	Status	Vital Business Function
------------------	---------------	--------	-------------	--------------------	------------------	--------	-------------------------

- Go to the AGENCY WORKSPACE tab
- Then click the dropdown for the ACTIONABLE APPLICATION INFORMATION dashboard.



Sensitive System Conflicts

https://itgrcs.vita.virginia.gov/foundation/Worksp... Commonwealth Security a... x

File Edit View Favorites Tools Help

Symantec Enterprise Vault... Web Slice Gallery VITA WELCOME TO EMC Commonwealth Enterpris... C

Virginia Information Technologies Agency

Enterprise Governance Risk and Compliance

Threat Management Issue Management COV Incident Management **Agency Workspace** CSRM Analysis

Add/Change Datasets (Information) | Add/Change Devices | Change Applications | Device Reports | Dataset Reports

- COV: Application Appears to be SENSITIVE
- COV: Applications WITHOUT a DATASET
- COV: Applications Not Associated With Business Processes
- COV: Critical Systems that are not Sensitive
- COV: Applications without DEVICES Associated
- COV: Critical Systems NOT on Audit Plans
- COV: Sensitive Systems Missing a Agency IT Risk Assessment
- COV: Sensitive Systems Missing a Security Audit
- COV: Sensitive Systems That Are Not On an Audit Plan
- COV: Applications Marked as Vital Business Function
- COV: Applications Marked as Vital Business Function

Review the reports on the “Actionable Application Information” dashboard.



Any Questions?





Virginia Information Technologies Agency

Upcoming Events





OSIG Training

Incident/Breach Response Management Program Training

- **Instructor: David Cole – SysAudits.com**
- **Date:** March 22, 2016 and March 23, 2016
- **Location:** The Commonwealth Enterprise Solutions Center (CESC)
- **Pricing Terms:** \$350.00
- **CPE: 16 hours**
- **General Overview:**
- This course is intended to provide a general overview of assessing an organization's incident handling and event management program (IHP) as well as information on how to audit the secure configuration of operating systems and network devices. Attendees will gain an understanding of the NIST Incident Handling framework as well as other best practices for assessing an IHP.



OSIG Training

Introduction to Digital Forensics for State Government

- **Instructors: David Raymond and Randy Marchany**
- **Date: April 12, 2016**
- **Location: CESC**
- **Pricing Terms: \$40.00**
- **CPE: 8 hours**
- **Course Overview:**

An understanding of digital forensics is essential to the protection of your agency/university in the event of a security breach that involves the loss of confidential information.

This course is designed to deliver a comprehensive introduction to digital forensics and help you develop an effective forensic readiness plan for your organization.



IS Orientation

When: Thursday, March 30th, 2016

Time: 10:00 am to 12:00 pm

Where: CESC , Room 1221

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



IS Security Conference 2016

“Securing the Commonwealth”

Save the Date: April 7 & 8, 2016

Location: Crowne Plaza Hotel (Downtown)

Cost: \$125 per person

Registration website:

<http://www.vita.virginia.gov/itac/default.aspx?id=6442472001>

***Space is limited, please register early**

Note: There will not be a waiting list

Conference Keynote Speaker



Eric O'Neil

Thursday, April 7, 2016

Eric M. O'Neill, attorney, security consultant professional public speaker. In 2001, Eric helped capture the most notorious spy in United States history: Robert Hanssen, a 25 year veteran of the FBI.

Conference Keynote Speaker



Teresa H. Carlson

Friday, April 8, 2016

Vice President Worldwide Public Sector, Amazon Web Services. Teresa is responsible for strategy, operations, sales and business development for Amazon's cloud computing business for governments, educational institutions and nonprofits globally.



Conference Questions



Contact: CommonwealthSecurity@Vita.Virginia.Gov

IS Conference Co-Chairs: Rosario Igharas (VA529)

Marice Stout (Supreme Court of Va)



Future ISOAG

April 6, 2016 1:00 - 4:00 pm @ CESC

Speaker: TBA

ISOAG meets the 1st Wednesday of each month in 2015

ADJOURN

THANK YOU FOR ATTENDING

