



Virginia Information Technologies Agency

# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

November 6, 2013



# ISOAG November 2013 Agenda

- |       |   |   |
|-------|---|---|
| I.    | Welcome & Opening Remarks               | Mike Watson, VITA                       |
| II.   | Life on the Bleeding Edge of Technology | David Ihrie, CIT                        |
| III.  | COV IS Council 2014 Committees          | Bob Auton, DJJ                          |
| IV.   | COV IS Council ISO Meetings             | Andrew Hallberg, ABC                    |
| V.    | FAQ's                                   | Michael Watson, VITA                    |
| VI.   | EOL Software: Considerations & Controls | Bob Baskette, VITA                      |
| VII.  | 2013 Penetration Test                   | Bob Baskette, VITA                      |
| VIII. | Upcoming Events                         | Mike Watson, VITA                       |
| IX.   | Partnership Update                      | Bob Baskette, VITA<br>Michael Clark, NG |



# CIT, IEIA, VITA ...and BEYOND

## *Life on the Bleeding Edge of Technology*

ISOAG Meeting, November 6, 2013

David Ihrie, CTO  
**MACH37**™  
[David.Ihrie@MACH37.com](mailto:David.Ihrie@MACH37.com)  
[www.mach37.com](http://www.mach37.com)

David Ihrie, CTO/CIO/ISO  
Center for Innovative Technology  
[David.Ihrie@CIT.Org](mailto:David.Ihrie@CIT.Org)  
[www.cit.org](http://www.cit.org)

# Topics

---

- What is CIT, and Why Do You Care
- The IT Impacts of the CIT Mission
- Three Case Studies:
  - BYOD Transition
  - Financial System Cloud Migration
  - MACH37™ Cybersecurity Accelerator
- Final Thoughts/Q&A

# Mission

---



*CIT accelerates the next generation of technology and technology companies*

---

***Our objective is to be globally recognized as the innovator, builder and premier provider of services that accelerate technology company development***

---

# Background

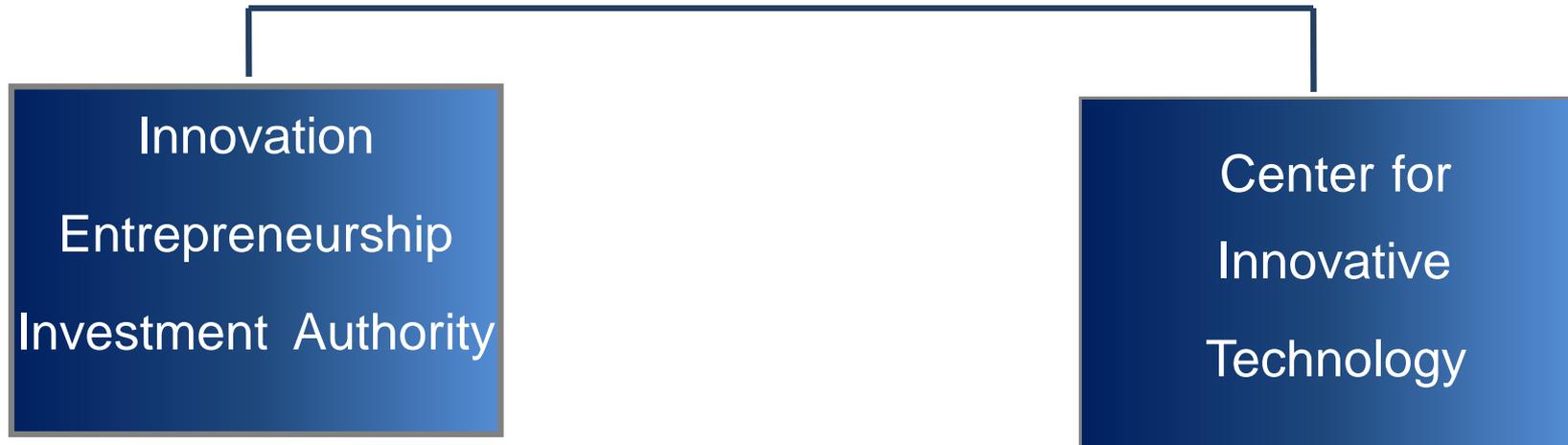
---

- Established in 1984 as the Innovative Technology Authority (ITA)
- Seven chartered objectives:
  - Attract high technology business
  - Apply technology for productivity
  - Support new product development
  - Expand university R&D
  - Expand knowledge of R&D
  - Attract R&D
  - Facilitate marketing R&D



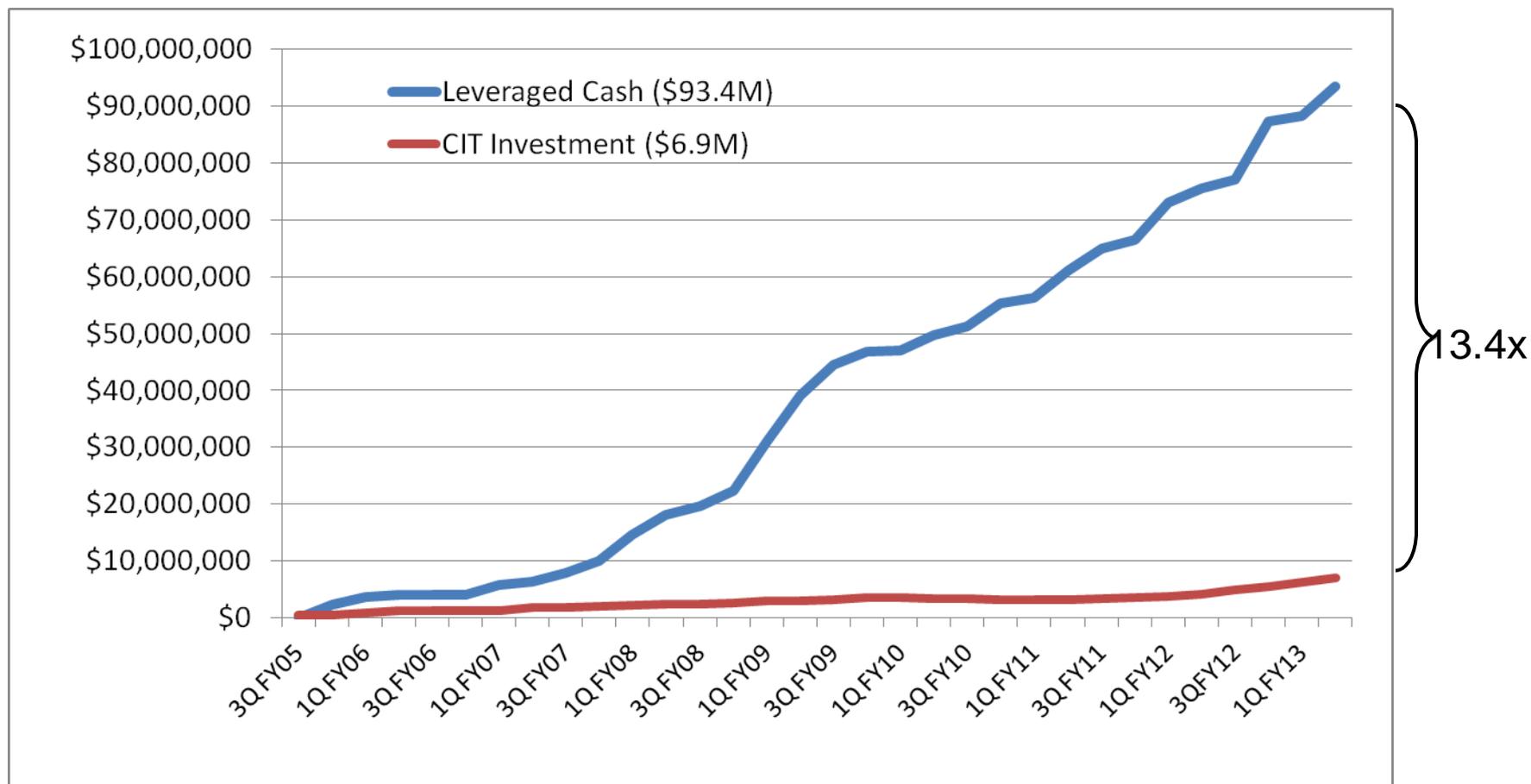
# Organizational Structure

---



- **Two separate and mission integrated organizations**
- **Organizational structure supports:**
  - **Public funding of a private company**
  - **Operational execution without normal limits imposed by statutes**

# Huge leverage for COV Investment



# Track Record (as of end of FY13)

---

81 New Companies Seeded

7 Spin-Outs from Universities and Federal Labs

13X Private : Public Funding Secured

8 Portfolio Companies Exited

4X Named “Top 100 Venture Fund”

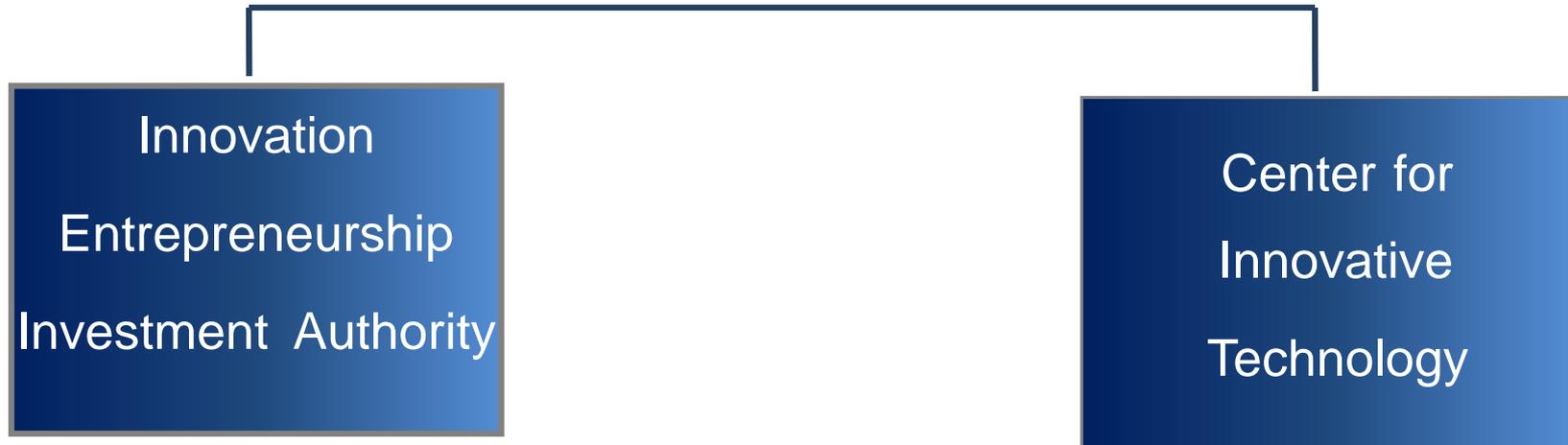
**Entrepreneur.com**

Value Creation for ...

- ✓ Entrepreneurs
- ✓ Co-Investors
- ✓ Commonwealth of Virginia

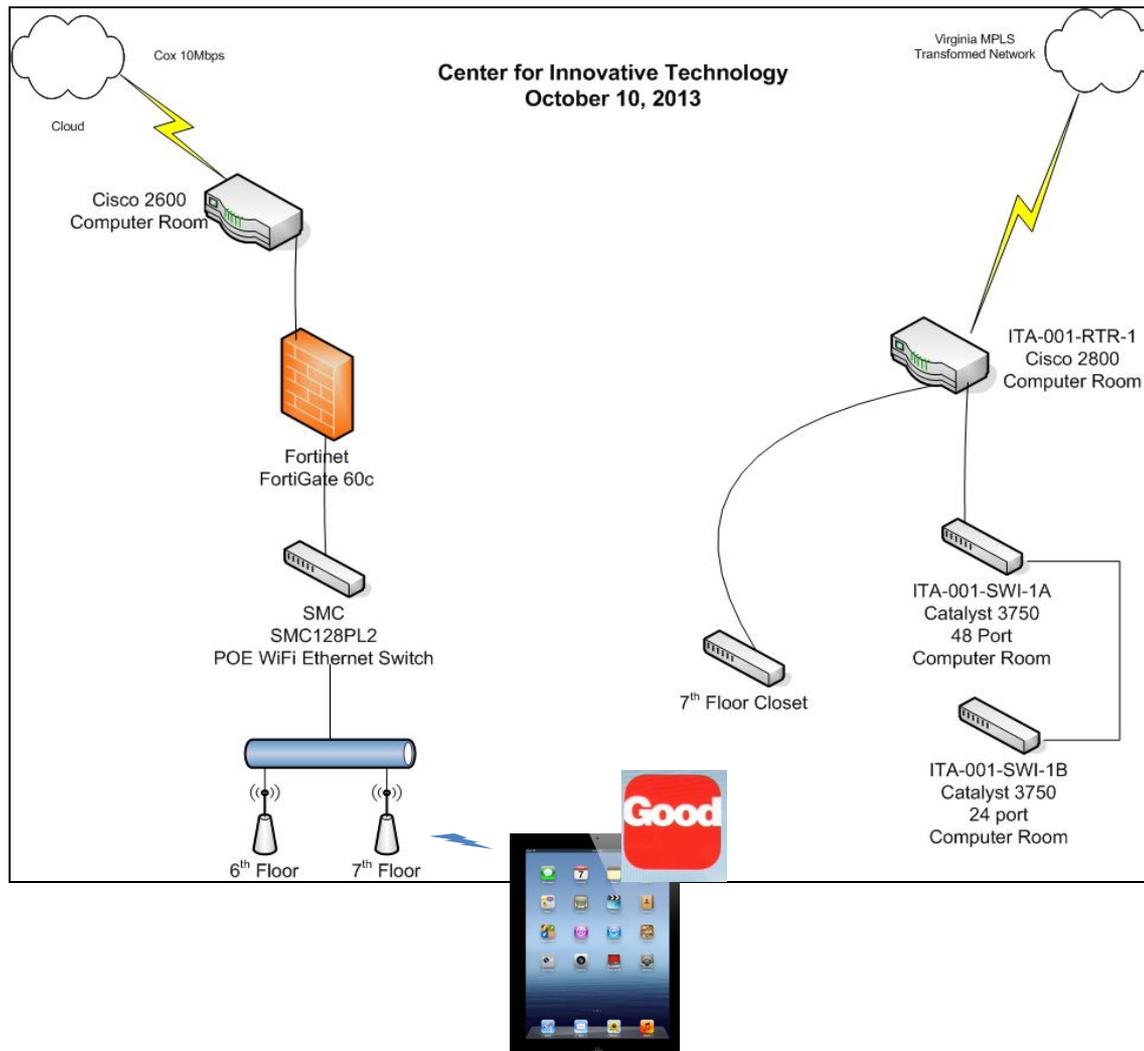
# Public-Private Partnership

---



- **VITA Provides IT Infrastructure under IEIA authority**
- **CIT has some mission elements outside scope of COV Government**
  - **Not State employees**
  - **Some Federal and private contractual arrangements**
- ➔ • **Some IT infrastructure provided independent of VITA**

# Case Study #1: BYOD



- Full scale implementation July 2012
- Every employee has personally-owned iPad and smart phone
- GOOD provides the COV security boundary on each device

## Case Study #1: BYOD Policy

- CIT decision to move ahead
- VITA “*Acceptable Use of Non-COV Mobile Device Security Policy*” used as basis to tailor custom policy
- User issue: privacy  
Admin issue: tech support
- 15 months with high user acceptance, no issues
- Now supporting VITA BYOD committee

7/16/2012

### Mobile Workforce Computing Acceptable Use Policy

**Goal:** CIT seeks to enable and encourage a maximally productive mobile computing capability for our workforce, and integrate this capability as part of our normal business operations. In doing so, we also seek to model the capabilities and policies that support this goal for the Commonwealth of Virginia (COV).

To achieve these goals, it is essential that reasonable measures are included to protect the security of CIT and COV information. Additionally, in order to minimize the number of devices employees are expected to carry, we are supporting and encouraging dual-use business and personal usage of devices. This policy seeks to address some of the inherent tensions between mobility and access, and between personal and business usage by specifying acceptable use of the devices, and outlining CIT and employee responsibilities in support of our mobile computing goals. The areas addressed fall into four categories: Usage, Security, Data Integrity, and Privacy.

**Policy Summary:** All employees shall be aware of, and shall comply with, the requirements established by this policy for mobile access.

#### Definitions:

“Mobile Access.” Mobile access means any access to CIT or COV networks or non-public data over wireless links, including Wi-Fi or commercial carriers (such as AT&T, Verizon or Sprint), where employees take specific action to initiate the access. Thus, logging into a device to check your CIT e-mail over any wireless link is considered “mobile access,” while receipt of an e-mail from CIT on a personal device using a public e-mail account is not considered “mobile access.” Note that the location where the access occurs is not relevant to this definition, so “mobile access” may occur from your normal office work space as well as from off-site locations.

“Devices” (or, “mobile devices”). The devices covered under this policy are defined to be any device used for mobile access. Generally this includes smart phones and tablet computers (such as iPads), but may also include laptops or other devices. Note that the defining feature for purposes of this policy is use of the device for information access, and is not related to the device type or ownership of the device. CIT may choose to provide financial incentives or similar support for one or more devices or software to encourage mobile access, but this policy applies to devices whether or not such financial incentives are provided.

#### Related Policies:

The CIT “*Smart Devices Mobile Policy*” establishes the requirement for “all permanent CIT employees ... to have a smart device for voice and data business communications” as a condition of employment, along with related conditions. This policy duplicates the usage requirements of the “*Smart Devices Mobile Policy*” and adds requirements for mobile devices generally.

The VITA “*Acceptable Use of Non-COV Mobile Device Security Policy*” provides specific usage requirements related to security as established by COV for mobile devices not owned by COV. Devices under the CIT policy are generally not owned by COV, and so are subject to the Non-COV Mobile Device policy, and CIT employees are required to sign the Acceptable Use form associated with that policy prior to using mobile device(s). This CIT policy seeks to be consistent with the COV policy, and the intention is to work with COV to resolve any inconsistencies. In the case of inconsistencies, the COV policy takes precedence. This CIT policy seeks to provide a more bi-lateral understanding of employee rights and responsibilities while encouraging the use and adoption of mobile computing capability.

# Case Study #1: BeYOnD BYOD

- Testing mobile security stack entrepreneurial products
- A HEAP O APPS

Category	App	Cost	Platform (Devices, OS, memory constraints)	Recommendation (positive, negative, conditional)	Usability (easy to learn, easy to use)	Best Use Case	Security (strengths or issues)	Comments	Current Power Users
Remote Meetings									
	GoTo Meeting								
	WebEx								

Remote Meetings		Document Sharing/ Collaboration	
	GoToMeeting		DropBox
	WebEx		Wuala
	Speek		Google Drive
	Google Hangout		Sharepoint 2013
	Join.Me		Feng Office
	Skype	Project Management	
	Face Time		Unanet
CRM			SmartSheet
	Nimble		Microsoft Project
	Evolved		

Small Surveys	
	Survey Monkey
	Qualtrics
	Doodle
Form Builder	
	Acrobat
	Google Forms
	ZoHo
Format Exchange	
	pdf Reader
	AbletoExtract
	SlideShark

Secure E-mail	
	GOOD
	Gmail
	[new VITA offering]
Productivity	
	QuickOffice
	Numbers/Pages
	Notability
Browsers	
	IE
	Firefox
	Chrome
	Safari

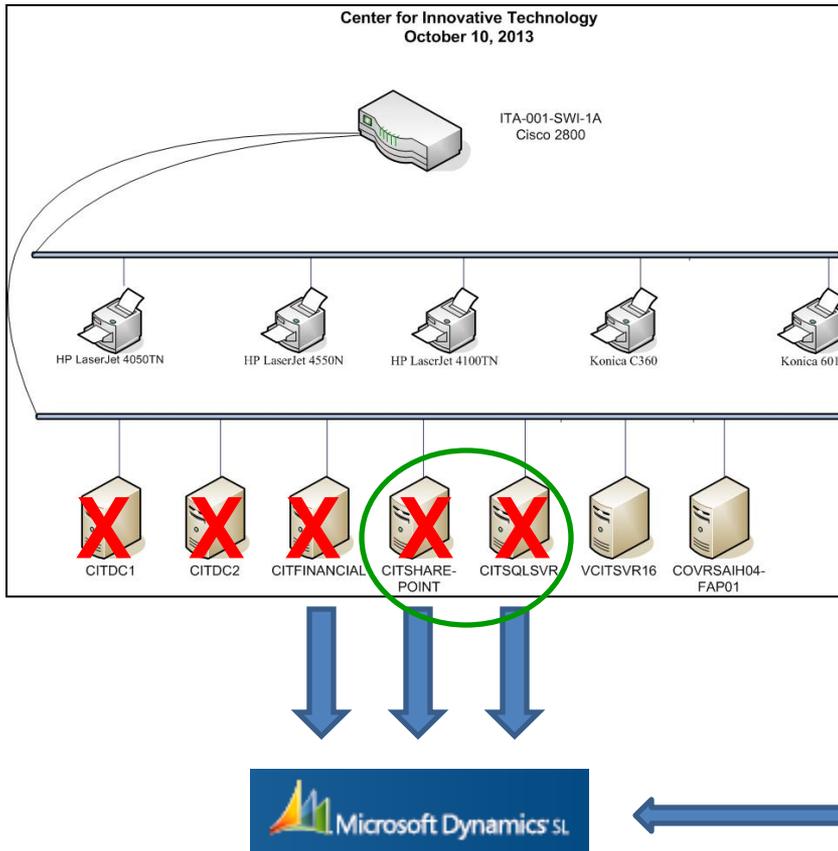
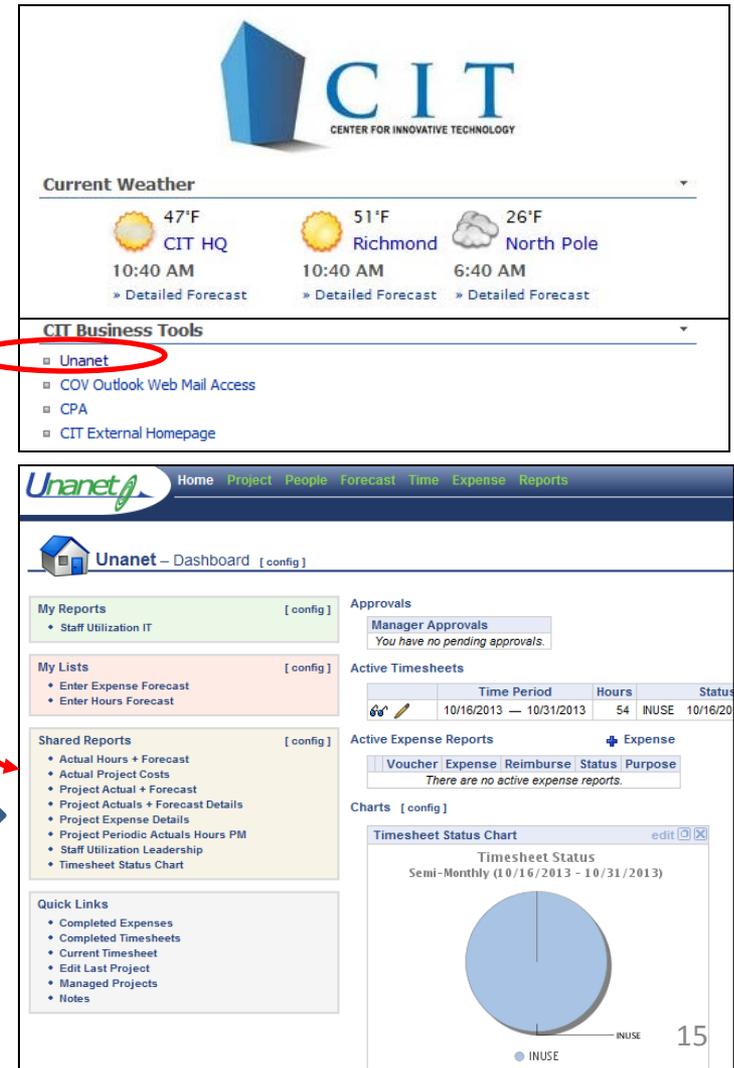
## Case Study #2: Financial System Cloud Migration

---

- Windows 2003 server-based, past end-of-life with periodic hardware failures
- Microsoft accounting system revision no longer supported
- Horrible process, universally hated: quarterly planning exercise took two intensive weeks of labor for most senior staff
- Unique CIT accounting requirements not fully satisfied by any vendor, resulting in decision paralysis

 Time for Disruption!

# Case Study #2: Financial System Cloud Migration

CIT CENTER FOR INNOVATIVE TECHNOLOGY

Current Weather

47°F CIT HQ 10:40 AM  
51°F Richmond 10:40 AM  
26°F North Pole 6:40 AM

CIT Business Tools

- Unanet
- COV Outlook Web Mail Access
- CPA
- CIT External Homepage

Unanet Home Project People Forecast Time Expense Reports

Unanet - Dashboard [config]

My Reports [config]  
• Staff Utilization IT

My Lists [config]  
• Enter Expense Forecast  
• Enter Hours Forecast

Shared Reports [config]  
• Actual Hours + Forecast  
• Actual Project Costs  
• Project Actual + Forecast  
• Project Actuals + Forecast Details  
• Project Expense Details  
• Project Periodic Actuals Hours PM  
• Staff Utilization Leadership  
• Timesheet Status Chart

Quick Links  
• Completed Expenses  
• Completed Timesheets  
• Current Timesheet  
• Edit Last Project  
• Managed Projects  
• Notes

Approvals  
Manager Approvals  
You have no pending approvals.

Active Timesheets

Time Period	Hours	Status
10/16/2013 - 10/31/2013	54	INUSE 10/16/20

Active Expense Reports  
Expense  
Voucher Expense Reimburse Status Purpose  
There are no active expense reports.

Charts [config]  
Timesheet Status Chart  
Timesheet Status  
Semi-Monthly (10/16/2013 - 10/31/2013)

INUSE 15

## Case Study #2: Financial System Cloud Migration

---

- Costs cut in half or better
- Dramatically reducing # servers in conjunction with VITA hosting of some services (Sharepoint, legacy SQL db)
- Users deliriously happy: real-time project control, unified interface for major functions; two weeks planning process now down to a day or so for most senior staff
- Some Issues:
  - remote print jobs
  - electronic invoice e-mail forwarding

# Case Study #3: MACH37™

---

April 11, 2013

## **Governor McDonnell Announces Creation of MACH37, America's First Market Centric Cyber Security Accelerator**

*Accelerator to lead the nation in new cyber technology  
company creation*



# MACH37™ Business Description

---

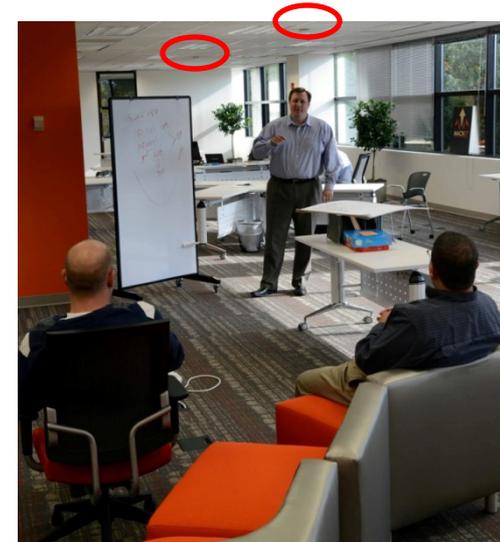
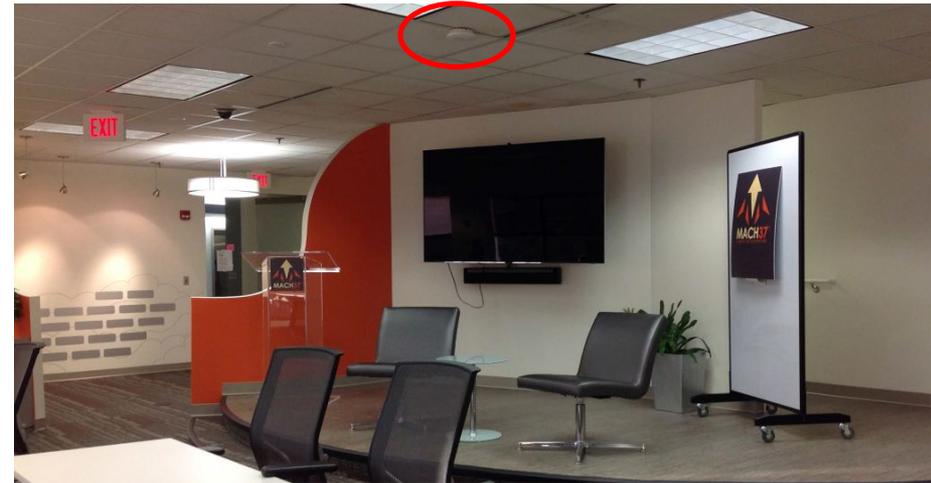
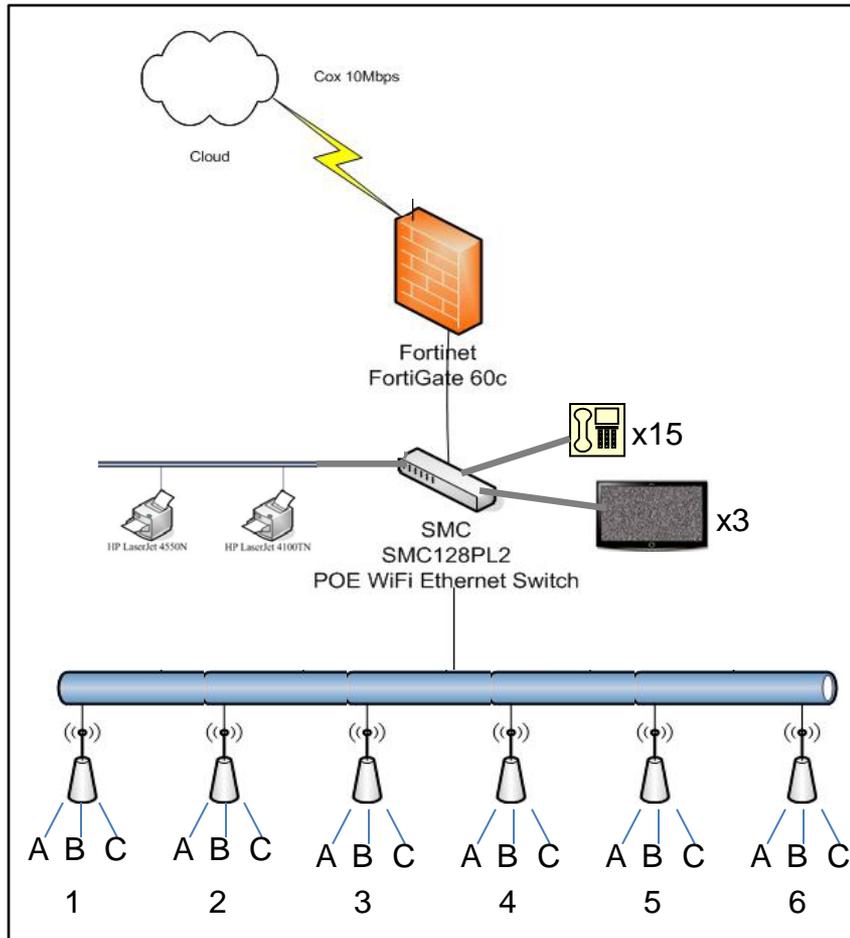
---

## Investment Fund



*Hybrid investment and development services firm*

# Case Study #3: A Grand Experiment



## Case Study #3: Security???

---

- Obvious target for external attack
- Multiple cyber companies co-existing inside firewall
- Learn by doing:
  - Alpha-test evolving products
  - Evaluate hacker/open source protection techniques
  - Teach companies to protect themselves
- Results applicable to small, funding limited orgs like:
  - Local Governments?
  - Schools?

## Futures

---

- CIT relies on VITA to provide a stable, secure baseline for our operational networks...
  - ...enabling us to continue exploring higher risk, potentially disruptive technologies of mutual interest
- 
- As VITA moves to adapt to the recent major IT changes...
  - ...we want to find new ways to leverage CIT efforts in conjunction with VITA on behalf of the Commonwealth of Virginia

Questions??

# **COV Information Security Council Potential 2014 Committees**

Bob Auton  
IS Council Member

# **COV IS Council Committees Proposed Committees for 2014 :**

1. Scope & Percentage of IT Budget
2. ISO Communication and Knowledge Sharing web site
3. IT Standards & Policies
4. Repository for IT Projects/Policies/Guidelines
5. IPv6
6. IT Legislature

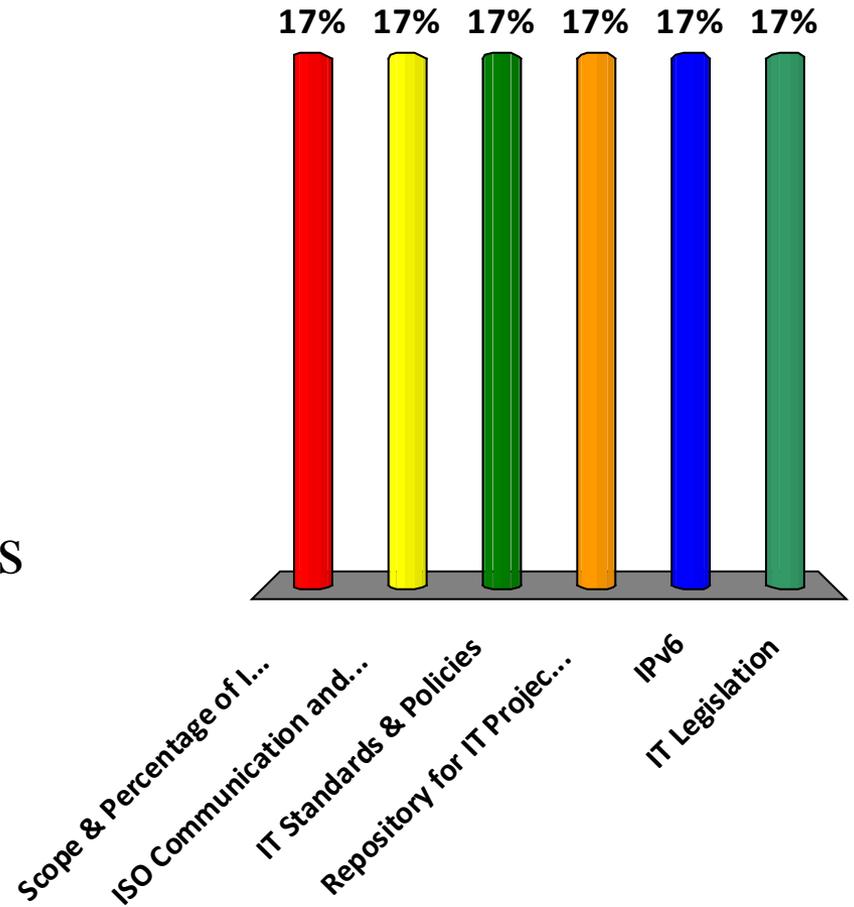
## **Committees will consist of:**

- **5 – 10 people**
- **Chairmen will be IS Council Members**
- **Will Meet Every Other Month**
- **Deliverables will be achieved in 6 – 12 months**

# Choose Top 4 Committees

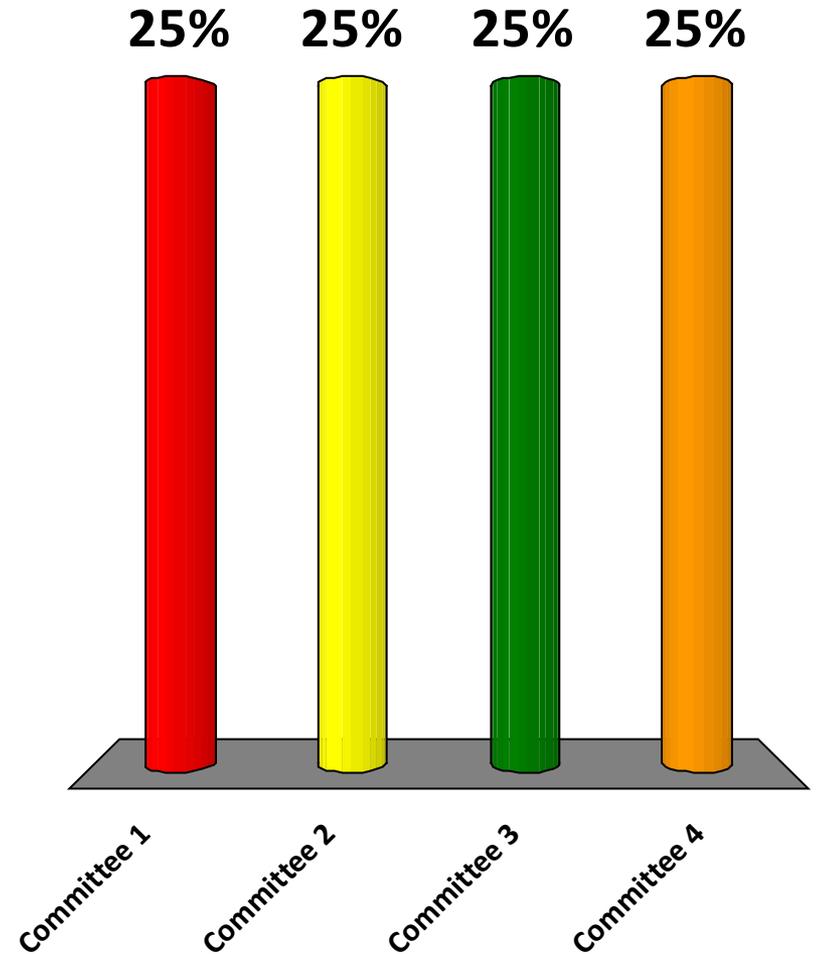
In order of Preference

1. Scope & Percentage of IT Budget
2. ISO Communication and Knowledge Sharing web site
3. IT Standards & Policies
4. Repository for IT Projects/Policies/Guidelines
5. IPv6
6. IT Legislation



# Which Committee would you like to assist with?

1. Committee 1
2. Committee 2
3. Committee 3
4. Committee 4



# **COV IS Council 2014 Committees**

## **Meeting Day**

**Date: Monday, December 2**

**Time: 3:00pm to 5:00pm**

**Location: CESC in VITA meeting rooms**

**Register: at [CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)**

*Include the proposed committee you would like  
to serve on*

# **COV IS Council Committee**

**Questions  
Or  
Comments?**

**Email:  
CommonwealthSecurity@VITA.Virginia.Gov**



*Virginia Information Technologies Agency*

# COV IS Council ISO Meetings

Andrew Hallberg  
ABC



# Frequently Asked Questions

Michael Watson  
Chief Information Security Officer



# End of Life Software: Considerations and Controls

Bob Baskette  
Senior Manager, Security Operations  
and Architect



## End of the Line

- Every COV Agency has software within its environment that is considered End-of-Life or End-of-Support by the software vendor.
- Some EOL software is required to support legacy applications while other software is simply a legacy item.



## EOL Issues

- Vulnerabilities remain long after the vendor stops providing patches.
- Source code and installation media fade away.
- Developers often retire before the systems do.



## EOL Issues

- Old software and new hardware simply do not understand each other.
- License Keys are difficult to track and therefore upgrades are difficult to achieve.



## Microsoft Server OS

OS	EMS	EOL
Server 2003	7/13/2010	7/14/2015
Server 2008	1/13/2015	1/14/2020
Server 2012	1/9/2018	1/10/2023

EMS = End of Mainline Support

EOL = End of Life/Extended Support



## Microsoft Desktop OS

OS	EMS	EOL
Windows XP	4/14/2009	4/8/2014
Windows Vista	4/10/2012	4/11/2017
Windows 7	1/13/2015	1/14/2020
Windows 8	1/9/2018	1/10/2023



# Microsoft SQL Server Software

	EMS	EOL
Server 2000	4/8/2008	4/9/2013
Server 2005	4/12/2011	4/12/2016
Server 2008	7/8/2014	7/9/2019
Server 2012	7/11/2017	7/12/2022



# Microsoft SQL Server Software

	EMS	EOL
Server 6.0	3/31/1999	Not Applicable
Server 6.5	1/1/2002	Not Applicable
Server 7.0	12/31/2005	1/11/2011



## Red Hat Support Levels

### Production 1 Phase IV:

- Includes qualified Critical and Important Security errata advisories (RHSAs) and Urgent and Selected High Priority Bug Fix errata advisories (RHBAAs)
- Other errata advisories may be delivered as appropriate.



## Red Hat Support Levels

### Production 1 Phase IV:

- Includes new or improved hardware enablement and select enhanced software functionality
- Includes Minor software releases as well as qualified errata advisories (RHSAs, RHBAs, and RHEAs).



## Red Hat Support Levels

### Production 2 PhaseV:

- Includes qualified Critical and Important Security errata advisories (RHSAs) and Urgent Priority Bug Fix errata advisories (RHBAAs)
- Hardware enablement that does not require substantial software changes may be provided at the discretion of Red Hat



## Red Hat Support Levels

### Production 2 PhaseV:

- New software functionality is not available during this phase.
- Minor releases will also include all available and qualified errata.



## Red Hat Support Levels

### Production 2 PhaseV:

- The focus for minor releases during this phase lies on resolving urgent- or high-priority bugs.
- Updated installation images will be provided only if required because of installer changes.



## Red Hat Support Levels

Production 3 Phase VI:

- Includes Critical Impact Security Advisories (RHSAs) and selected Urgent Priority Bug Fix Advisories (RHBAAs)
- Other errata advisories may be delivered as appropriate.



## Red Hat Support Levels

### Production 3 Phase VI:

- New functionality and new hardware enablement are not planned for availability.
- Minor releases with updated installation images may be made available.



## Red Hat Support Levels

### Extended Life Phase:

- Includes access to previously released content on the Red Hat Customer Portal
- Also includes critical impact security fixes and selected urgent-priority bug fixes.



# Red Hat Enterprise Linux 3

General Availability	10/23/2003
End of Production 1	7/20/2006
End of Production 2	6/30/2007
End of Production 3	10/31/2010
End of Life	1/30/2014



# Red Hat Enterprise Linux 4

General Availability	2/14/2005
End of Production 1	3/31/2009
End of Production 2	2/16/2011
End of Production 3	2/29/2012
End of Life	2/28/2015



# Red Hat Enterprise Linux 5

General Availability	3/15/2007
End of Production 1	1/8/2013
End of Production 2	1/31/2014
End of Production 3	3/31/2017
End of Life	Q1 of 2020



# Red Hat Enterprise Linux 6

General Availability	11/10/2010
End of Production 1	Q2 of 2016
End of Production 2	Q2 of 2017
End of Production 3	11/30/2020
End of Life	Q4 of 2023



# Adobe ColdFusion Software

	EMS	EOL
ColdFusion 10	5/16/2012	5/16/2019
ColdFusion 9	12/31/2014	12/31/2016
ColdFusion 8	7/31/2012	7/31/2014
ColdFusion 7	2/7/2010	2/7/2012



# Adobe Acrobat Software

	EMS	EOL
Acrobat XI Pro 11	10/15/2017	N/A
Acrobat XI Std 11	10/15/2017	N/A
Acrobat X Pro 10	11/15/2015	N/A



## Adobe Acrobat Software

	EMS	EOL
Acrobat X Std 10	11/15/2015	N/A
Acrobat X Suite 10	11/23/2015	N/A
Acrobat Pro 9.x	6/26/2013	N/A
Acrobat Std 9.x	6/26/2013	N/A



## Adobe Acrobat Software

	EMS	EOL
Acrobat 3D 8.x	11/3/2011	N/A
Acrobat Pro 8.x	11/3/2011	N/A
Acrobat Std 8.x	11/3/2011	N/A



## Adobe Acrobat Software

	EMS	EOL
Acrobat Elements 7	4/6/2010	N/A
Acrobat Pro 7	12/28/2009	N/A
Acrobat Std 7	12/28/2009	N/A



## Adobe Reader Software

	EMS	EOL
Reader X 10	11/18/2015	N/A
Reader XI 11	10/15/2017	N/A
Reader 9	6/26/2013	N/A



# Adobe Reader Software

	EMS	EOL
Reader 8	11/3/2011	N/A
Reader 7	12/28/2009	N/A



# Oracle Database Software

	EMS	EOL
Oracle 11.1.0.X	8/2012	8/2015
Oracle 10.2.0.X	7/2010	7/2013
Oracle 10.1.0.X	1/2009	1/2012
Oracle 9.2.0.X	7/2007	7/2010



## Oracle Solaris Unix

	EMS	EOL
Solaris 8	3/2009	3/2012
Solaris 9	10/2011	10/2014
Solaris 10	1/2018	1/2021
Solaris 11	11/2021	11/2024



# Oracle Solaris Linux

- Solaris 9
  - The last update for Solaris 9 was 9/05
  - Extended Support for Solaris 9 ends in October, 2014. After which it enters in Sustaining Support phase.
- Solaris 8
  - The last update for Solaris 8 was 2/04
  - Solaris 8 is in Sustaining Support phase of its life cycle.



# Oracle Sustaining Support

- May be offered for an indefinite period.
- Provides continued access to technical experts, online tools, and knowledgebase resources.
- Can provide updates, patches, fixes, security patches and security alerts created during the Oracle Premier Support period.
- Does not provide new program updates, patches, fixes, security patches, security alerts, general maintenance releases, selected functionality releases, documentation updates or upgrade tools



## Oracle Sustaining Support

- Does not provide new program updates, patches, fixes, security patches, security alerts, general maintenance releases, selected functionality releases, documentation updates, or upgrade tools.



# Oracle Unbreakable Linux

	EMS	EOL
Linux 3	10/2011	N/A
Linux 4	2/2013	N/A
Linux 5	3/2017	N/A
Linux 6	3/2021	N/A



## EOL Considerations

- Section SI-2-COV of ITRM COV SEC 501-07 requires the organization to:
  - a. Applies all software publisher security updates to the associated software products.
  - c. Prohibits the use of software products that the software publisher has designated as End-of-Life/End-of-Support (i.e. software publisher no longer provides security patches for the software product).



## EOL Controls

- EOL software requires compensating controls to protect the environment.
  - Deploy Integrity Control software to prevent system-level changes
  - Remove all unneeded/unnecessary software and services
  - Configure firewall rules to block all unneeded/unnecessary ports and protocols
  - Remove all unneeded accounts
  - Set all required accounts to the minimal privilege level



## EOL Paperwork

- To continue the use of EOL software an Agency will need to submit the following paperwork:
  - Security Exception Request for Section SI-2-COV of ITRM COV SEC 501-07
  - Documentation of installed system integrity controls
  - Remediation plan to decommission the EOL software

# Questions???

For more information, please contact:  
[CommonwealthSecurity@vita.virginia.gov](mailto:CommonwealthSecurity@vita.virginia.gov)

Thank You!





# 2013 Penetration Test

Bob Baskette  
Senior Manager, Security Operations  
and Architect



Virginia Information Technologies Agency

# Upcoming Events





# Information Security System Association

## ISSA

**DATE: Wednesday, November 13, 2013**

**LOCATION: Maggiano's Little Italy**

11800 West Broad Street, #2204, Richmond, VA 23233

**TIME: 11:30 - 1:00pm. Presentation starts at 11:45.**

**Lunch served at 12.**

**COST: ISSA Members: \$20 & Non-Members: \$25**

**SPEAKER: CISO Panel**

*More info located here: <http://centva.issa.org/central-va-issa-feb-2013-meeting/>*



# Future ISOAG

Dec 4                      1:00 – 4:00 pm @ CESC  
Keynote Speakers:      Center for Innovative Technology  
   on “MACH37 Project”

*ISOAG meets the 1<sup>st</sup> Wednesday of each month in 2013*



## Upcoming Training Available

### *Fraud & Awareness for Gov't Finance Professionals*

**DATE:** Wednesday, December 4, 2013

**LOCATION:** James Monroe Building

**TIME:** 8:15 - 4:45pm.

**COST:** \$160 with 8 CPE's awarded

**Trainer:** Courtenay Thompson

To Register and More info located here: <https://hrtraining.doa.virginia.gov/>



# IS Orientation

**When: Thursday, Dec 5, 2013**

**Time: 10:00 am to Noon**

**Where: CESC , Room 1221**

**Register here:**

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

**Next IS Orientation will be held on Mar 9, 2014**



## Save The Date

### **IT Security Conference** ***“Information Security Enabling the Business”***

**Date: April 3 & 4, 2014**

The event will include numerous topics.

*More details will be provided soon!*



## Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)



# ISOAG-Partnership Update

*IT Infrastructure Partnership Team  
Bob Baskette*

6 November, 2013



**NORTHROP GRUMMAN**



# ADJOURN

## THANK YOU FOR ATTENDING

