



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

February 25, 2009

February





ISOAG February 2009 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, VITA
II.	2008 Statewide Review of Information Security in the Commonwealth of Virginia	Goran Gustavsson, Auditor of Public Accounts
III.	USB Drive Encryption Methods, Procedures, & Workplace Security	Richard Seweryniak, Va. State Police
IV.	SAS 70 and Security Audits Update	Eric Bowlin & Brownell Combs, Deloitte & Touche
V.	DNS Security Extensions	Michael Watson, VITA
VI.	Status of New Guidelines	John Green, VITA
VII.	FACTA Red Flag Rules	John Green, VITA
VIII.	IREC	Peggy Ward, VITA
IX.	General Assembly Legislation Session 2009	Peggy Ward, VITA
X.	Upcoming Events & Other Business	Peggy Ward, VITA



CoV ISOAG Briefing



2008 Statewide Review of Information Security in the Commonwealth of Virginia

Goran Gustavsson
Auditor of Public Accounts



Objectives

1. Determine whether agencies and institutions of higher education have adequately established and documented their information security programs.



Objectives

2. Determine whether agencies and institutions of higher education have adequately operationalized* and adhered to their information security programs.

* Yes, *Operationalize* is a word according to Webster's New Millennium™ Dictionary of English



Objectives

3. Analyze the progress made by agencies and institutions of higher education since our last statewide information security report.
- Last report mandated by SJR51 by the 2006 General Assembly.



Objectives

4. Determine if the Commonwealth's information security strategies continue to follow best practices.



Scope

- March 2007 and November 2008
- Majority part of scheduled audits
- Included 74 agencies
- Agencies also part of 2006 study



Methodology

- Objective 1 – Program Documentation
 - Same review criteria and process as the 2006 study.
 - Evaluated 11 security program components



Methodology

- Objective 1 – Program Documentation
 - BIA, RA, COOP, and DRP
 - ISO assignment in Organization
 - Security Awareness Training
 - P&P for approving logical access
 - User authentication to all systems
 - Password controls
 - Physical safeguards
 - Monitoring



Methodology

- Objective 1 – Program Documentation
 - Adequate: Included documentation of all 11 security program components
 - Inadequate: At least started one of the four fundamental documents (BIA, RA, COOP, DRP)
 - No Program: None of the fundamental documents started



Methodology

- Objective 2 – Program Adherence
 - Adequate : Agency follows and periodically updates and refines its security program.
 - Inadequate: Agency does not perform, update or test significant portions of its security program.



Results

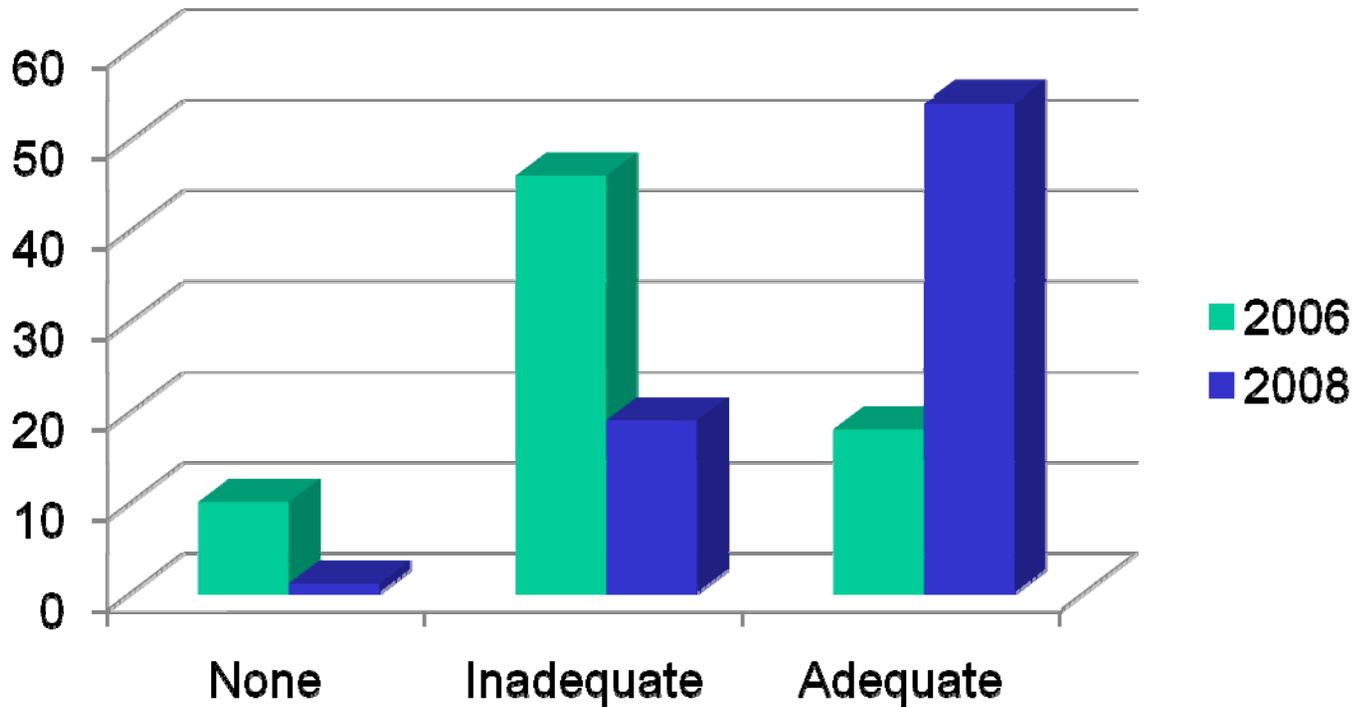
- Objective 1 – Program Documentation

	2006		2008	
Rating	Agencies	%	Agencies	%
None	10	14%	1	1%
Inadequate	46	62%	19	26%
Adequate	18	24%	54	73%



Results

- Objective 1 – Program Documentation





Results

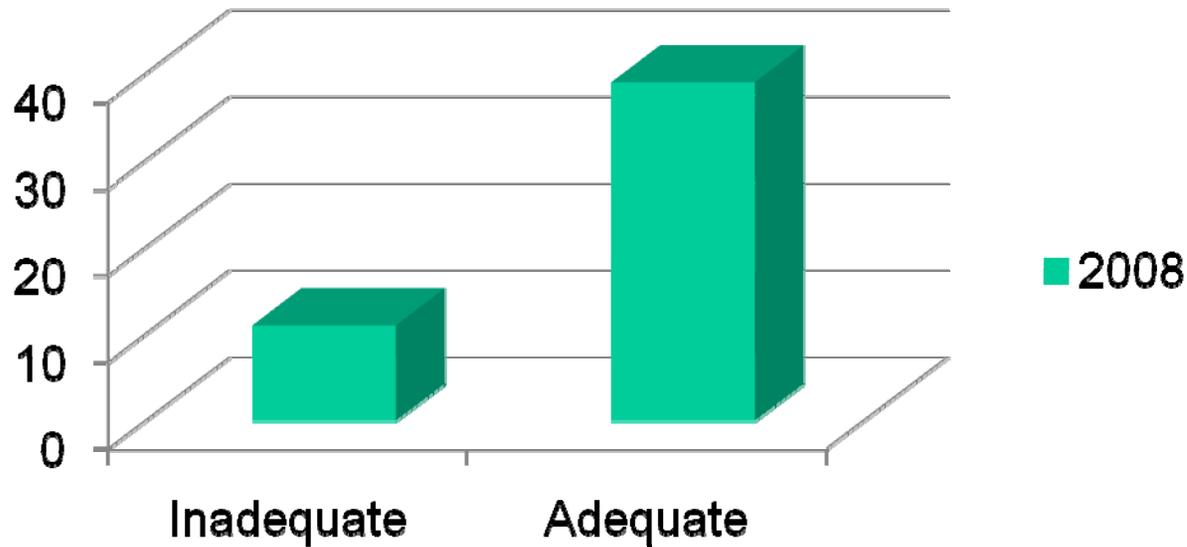
- Objective 2 – Program Adherence

	2008	
Rating	Agencies	%
Inadequate	11	22%
Adequate	39	78%



Results

- Objective 2 – Program Adherence





Results

- Objective 3 - Analysis
- Most noticeable weaknesses
 - Contingency Plans (COOP & DRP)
 - Security Awareness Training



Results

- Objective 4 – Policies and Standards
 - CoV's Info. Sec. policies, standards and guidelines are constantly updated using ORCA
 - Solicits comments from the ISO community
 - Additional guidelines developed to aid agencies in implementing InfoSec programs



2006 Report Recommendations Follow-up

- Four recommendations
 - #1: VITA Communication & Assistance
 - #2: CIO InfoSec Program Authority
 - #3: Additional best practices for SEC501
 - #4: Small agency support
- All four recommendations have been addressed.



Conclusion

- Significant improvements
 - 20% to 73% documented programs in 2 years.
 - 76% of agencies follows and periodically update and refine their programs
 - Commonwealth received 2008 award from NASCIO – Information Security and Privacy category
 - **Keep up the good job!**



Questions?

- **Contact**

Goran Gustavsson

Audit Director

Information Systems Security Specialty Team

Auditor of Public Accounts

Commonwealth of Virginia

(804) 225-3350 ext. 306

goran.gustavsson@apa.virginia.gov

USB drive encryption methods, procedures, and workplace security

Richard Seweryniak
Digital Forensic Examiner

Virginia State Police

Introduction



Mr. Richard Seweryniak
Digital Forensic Examiner

(804) 674-2593

richard.seweryniak@vsp.virginia.gov

Master of Science,
Information Technology
specializing in Information Assurance
University of Maryland

Introduction



Bureau of Criminal Investigation
Criminal Intelligence Division
Computer Evidence Recovery Unit

State Police Headquarters
7700 Midlothian Turnpike
Richmond VA, 23235

CERU

Computer Evidence Recovery Unit of the Virginia State Police provides assistance to local, state and federal law enforcement agencies with on-scene execution of search warrants for computer-related evidence, evidence recovery through forensic examination, and quarterly training classes in computer search and seizure.

CERU

- Investigate the crime or incident, not the technology
 - Network intrusion
 - Peer-to-peer networks
 - Concealed digital cameras
- Not a replacement for internal security
- CERU is “evidence recovery”

Identifying USB Storage

- USB Storage devices can morph into many familiar shapes and devices
 - iPod, iPhone
 - Cell phones
 - Handheld gaming devices
 - Thumb drives
 - Backup storage devices, hard drives

Cultural Integration

- Personal accessories
- Designed for communication, play, and marketed to increase efficiency
- May also serve as a link among work, home, family, friends
- Perceived as personal device, but used at work or school and connected to another machine

Acceptable Use Policy?

- What is your acceptable use policy regarding personal USB devices?
 - Attached to controlled machine with HIPPA, HR, or Security concerns?
 - Storage and Transfer of documents
 - Use of illegal or unlicensed software

Personal Use

- Does Acceptable Use Policy allow personal use as long as it does not interfere with work performance?
- May interfere with “consent to search” if personal items and time are permitted by the policy

Ability to detect?

- Small device size
- Integrated into other devices
- Hidden partitions

- ENCRYPTION !!!



Hidden Partitions

- U3 is most common with autorun “CD-ROM” partition for login authentication then permits the other partition to be accessible.



 Disk 2 Removable 7.48 GB Online	 Partition (G:) 7.48 GB FAT32 Healthy
 CD-ROM 2 CD-ROM 6 MB Online	 U3 System 6 MB CDFS Healthy

Encryption Methods

- Sandisk U3
u3.sandisk.com
- TrueCrypt
truecrypt.org
- Toucan
portableapps.com/apps/utilities/toucan/
- Cryptzone
www.cryptzone.com
- Many others...

Encryption Installation

- By default, such as U3
- As add-on application

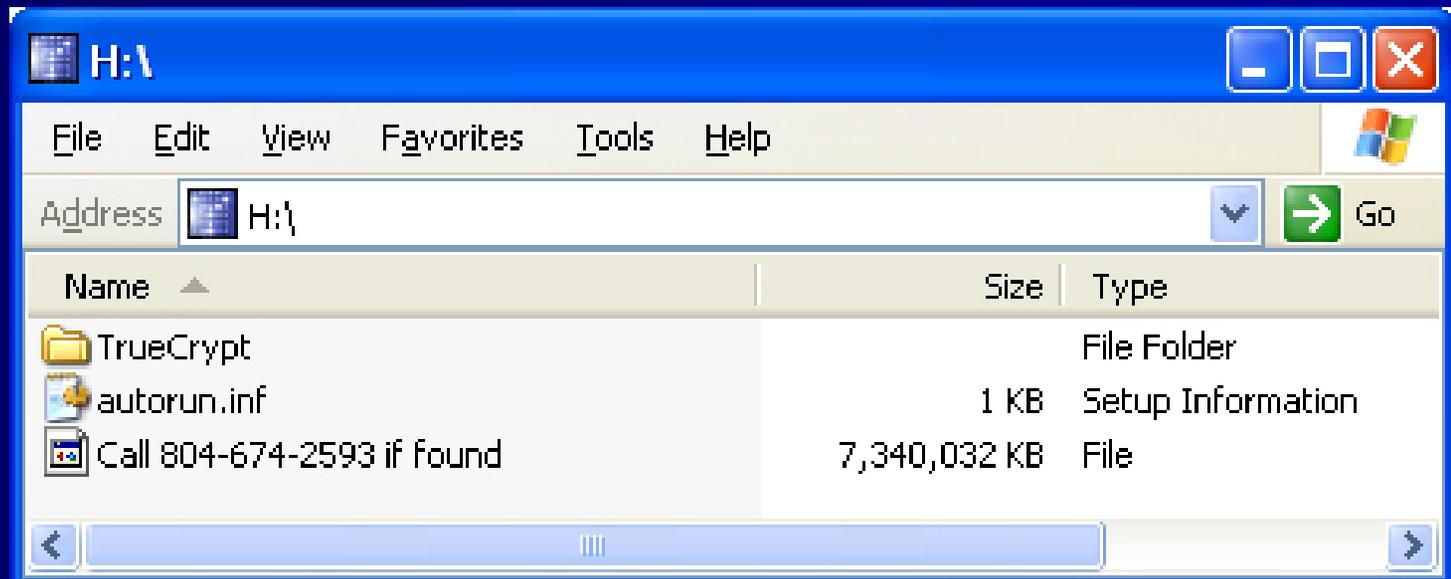


Encryption Abilities

- All or part of the USB drive
- Hidden storage areas and partitions
- TruCrypt is very common
 - Ability to hide partitions, file extensions
 - Entire contents within single data file
 - Must use TrueCrypt application to view

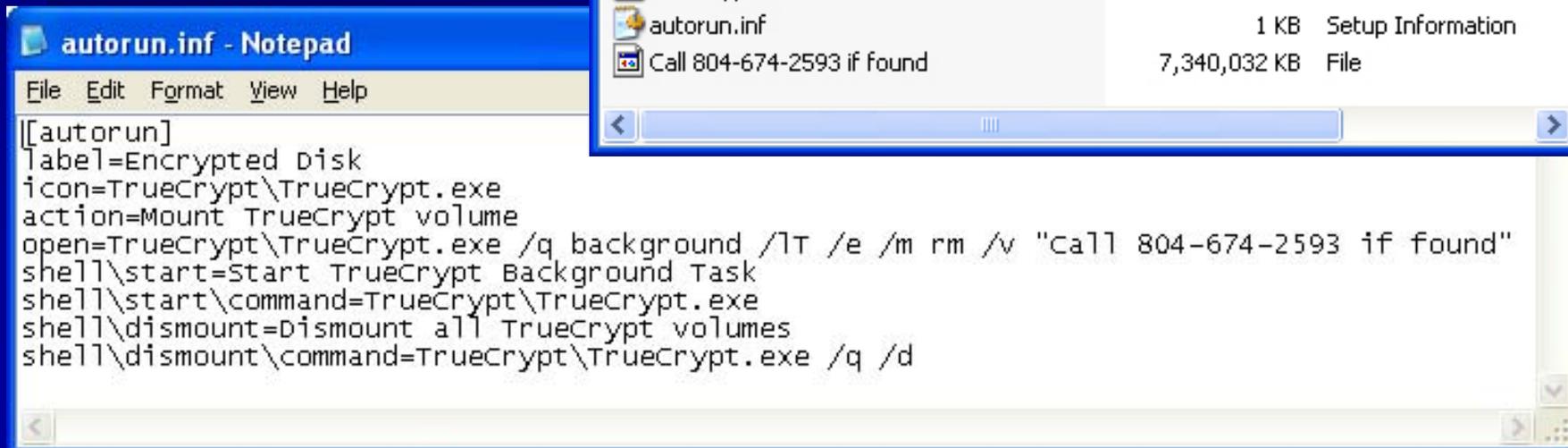
TrueCrypt, non-hidden

- TrueCrypt “Traveler Mode” for USB
 - Typically has autorun.inf file
 - Data file can be in hidden partition or in data file with unknown file extension



TrueCrypt autorun.inf

- www.TrueCrypt.org



The image shows two overlapping windows. The foreground window is a Notepad application titled "autorun.inf - Notepad". It contains the following text:

```
[[autorun]
label=Encrypted disk
icon=TrueCrypt\TrueCrypt.exe
action=Mount TrueCrypt volume
open=TrueCrypt\TrueCrypt.exe /q background /!T /e /m rm /v "call 804-674-2593 if found"
shell\start=Start TrueCrypt Background Task
shell\start\command=TrueCrypt\TrueCrypt.exe
shell\dismount=Dismount all TrueCrypt volumes
shell\dismount\command=TrueCrypt\TrueCrypt.exe /q /d
```

The background window is a Windows Explorer window titled "H:\". It shows the contents of the H:\ drive. The address bar shows "H:\". The file list is as follows:

Name	Size	Type
TrueCrypt		File Folder
autorun.inf	1 KB	Setup Information
Call 804-674-2593 if found	7,340,032 KB	File

Arguments for Encryption

- Removable devices not as easily protected by physical security measures
- Vulnerable to interception and theft
- Portability lends itself to misplacement
- Keep data secure even if lost or stolen

Business Solutions

- Part of a backup routine
- Part of "offsite" storage solution
- Ensures data safety during transport

Arguments Against

- It's a storage device!
- Able to transfer documents and data outside of authorized machines, network, and security measures
- May introduce virus, worm, or other harm to machines and network
- Security breaches, HIPPA violations

Detecting using Registry

- Windows Registry retains records of all USB devices connected, even if no longer connected!
- Excellent ability to audit remotely

Registry Locations

- Start → Run → regedit
- HKEY_LOCAL_MACHINE
 - \SYSTEM
 - \CurrentControlSet
 - \Enum
 - \USB

Things to look for

- Friendly Name
- Device Description
- Service

- Hardware ID may provide details on serial number, revision number, and manufacturer

iPod entry

The screenshot shows the Windows Registry Editor window. The left pane displays the tree structure of the registry, with the path `USB\000A270012DD9DEF` selected. The right pane shows a list of registry values for this path, including `(Default)`, `Capabilities`, `Class`, `ClassGUID`, `CompatibleIDs`, `ConfigFlags`, `DeviceDesc`, `Driver`, `HardwareID`, `LocationInformation`, `Mfg`, `Service`, and `UIINumber`.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000014 (20)
Class	REG_SZ	USB
ClassGUID	REG_SZ	{36FC9E60-C465-11CF-8056-444553540000}
CompatibleIDs	REG_MULTI_SZ	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubClass_06 USB\Class_08
ConfigFlags	REG_DWORD	0x00000000 (0)
DeviceDesc	REG_SZ	USB Mass Storage Device
Driver	REG_SZ	{36FC9E60-C465-11CF-8056-444553540000}\0020
HardwareID	REG_MULTI_SZ	USB\Vid_05ac&Pid_120a&Rev_0001 USB\Vid_05ac&Pid_120a
LocationInformation	REG_SZ	iPod
Mfg	REG_SZ	Compatible USB storage device
Service	REG_SZ	USBSTOR
UIINumber	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\Vid_05ac&Pid_120a\000A270012DD9DEF

iPhone Entry as "usbscan"

Registry Editor

File Edit View Favorites Help

USB

- ROOT_HUB
- ROOT_HUB20
- Vid_0000&Pid_0000
- Vid_03ee&Pid_6901
- Vid_0403&Pid_6001
- Vid_0430&Pid_0205
- Vid_0457&Pid_0151
- Vid_046d&Pid_c016
- Vid_04b4&Pid_120d
- Vid_04b4&Pid_120d&MI_00
- Vid_04b4&Pid_120d&MI_01
- Vid_058f&Pid_6362
- Vid_05ac&Pid_120a
- 000A270012DD9DEF
- Vid_05ac&Pid_1292
 - 1ca2cb9db0284cb2720c27de624f06111f87c471
- Vid_05dc&Pid_0080
- Vid_05e3&Pid_0301
- Vid_064f&Pid_03e9
- Vid_0718&Pid_0147
- Vid_072f&Pid_9000
- Vid_0781&Pid_5151
- Vid_0781&Pid_5406
- Vid_0781&Pid_5408
- Vid_07c4&Pid_a400
- Vid_0aec&Pid_3260
- Vid_0bb4&Pid_0b04
- Vid_13fe&Pid_1a00

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000094 (148)
Class	REG_SZ	Image
ClassGUID	REG_SZ	{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}
CompatibleIDs	REG_MULTI_SZ	USB\Class_06&SubClass_01&Prot_01 USB\Class_06&SubClass_01 USB\Class_06
ConfigFlags	REG_DWORD	0x00000000 (0)
DeviceDesc	REG_SZ	Digital Still Camera
Driver	REG_SZ	{6BDD1FC6-810F-11D0-BEC7-08002BE2092F}\0000
FriendlyName	REG_SZ	Apple iPhone
HardwareID	REG_MULTI_SZ	USB\Vid_05ac&Pid_1292&Rev_0001 USB\Vid_05ac&Pid_1292
LocationInformation	REG_SZ	iPhone
Mfg	REG_SZ	Generic
Service	REG_SZ	usbscan
UINumber	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB\Vid_05ac&Pid_1292\1ca2cb9db0284cb2720c27de624f06111f87c471

Modifying Registry

- Simple change can be enacted in broadcast update using .REG file
- The .REG file can be distributed to remote users and telecommuters
- Incorporate into agency-wide "image" of desktop machines and laptops

Pitfalls

- Accepted USB storage devices and backups would be disabled
- Policy may prohibit disabling of devices, should you modify the policy?
- Increase in number of help desk calls regarding personal devices no longer working with company computers

Registry Locations

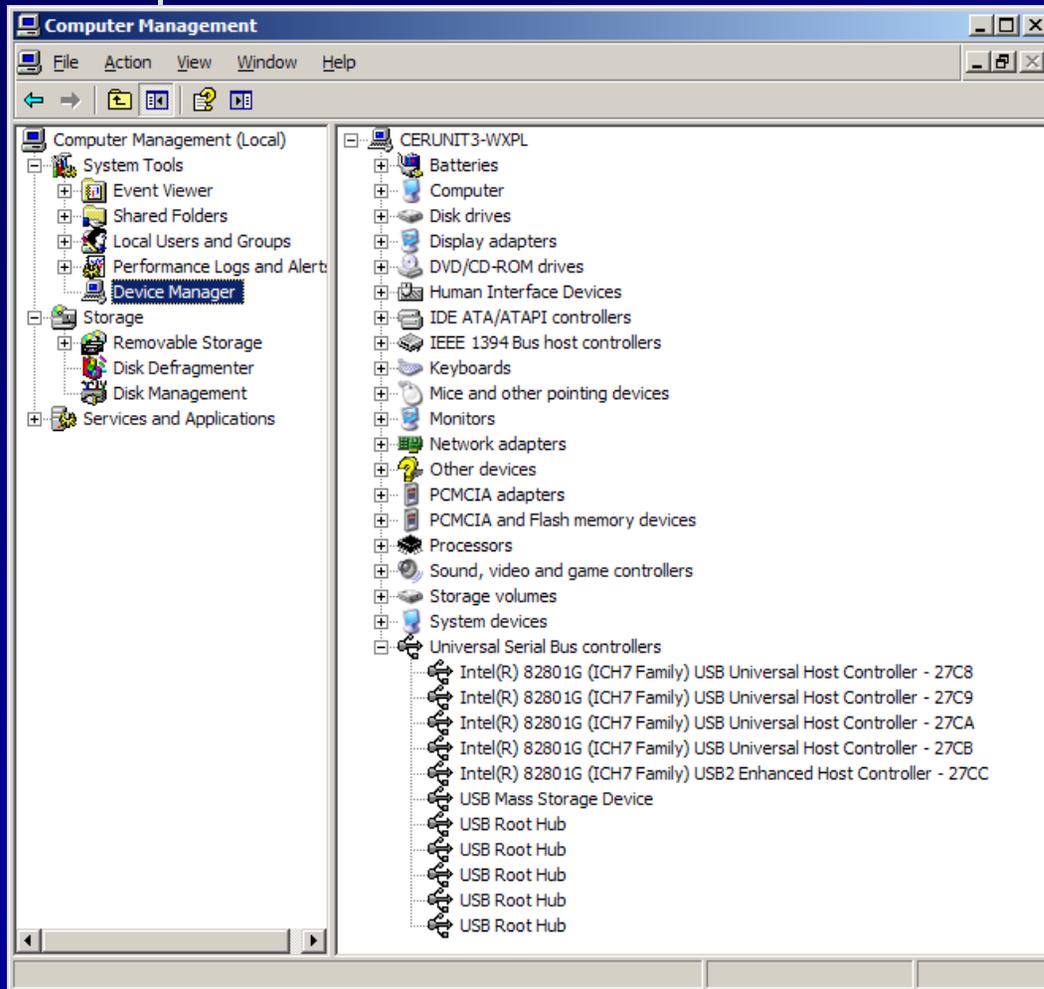
- Start → Run → regedit
- HKEY_LOCAL_MACHINE
 - \SYSTEM
 - \CurrentControlSet
 - \Services
 - \USBSTOR

Lists USB Storage Devices

The image shows a screenshot of the Windows Registry Editor. The left pane displays the tree structure under **USBSTOR**. The right pane shows a list of registry values for the selected path: **My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk\Ven_Apple&Prod_iPod&Rev_1.62\000A270012DD9DEF&0**.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
DeviceDesc	REG_SZ	Disk drive
Driver	REG_SZ	{4D36E967-E325-11CE-BFC1-08002BE10318}\0015
FriendlyName	REG_SZ	Apple iPod USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskApple__iPod_____1.62 USBSTOR\DiskApple__iPod_____1.62
Mfg	REG_SZ	(Standard disk drives)
ParentIdPrefix	REG_SZ	7839946632&0
Service	REG_SZ	disk
UIINumber	REG_DWORD	0x00000000 (0)

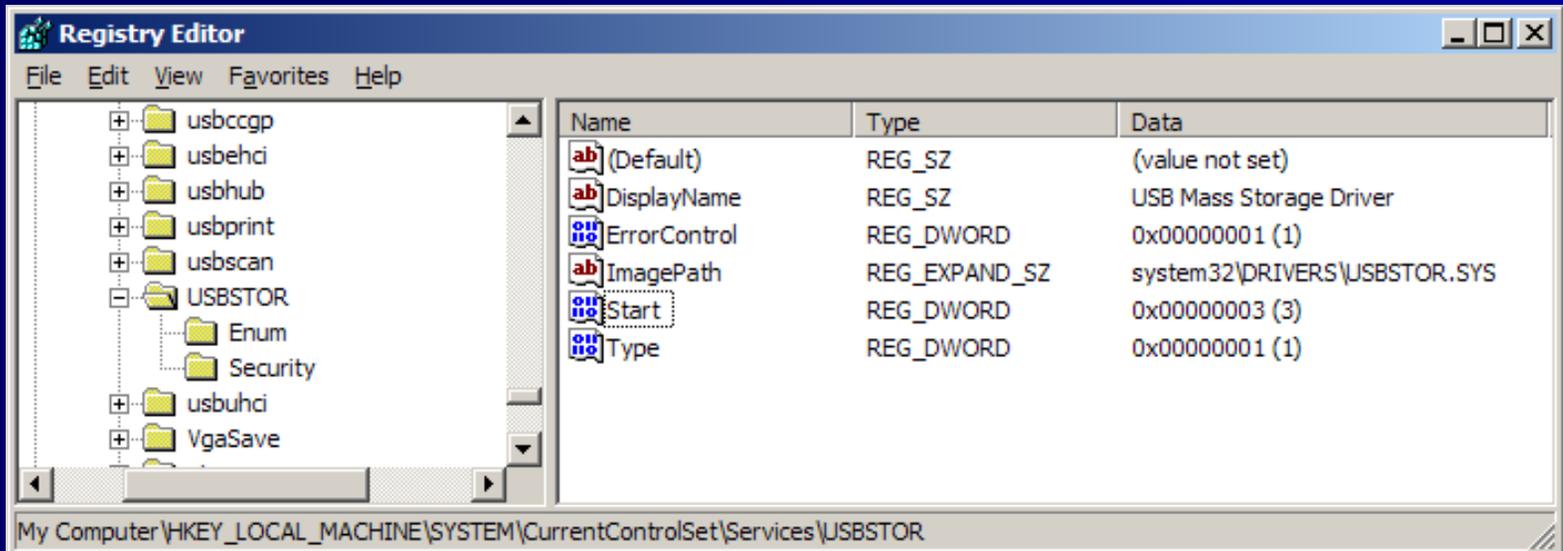
Device Manager



- Lists only currently connected devices
- Note the USB Mass Storage Device entry
- Right-click icon for “My Computer” and then select option “Manage”

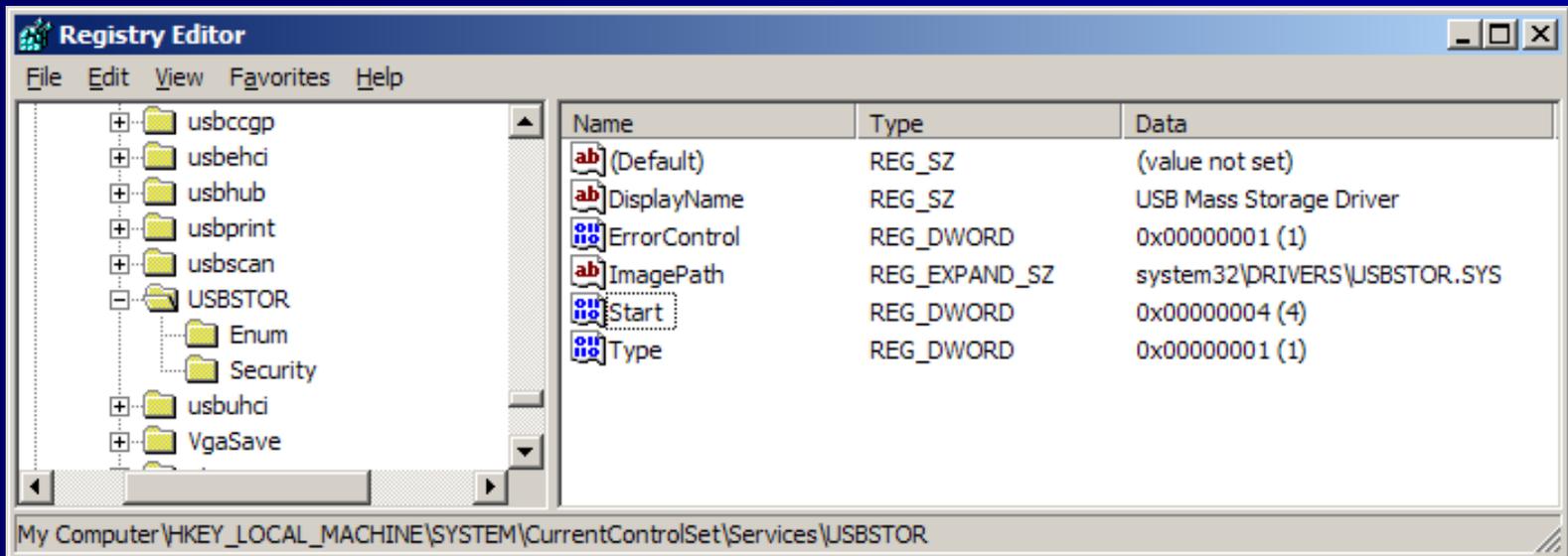
Registry Value = 3

- \HKEY_LOCAL_MACHINE
 \SYSTEM
 \CurrentControlSet
 \Services
 \USBSTOR



Registry Value = 4

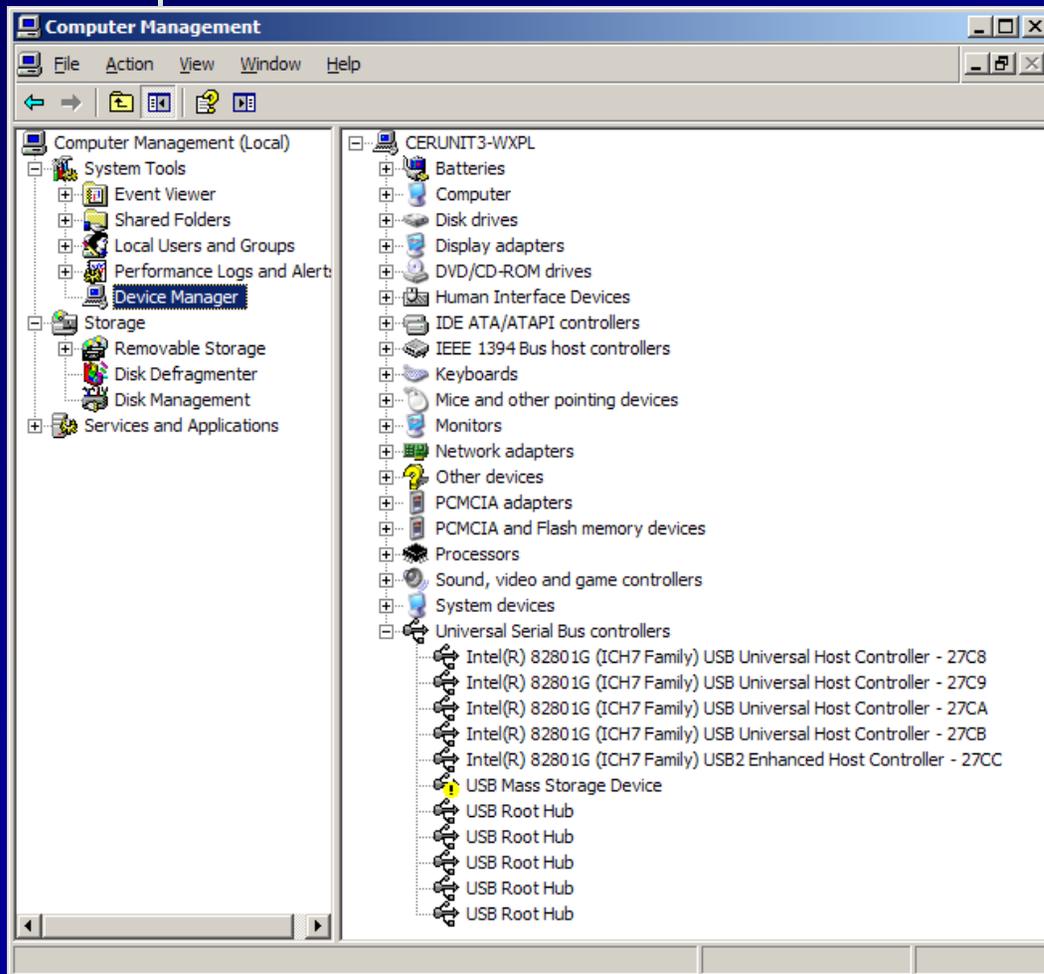
- Double-click entry name "Start" and change the value to "4" to modify.



After the change

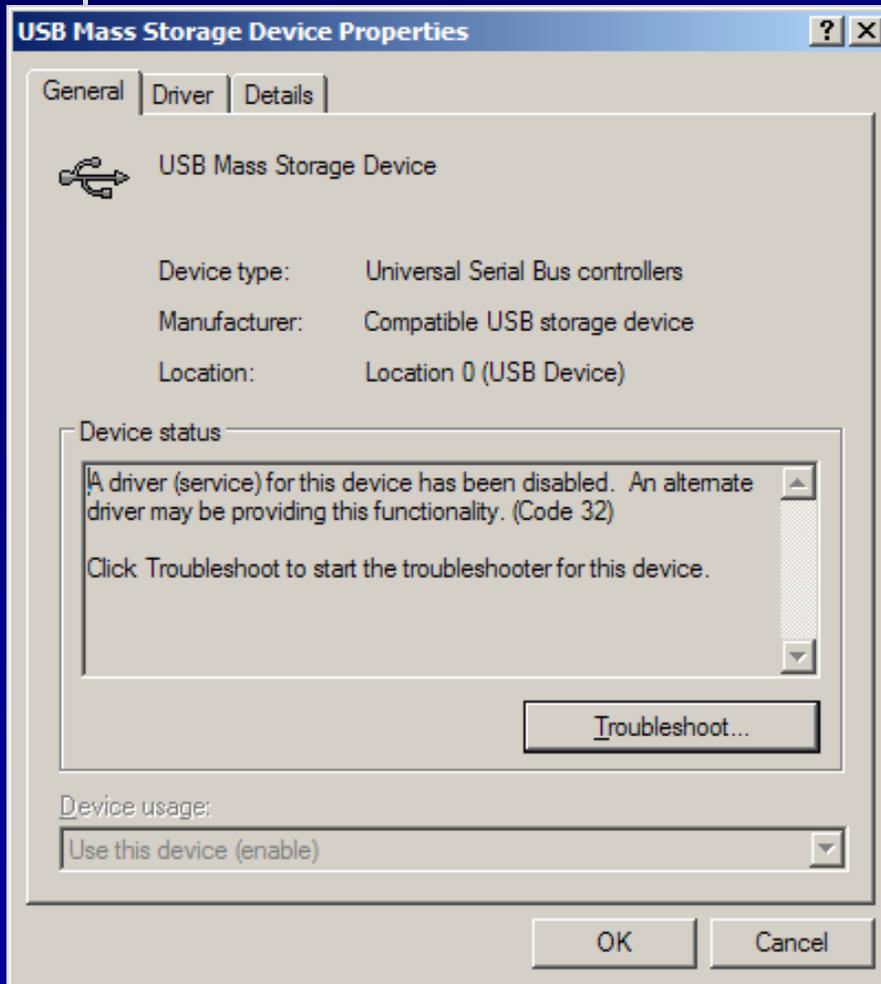
- Recommend users reboot after the change or using .REG file because some USB devices may be currently connected
- Newly connected USB devices will no longer have storage capability based on registry settings

Device Manager



- USB Storage devices will show an error
- Note the USB Mass Storage Device entry
- Does NOT affect non-storage devices such as USB keyboards and mice

Device Properties



- What the user sees if double click the icon in Device Manager
- "A driver for this device (service) has been disabled."

Service

- Remember that the Service is basically a driver for a type of device, such as USBSTOR vs another type of device such as USB keyboard or mouse
- Change did not affect any other types of services

Acceptable Use Policy

- Clause for seizure of personal devices
- Disable storage capability
- Enforcement of document and data transfer outside of security measures

Thank You!

Mr. Richard Seweryniak
Digital Forensic Examiner

(804) 674-2593

richard.seweryniak@vsp.virginia.gov

Bureau of Criminal Investigation
Criminal Intelligence Division
Computer Evidence Recovery Unit

State Police Headquarters
7700 Midlothian Turnpike
Richmond VA, 23235

SAS 70 & Security Audits Update

February 25, 2009

Discussion Outline

A. SAS 70

B. Security Audits

C. Schedule

D. Your role

E. Questions

SAS 70 Background

- SAS = Statement on Auditing Standards (American Institute of Certified Public Accountants)
- Required by the Comprehensive Infrastructure Agreement (CIA)
- SAS 70 sets the standard for an audit of a service provider's internal controls
- Used by the Commonwealth's Auditor of Public Accounts (APA) for their Consolidated Annual Financial Report (CAFR)
- Consideration of Risk and Materiality

Scope Considerations

- 11 Control Objectives – Input from the Partnership & the APA
- Single Report covers entire fiscal year (7/1/08 – 6/30/09)
- Primary areas covered:
 - ▶ Job Scheduling & Monitoring
 - ▶ Backup, Retention & Restoration
 - ▶ System Monitoring
 - ▶ Help Desk
 - ▶ Physical Security
 - ▶ Environmental Security
 - ▶ Logical Security (Mainframes, Servers, Databases, Firewalls, Routers)
 - ▶ Change Management

IT Infrastructure Scope Considerations

Central Operations (CESC)

DOA

VDA

ABC

DOC

CB

DOE

VEC

DEQ

DGS

VDH

DHRM

DMHMRSAS

DMA

DMV

DPB

DRPT

DRS

DSS

TAX

VDOT

TD

Scope Considerations: *Prior Observation Follow-Up*

- Not a full scope audit
- Only testing previous issues for which remediation has been implemented
- Covers IT infrastructure operations at the following agencies:
 - DVS
 - SBE
 - DJJ
 - DHP
 - VMFA
 - DFP

Security Audit

- Required by the CIA
- Used to assess adherence to VITA Security Standards and commonly accepted industry practices.
- Scope includes eight agencies based on risk assessment.
- Point-in-time coverage.
- Separate reports for operations at each agency.

Security Audit Scope

Relevant Agencies

- ▶ VITA Central (CESC)
- ▶ ABC
- ▶ DOC
- ▶ VDH
- ▶ DMV
- ▶ DSS
- ▶ TAX
- ▶ VDOT

Scope

- ▶ Backup, Retention & Rotation
- ▶ Operating System Security
- ▶ Network Security
- ▶ Malicious Code Protection
- ▶ Threat Management
- ▶ IT Security Awareness & Training
- ▶ Personnel Security
- ▶ Facilities Security

Schedule

as of February 18, 2009 (subject to change)

Expected Relevant Agencies (TBD)	Performance Dates																		
	2/9 - 2/27	3/2 - 3/20	3/23	3/30 - 4/17	4/20 - 5/8	5/11	5/18	5/25	6/1	6/8	6/15	6/22	6/29	7/6	7/13	7/20	7/27		
Accounts, Department of			No onsite fieldwork. Documentation week for D&T staff.			No onsite fieldwork. Documentation week for D&T staff.													
Aging, Department for the																			
Alcoholic Beverage Control, Department of																			
Compensation Board																			
Corrections, Department of																			
Education, Department of																			
Employment Commission, Virginia																			
Environmental Quality, Dept. of (Remediation Only)																			
General Services, Department of (eVA Only)																			
Health, Department of																			
Human Resource Management, Department of																			
Mental Health, Mental Retardation and Substance Abuse																			
Military Affairs, Department of																			
Motor Vehicles, Department of																			
Planning and Budget, Department of																			
Rail and Public Transportation, Department of																			
Rehabilitative Services, Department of																			
Social Services, Department of																			
Taxation, Department of																			
Transportation, Department of																			
Treasury, Department of the																			
VITA Central Operations																			
Remediation Testing (VMFA, DFP, DHP, DVS, DJJ, SBE)																			
Rollforward Testing (for agencies with interim testing prior to 6/1)																			

- Team 1
- Team 2
- Both teams

What we'll need from you

- Very little!
- Any contact from our teams will be coordinated through your VITA CAM.
- The focus will be non-agency control activities and should have a minimal impact on agency personnel.
- Please understand and appreciate that Partnership personnel will have increased demands on their time while we're onsite.
- Other possibilities:
 - ▶ Agency contractor lists
 - ▶ Agency employees with administrative rights to infrastructure devices

Questions?

Thanks for your time!



Virginia Information Technologies Agency

DNS Security Extensions

Michael Watson

Security Incident Management Director





DNS Security Extensions (DNSSEC)

- Discuss basic DNS terminology
- Current problems with DNS
- The proposed solution
- How it affects COV



DNS Security Extensions (DNSSEC)

- The Basics
 - DNS – Domain Name Service
 - Translator between computer speak and the human language.
 - DNS Recursion – When a DNS query cannot be resolved by a local DNS server the query is made by the DNS server to another DNS server to try and get the answer.
 - Root Servers – The servers that contain the top level domain server information.
 - Top Level Domain – TLD - .com, .org, .gov, etc.
 - DNS Cache – The data about the domain name that the DNS servers and clients keep after a query.

Security Issues With DNS

- DNS Poisoning – Tricking a DNS client or server into sending back a different IP address than what is registered.
 - Kaminsky Attack
 - Virus/Malware
- DNS Denial of Service – Using DNS servers to perform denial of service attacks.
 - Request a root server DNS lookup by spoofing the DoS target IP address.



How Does DNSSEC Help?

- DNS Security Extensions
 - Provides Authentication and Integrity
 - Authentication of the origin
 - Authentication for denial of existence
 - Data integrity
 - Uses public keys and signatures
 - Requires additional data in the DNS packets
 - Does not provide protection from denial of service
 - Helps to prevent spoofing



How Does DNSSEC Hurt?

- More network traffic
 - Infrastructure load increases
 - Larger packets
 - Easier to cause a denial of service
- More resources required
 - Encryption requires more processing
- Requires reconfiguration
 - Planning
 - DNS servers must support it.



What Does DNSSEC Mean for COV?

- .GOV root servers have already made the switch
 - .mil is coming soon
 - More domains are likely to change soon
- Virginia will eventually be following suit
 - Main virginia.gov server will eventually change
 - Agency hosted DNS servers will need to change at some point



Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

For more information on the tools mentioned in this
presentation:

Michael.Watson@VITA.Virginia.GOV

Thank You!



Virginia Information Technologies Agency

Status of New Guidelines

Facilities Security and IT Asset Management

John Green

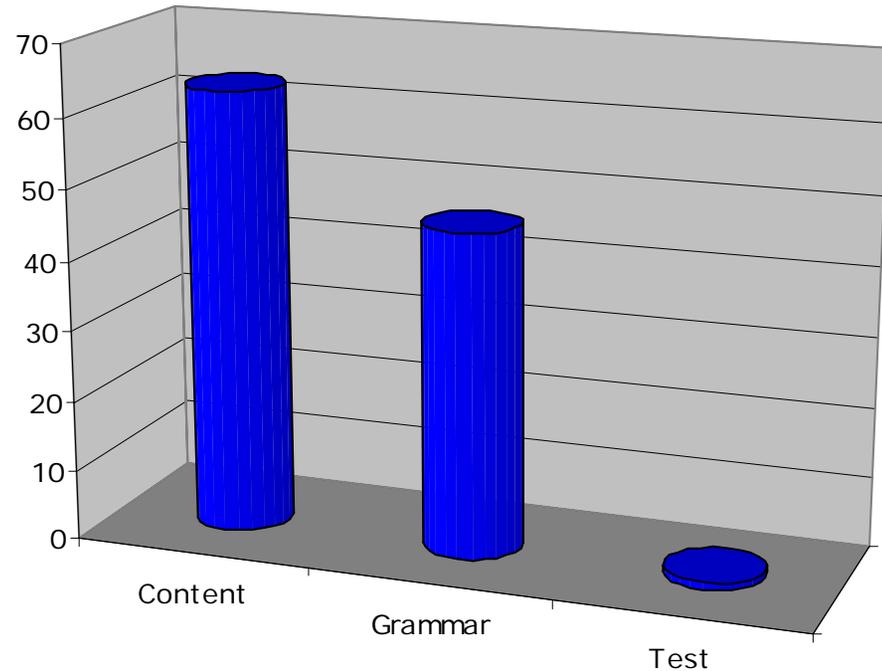
Deputy Chief Information Security Officer



Facilities Security Guideline

- Posted on: 01/08/09
- Duration: 30 days
- Comments: 110
 - 63 Content
 - 46 Grammar
 - 1 Test
- Comment review
- Reviewer feedback
- Completion: 03/31/09

Comment Distribution





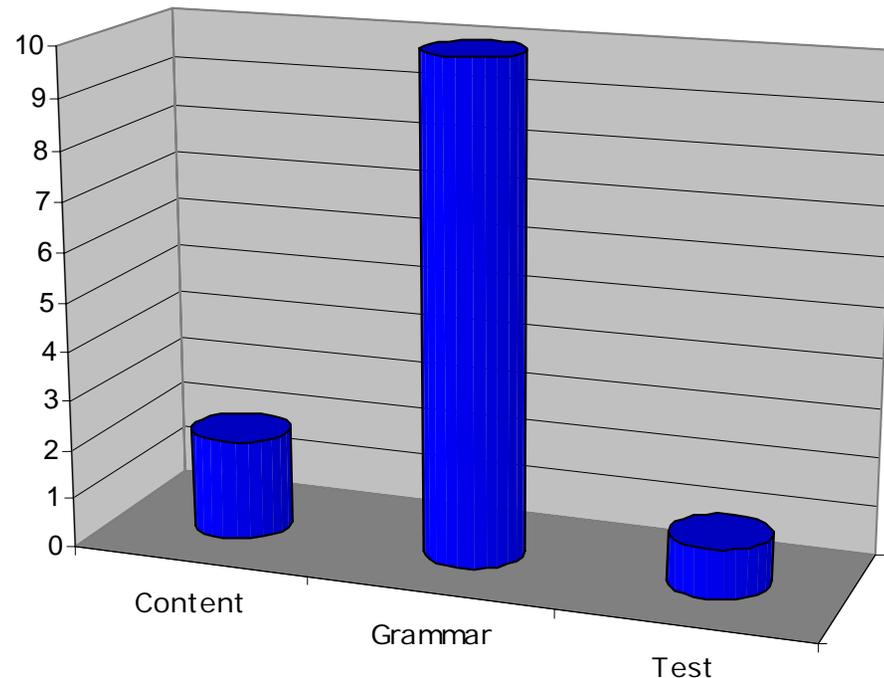
Hotspots: Facilities Security

- Pages 7 and 8 received 34 total comments
 - Facilities Security Practices and Safeguards
 - Safeguarding IT Systems and Data
 - Safeguards to Protect Against Human, Natural, and Environmental Risks
 - Logical Access Controls
 - Electronic Access Control

IT Asset Management Guideline

- Posted on: 01/30/09
- Duration: 30 days
- Will close: 02/28/09
- Comments: 13
 - 2 Content
 - 10 Grammar
 - 1 Test
- Comment review
- Reviewer feedback
- Completion: 03/31/09

Comment Distribution





QUESTIONS?





Virginia Information Technologies Agency

FACTA





FACTA Red Flag Requirements

Implementation Date: May 1, 2009

Are you aware of the red flag requirements in the Fair and Accurate Credit Transactions Act (FACTA) of 2003?

Please read carefully as it is not only banks and financial institutions!

<http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>



General Assembly Legislation Session 2009

Peggy Ward





HOTLINK

For easy web access to any of the House or Senate Bills right click on the bill number and choose Open Weblink.



HB 1797

Unsolicited bulk electronic mail (spam); penalty.

Unsolicited bulk electronic mail (spam); penalty. Creates a Class 1 misdemeanor for (1) the use of a computer or computer network to transmit, with the intent to falsify or forge electronic mail transmission information or other routing information, unsolicited bulk electronic mail (spam) through or into the computer network of an EMSP that has implemented anti-spam security measures; or (2) knowingly selling, giving, or otherwise distributing or possessing with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of the transmission information or other routing information of spam in an effort to bypass anti-spam security measures of an EMSP; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of the transmission information or other routing information of spam; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of the transmission information or other routing information of spam.

A person is guilty of a Class 6 felony if, in addition to the Class 1 misdemeanor offense, (i) the volume of spam transmitted exceeded 10,000 attempted recipients in any 24-hour time period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or (ii) the revenue generated from a specific spam transmission exceeded \$1,000 or the total revenue generated from all spam transmitted through any EMSP exceeded \$50,000. This bill parallels the existing spam law but adds provisions requiring that a person bypass an anti-spam security measure implemented by an EMSP to be culpable for the offense. **Patron: Loupassi**

Status:

02/10/09 House: Left in Courts of Justice



HB 2028

Surplus materials; DGS to establish procedure to allow members to purchase certain laptop computers.

Disposition of surplus materials; certain laptop computers. Requires the Department of General Services to establish procedures that allow members of the General Assembly in accordance with rules established by the Joint Rules Committee to purchase, at a reasonable cost not to exceed the trade-in value for such equipment, the laptop computers, software, and related peripheral equipment provided to them by the respective clerk of the House of Delegates or the Senate of Virginia. ***Patron: Marshall***

Status:

01/29/09 House: Stricken from docket by General Laws by voice vote



HB 2421

Freedom of Information Act; definition of public record.

Freedom of Information Act; definition of public record. Clarifies that the definition of public record does not include correspondence, messages or other records or portions thereof created or received by a public employee, appointee or officer that relate to personal matters and do not address public business; however such records may be disclosed in the discretion of the custodian. ***Patron: May***

Status: 02/10/09 House: Left in General Laws



HB 2033

State employees; four-day work week.

State employees; four-day work week. Creates the "Work 4 Savings Initiative" and requires the Department of Human Resource Management, among other duties, to (i) establish and implement a program, with the approval of the Governor, that permits any state employee to work a four-day work week consisting of four 10-hour days, Monday through Friday, per week, the impact of which is fiscally neutral and keeps state employee annual holiday leave accrual whole and (ii) report to the Governor and General Assembly on the implementation of this program. The bill exempts certain public safety and other agencies from participation in the program. The bill provides that implementation of the four-day work week program shall be mandatory for state agencies covered in the bill when the Revenue Stabilization Fund is impacted. The Governor shall by executive order direct such state agencies to implement the four-day work week program within such time and manner as directed in the executive order, not to exceed 60 days of the issuance thereof. When the Revenue Stabilization Fund is no longer impacted, the Governor may rescind the executive order requiring implementation of the four-day work week program. The bill provides that its provisions will expire on July 1, 2012. **Patron: Lingamfelter**

Status:

02/05/09 House: Stricken from docket by General Laws by voice vote



HB 2438

Electronic reforms; various amendments to Title 24.2 that authorize State Board of Elections.

Electronic reforms; State Board of Elections. Makes various amendments to Title 24.2 (Elections) that authorize the State Board of Elections to utilize various electronic systems. The bill specifies that the State Board shall (i) accept absentee voter applications and receive changes of a registered voter's name or address electronically; (ii) conduct a pilot program permitting a participating candidate for office, other than a party nominee, to provide electronically some or all of the signatures of qualified voters required to get his name on the ballot; and (iii) provide electronic pollbooks for each precinct or locality that uses them at least five days, rather than 10 days, before an election. The bill also provides that the State Board shall provide only electronic pollbooks, and not written pollbooks, for any election held on or after July 1, 2010, or any subsequent year and makes corresponding amendments that become effective on July 1, 2010. The bill also provides that the State Board of Elections may furnish absentee voter applicant lists to candidates or political party chairmen for use only for campaign and political purposes. Such lists shall not contain any voter's social security number, or part thereof, day and month of birth, or the residence address of a voter who has provided a post office box in lieu of a residence street address.

Patron: Poisson

Status: 02/06/09 House: Tabled in Privileges and Elections (15-Y 7-N)



HB 2497

Electronic government; Secretary of Technology to develop and implement strategies therefore.

Facilitation of electronic government. Requires the Secretary of Technology to develop and implement strategies for the adoption of electronic government and electronic signature initiatives that would allow for the electronic submission of documents and forms, with a goal of adoption of electronic government initiatives by July 1, 2013. Each agency would be required to identify such electronic government initiatives that could improve services to citizens and improve efficiencies as part of its strategic plan, and would be required to report to the Secretary of Technology a list of all paper or electronic forms currently in use by the agency. *Patron: Nixon*

Status: 02/10/09 House: Left in Appropriations



HB 2608

Secretary of Administration; telecommuting and alternative work schedules for state employees; effectiveness.

Secretary of Administration; telecommuting and alternative work schedules for state employees; effectiveness. Provides that the Secretary of Administration, in cooperation with the Secretary of Technology and in consultation with the Council on Technology Services, shall measure the effectiveness of the comprehensive statewide telecommuting and alternative work schedule policy. The bill provides that the head of each agency shall report annually to the Secretary on the status of any programs or policies developed and implemented pursuant to this section. Any agency head failing to comply with the requirements of this section shall forfeit one percent of the moneys appropriated for the operation of the agency as provided in the appropriation act. The Secretary shall so notify the Comptroller, who shall take such moneys and deposit them into the Literary Fund. The bill also requires the Department of Human Resource Management to notify state employees by email or other method deemed appropriate by the Department of the statewide telecommuting and alternative work schedule policy.

Patron: Hugo

Status: 02/10/09 House: Left in General Laws



SB 841

REAL ID Act and citizens' privacy; prohibits DMV, etc. from using any type of computer chip, etc.

REAL ID Act and citizens' privacy. Prohibits DMV or any other agency of the Commonwealth from using any type of computer chip or radio-frequency identification on licenses and identification cards and from sharing certain data with other states or with any federal government agency. Further provides that no biometric data will be gathered or retained.

Patron: Cuccinelli

Status: 02/05/09 Senate: Stricken at request of Patron in Transportation (15-Y O-N)



SB 1499

State agency employment and procurement; participation in E-Verify program.

State agency employment and procurement; participation in E-Verify program. Requires state agencies and contractors with state agencies to verify the social security number of newly hired employees using the E-Verify Program. The bill defines "E-Verify Program" as an Internet-based system operated by the Department of Homeland Security in partnership with the Social Security Administration to determine the validity of social security numbers. Under the bill, the effective date of the provisions is contingent on the General Assembly and the governor determining that the E-Verify Program is fully functional and properly funded. ***Patron: Barker***

Status:

01/28/09 Senate: Failed to report (defeated) in General Laws and Technology (4-Y 9-N 2-A)



HB 1660

Telework assistance; Director may advise & assist public & private employers upon request.

Telework assistance to public and private employers; reporting requirements. Transfers certain responsibilities regarding telework assistance from the Secretary of Administration to the Office of Telework Promotion and Broadband Assistance. ***Patron: Scott***

Status:

02/23/09 Senate: Passed Senate (40-Y 0-N)



HB 1796

Unsolicited bulk electronic mail (spam); penalty.

Unsolicited bulk electronic mail (spam); penalty. Creates a Class 1 misdemeanor when a person (1) uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited commercial electronic mail ("spam") through or into the computer network of an electronic mail service provider or its subscribers; or (2) knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that (i) is primarily designed or produced for the purpose of facilitating or enabling the falsification of the transmission information or other routing information of spam; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of the transmission information or other routing information of spam; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of the transmission information or other routing information of spam. A person is guilty of a Class 6 felony if, in addition to the elements of the Class 1 misdemeanor offense, the volume of spam transmitted exceeds a certain limit or the revenue generated exceeds a certain amount. This bill parallels the existing spam law but limits application to commercial electronic mail. Commercial electronic mail is defined in the bill as electronic mail, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose). *Patron: Loupassi*

Status:

02/13/09 Senate: Assigned Courts sub: Criminal



HB 2022

**Technology Services, Council on;
eliminates Council.**

**Council on Technology Services;
repealed.** Repeals the Council on
Technology Services. *Patron: Rust*

Status:

02/18/09 Senate: Signed by President



HB 2023

Virginia Information Technologies Agency; to delegate powers & responsibilities.

Powers of VITA. Authorizes Virginia Information Technologies Agency (VITA), subject to approval by the Secretary of Technology, to delegate to an agency within the executive branch the power to provide for the centralized marketing, provision, leasing, and executing of license agreements for electronic access to public information and government services through the Internet, wireless devices, personal digital assistants, kiosks, or other such related media. The delegated agency would be authorized to fix and collect fees and charges for such services. **Patron: Rust**

Status:

02/18/09 Senate: Signed by President



HB 2044

Health information technology; adoption of standards.

Health information technology; adoption of standards.

Allows the Information Technology Investment Board to establish an advisory committee, consisting of persons with expertise in health care and information technology, to advise it on the adoption of health information technology technical and data standards. *Patron: Nixon*

Status:

02/18/09 Senate: Signed by President



HB 2181

Freedom of Information Act; protection of internal controls of State's financial systems.

Freedom of Information Act; protection of internal controls of the Commonwealth's financial systems. Exempts from the mandatory disclosure requirements of FOIA documentation or other information that describes the design, function, operation, or implementation of internal controls over the Commonwealth's financial processes and systems, and the assessment of risks and vulnerabilities of those controls, including the annual assessment of internal controls mandated by the Comptroller, the disclosure of which would jeopardize the security of the Commonwealth's financial assets. However, summary reports relating to the soundness of any fiscal process shall be disclosed in a form that does not compromise the internal controls. ***Patron: Phillips***

Status:

02/23/09 Senate: Passed Senate (40-Y 0-N)



HB 2285 / SB 936

Searchable Database Website of Revenue, Budget Item, & Expenditure; Sec. of Technology to create.

Secretary of Technology; Virginia Enterprise Applications Program; searchable database website of state budget expenditures and revenues. Provides for the Virginia Enterprise Applications Program (VEAP) within the Office of the Secretary of Technology to create and maintain a searchable database website containing information on state revenues, appropriations, and expenditures. Under the bill, the Director of VEAP shall develop a pilot searchable database website available for public use no later than July 1, 2010. Beginning in July 2011, the searchable database website shall be updated for (i) fiscal years that ended prior to July 1, 2009, and (ii) for future fiscal years not later than 60 days following the close of the fiscal year. The Director of VEAP, the Auditor of Public Accounts and the Joint Legislative Audit and Review Commission shall work together to coordinate efforts in obtaining, summarizing, and compiling information in order to avoid duplication of efforts. The website shall be made available in a format designed to encourage the greatest amount of use by the general public. The website shall provide access to all levels of budget spending in state government *Patron (House) Cline; (Senate) Cuccinelli*

Status: *HB:* 02/23/09 *Senate:* Constitutional reading dispensed (40-Y 0-N)

SB: 02/19/09 *House:* Subcommittee recommends reporting



HB 2423

Broadband Advisory Council; established.

Broadband Advisory Council. Establishes the Governor's Broadband Advisory Council. The purpose of the Council shall be to advise the Governor on policy and funding priorities to expedite deployment and reduce the cost of broadband access in the Commonwealth. The council shall be staffed by the Office of Telework Promotion and Broadband Assistance.

Patron: May

Status: [02/23/09 Senate: Constitutional reading dispensed \(40-Y 0-N\)](#)



HB 2426/SB 1318

Government Data Collection and Dissemination Practices Act; extends implementation of prohibition.

Government Data Collection and Dissemination Practices Act; collection of social security numbers. Extends from July 1, 2009, to July 1, 2010, the implementation of the prohibition against collecting an individual's social security number unless collection of such number is (i) authorized or required by state or federal law and (ii) essential for the performance of that agency's duties. The bill contains several technical amendments, all to become effective July 1, 2010.

Patron: (House) May; (Senate) Houck

Status: HB: 02/23/09 Senate: Passed Senate with substitute (40-Y 0-N)

SB: 02/23/09 Senate: Title replaced 091853244-H1



HB 2427

Protection of Social Security Numbers Act; first five digits to be confidential from disclosure.

Protection of Social Security Numbers Act; penalties. Provides that the first five digits of a social security number contained in a public record shall be confidential and exempt from disclosure under the Freedom of Information Act. The bill does allow release of a social security number under certain limited circumstances, including proper judicial order; to federal, state or local law-enforcement or correctional personnel; by one agency to another agency in Virginia or to an agency in another state, district, or territory of the United States; and to any data subject exercising his rights under the Government Data Collection and Dissemination Practices Act. The bill provides for penalties for violation.

Patron: May

***Status:* 02/23/09 Senate: Passed Senate with amendment (40-Y 0-N)**



HB 2508

Electronic filing; Secretary of Technology to assist state agencies in expanding citizen access.

Electronic filing with state agencies. Authorizes the Secretary of Technology to assist state agencies, as defined in § 2.2-2006, in expanding citizen access to government through the electronic filing of any information required or permitted to be filed with such state agencies. The bill also requires state agencies, as part of the Government Performance and Results Act, to identify in their strategic plan efforts to expand citizen access to government through electronic filing and reporting. ***Patron: Pollard***

Status: 01/26/09 House: Incorporated by Science and Technology (HB2497-Nixon) by voice vote



HB 2539

Information Technology Investment Board; oversight of information technology, etc. in State.

Oversight of information technology and applications in the Commonwealth; Information Technology Investment Board; Chief Information Officer. Includes oversight of agency and enterprise-wide technology applications under the purview of the powers and duties of the Information Technology Investment Board (ITIB). The bill clarifies that the ITIB's contract with the Chief Information Officer may be for a term of up to five years, and appoints the Secretary of Finance to the ITIB in place of the Governor's appointment from a list of individuals nominated by the legislature.
Patron: Nixon

Status: 02/23/09 House: Bill text as passed House and Senate (HB2539ER)



SB 833

Notaries public; equipment, etc. standards for electronic notarization to be developed by ITA.

Notaries public. Provides that equipment, security, and technological standards for electronic notarization shall be developed by the Virginia Information Technologies Agency in consultation with the Secretary of the Commonwealth. The process for developing and maintaining such standards shall be exempt from the Administrative Process Act. In addition, the bill requires that applicants submit a registration form for registering and being commissioned as an electronic notary public, which shall include certification of compliance to the Secretary of the Commonwealth with the aforementioned electronic notary standards developed. Furthermore, the bill provides that a notary's electronic signature and seal shall conform to the developed standards for electronic notarization. This bill contains an emergency clause. ***Patron: Locke***

***Status:* 02/23/09 House: Passed by for the day**



SB 892

Information Technology Investment Board; approval of development of certain major projects.

Information Technology Investment Board; approval of the development of certain major information technology projects. Requires the Information Technology Investment Board, within 30 days after approval of the development of any major information technology project in excess of \$5 million, to notify the House Appropriations and Senate Finance Committees of the scope, cost, and implementation schedule of the proposed project. Under the bill, the Board may proceed with the project unless objections are raised by either Committee within 30 days of the notification. If objections are made, the Board may not proceed with the project until the objections are resolved. ***Patron: McDougle***

Status: 02/19/09 House: Subcommittee recommends reporting



SB 935

Remote access to land records; allows occasional access thereto by public and sets a fee.

Occasional remote access to land records; fee. Allows for occasional remote access to land records by the general public and sets a fee in an amount not to exceed the usual copying fee. Such occasional remote users will not be charged the \$50 per month subscriber fee. ***Patron: Smith***

Status: 02/20/09 House: Reported from Courts of Justice with amendments (22-Y 0-N)



SB 1009

Electronic communication service providers, etc.; search warrants executed upon.

Search warrants executed upon electronic communication service providers or remote computing service providers. Provides that a search warrant for records or other information pertaining to a subscriber to, or customer of, an electronic communication service or remote computing service that is transacting or has transacted any business in the Commonwealth, including the contents of electronic communications, may be served upon such a provider within or without the Commonwealth by mail, facsimile, or other electronic means. Currently, there is no provision for service of such a warrant outside the Commonwealth nor is there a specific provision allowing for mail, fax or electronic service. Additionally, under current law, electronic communications are expressly excluded from the coverage of the warrant. ***Patron: Deeds***

Status:

02/20/09 House: Committee substitute printed 090954220-H1



SB 1046

REAL ID Act, federal; amends provisions for obtaining licenses.

Obtaining licenses and identification cards; federal REAL ID Act. Amends provisions for obtaining licenses to comply with federal REAL ID Act requirements. *Patron: Miller*

Status: 02/23/09 House: Passed by for the day



SB 1277

Land records; social security numbers not be contained therein on Internet.

Land records; social security numbers. Requires, beginning July 1, 2012, that social security numbers not be contained in land records posted via secure remote access to the Internet.
Patron: Newman

Status:

02/16/09 House: Subcommittee recommends reporting



SB 1316

Freedom of Information Act; strikes requirement to publish a database index, etc.

Freedom of Information Act; requirements to publish a database index and a statement of rights and responsibilities. Strikes the requirement to publish an index of computer databases and amends the requirement to publish a statement of rights and responsibilities to ensure that the public can find out generally what types of public records a public body has and what exemptions may apply to those records. This bill is a recommendation of the Freedom of Information Advisory Council.

Patron: Houck

***Status:* 02/23/09 House: Read second time**



SB 1431

REAL ID Act; Commonwealth's participation.

REAL ID Act; Commonwealth's participation. Provides that the Commonwealth will not comply with any provision of the federal REAL ID Act and with any other federal law, regulation, or policy that would compromise the economic privacy, biometric data, or biometric samples of any resident of the Commonwealth. *Patron: Cuccinelli*

Status: 02/23/09 House: Read second time



Virginia Information Technologies Agency

IREC





IREC

Information Risk Executive Council (IREC) Renewal!

Based on the votes from our Information Security professionals we have renewed the Commonwealth of Virginia subscription to the Information Risk Executive Council (IREC). This membership allows every Commonwealth of Virginia State and Local government employee to register and use the services. The tools and papers include those around topics such as Information Security Awareness, Identity and Access Management, Information Protection and more!

Please register by going to:

<https://www.irec.executiveboard.com/Public/Register.aspx>

For questions or problems, please contact:

Jennifer Smith - (202) 587-3601

jsmith@executiveboard.com



Virginia Information Technologies Agency

Upcoming Events





UPCOMING EVENTS!

FBI Citizen's Academy Spring 2009 Class

- Four slots will be made available for InfraGard members.
- Begins: Tuesday, April 14th from 6-9pm. Runs for six weeks every Tuesday.
- Location: 1970 E. Parham Road, Richmond.
- Interested in learning more? Please contact:

Dee Rybiski

FBI Richmond, Community Outreach

804-627-4482



UPCOMING EVENTS! IS Orientation

IS Orientation

Monday, March 9th, 9:00 to 11:30 a.m. @CESC

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV Information Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

Register Online for this and future dates at:

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



UPCOMING EVENTS! IS Council

Commonwealth Information Security Council

Monday, March 16th, 12:00 - 2:00 p.m. @ CESC with
Committee meetings from 2:00 – 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to CommonwealthSecurity@VITA.Virginia.Gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at:

<http://www.vita.virginia.gov/security/default.aspx?id=5128>



UPCOMING EVENTS! March ISOAG

DRAFT AGENDA Wednesday, March 25th

NCFTA/IC3 Overview

**Ken Blotteaux, NCFTA &
Donna Gregory, IC3**

Electronic Content Management

Herb Ward, DEQ

System Access Request Application

Jim Austin, VDOT

Partnership Security Architecture Review

**Don Kendrick, VITA &
Bill Ross, NG**



UPCOMING EVENTS! Future 2009 ISOAG's

**All currently from 1:00 – 4:00 pm at CESC
(please let us know if you want to host in the
Richmond area!)**

Wednesday, March 25

Wednesday, April 29

Wednesday, May 20

Wednesday, June 17

Register Online at:

<http://www.vita.virginia.gov/registration/Session.cfm?MeetingID=3>



UPCOMING EVENTS: MS-ISAC Webcast 4/9

National Webcast:

Thursday, April 9, 2009, 2:00 – 3:00 p.m.

Topic: Application Security

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



UPCOMING EVENTS! CIO-CAO Mtg.

CIO-CAO Communications Meeting:

Formally known as AITR Meeting. This meeting has moved to an every other month schedule.

Thursday, April 23

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: DEQ

629 E. Main St.

Richmond, Va.



UPCOMING EVENTS! Virginia Security Summit

Virginia Security Summit Monday, April 27

8:00 am – 9:00 am: Refreshments

9:00 am: Opening Remarks

Location: Richmond Marriot

The 2009 Virginia Security Summit brings together government Information Security leaders to discuss tools, trends, strategies and best practices. The Summit is for and about government and is free to attend. Register online at <http://www.govtech.com/events/vatech2009>



Virginia Information Technologies Agency

Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING!!

