Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

July 16, 2008

JULY

ISOAG July 2008 Agenda

I.	Welcome and Opening Remarks	Peggy Ward, VITA
II.	JCOTS SSN Collection Survey	Lisa Wallmeyer, Executive Director JCOTS
III.	Roanoke County Information Security Program	Elton Ghee, Roanoke County
IV.	eSupport Implementation	Karen King, Chad Carter, COV IT Infrastructure Partnership
V.	Vulnerability Assessment Program	Matt Slaight, COV IT Infrastructure Partnership
VI.	Cyber Security Awareness Toolkit	Bob Baskette, VITA
VII.	Commonwealth IT Security Policy & Standard	Cathie Brown, VITA
VIII.	Commonwealth Security Annual Report	Peggy Ward, VITA
IX.	Upcoming Events & Other Business	Peggy Ward, VITA

Virginia Joint Commission on Technology and Science

Lisa Wallmeyer, Executive Director

JCOTS

What is JCOTS?

- JCOTS is a permanent legislative commission, established by the General Assembly in 1997 to…

"…study all aspects of technology and science and endeavor to ***stimulate, encourage, promote, and assist*** in the development of technology and science in the Commonwealth and sound public policies related thereto…"

(§ 30-85 of the Code of Virginia)

Personally Identifiable Information Subcommittee

- Convened in 2007 Interim; continued in 2008 Interim
- A joint subcommittee of JCOTS and the Freedom of Information Advisory Council
- Develop policy regarding protection of personally identifiable information
  - Discussions turned to focus on over-collection of Social Security Numbers by government entities

Recommended Legislation

- HB 634/SB 132 – Adopted by the General Assembly

- Beginning July 1, 2009, no agency may require a person to furnish or disclose a social security number unless it is:
  - 1) Required by law (state or federal); AND
  - 2) Essential to the performance of that agency's duties

Recommended Legislation con't.

- The bill also requires each agency to conduct an analysis and review of its collection and use of social security numbers, and to report to FOIA/JCOTS by October 1, 2008.

- Elements for review:
  - 1) When are SSNs being collected?
  - 2) What is the purpose of the collection?
  - 3) Is the collection essential to the agency's functions?

Why is the agency survey necessary?

- Ensure a smooth transition on July 1, 2009
- Determine if additional legislation is necessary to authorize certain uses and collections
- Identify possible sources of over-collection that can be eliminated

Survey will not be used to criticize or make public current agency practices

JCOTS

Survey Information

Background materials and survey information can be found online at the FOIA & JCOTS websites:

http://jcots.state.va.us

http://dls.state.va.us/foiacouncil.htm

Contact Information

Lisa Wallmeyer, Executive Director, Joint Commission on Technology & Science

(804) 786-3591

jcots@leg.state.va.us

Maria Everett, Executive Director, Freedom of Information Advisory Council

(804) 225-3056 or (toll free) 1-866-448-4100

foiacouncil@leg.state.va.us

JCOTS

Elton Ghee

Roanoke County CISO

ROANOKE COUNTY 2000 TO ROANOKE COUNTY 2008 WITH INFOSEC

ROANOKE COUNTY 2000

- The 411 on RC
- Funding
- Staff
- 2010 Strategic Plan
- The Beginning of RC Infosec

ROANOKE COUNTY MID 2000S

- Incidents
  - Notebooks
  - Library
  - Va Tech
- PSB
  - PPEA
  - 911, Communications, & Digital Radio

OUR CHALLENGES

- Regionalization
  - Water Authority, Libraries, Regional Jail
- Digital Radio Network
- 911, GIS
- Constitutional Officers
- Other Entities
- Generation Y

ROANOKE COUNTY 2008 & INFOSEC

- Infosec
  - Jan 07
  - CISO
- Security Awareness
- Infosec Policies
- Auditing
- DR

ROANOKE COUNTY

- You are Welcome to God's Country Anytime!
  - RoanokeCountyVA.gov

eSupport Implementation

Information Security Officers' Advisory Group (ISOAG) Meeting

Presented by: Karen King

July 16, 2008

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

eSupport Introduction

Project Description	eSupport encompasses a wide range of online self-service tools intended to enable agency employees to research and resolve certain types of computing issues before contacting a VITA Help Desk representative.
Initial Functionality	eSupport will allow agency employees to: ▸ Reset passwords on the COV domain ▸ Submit a help desk ticket or check the status of an existing ticket online ▸ View customer service alerts (CSAs)/status for up-to-the-minute information on system problems within their agency ▸ Access the Knowledge Center, a document library for answers and solutions to common problems
Future Functionality	▸ Enhanced Help Desk support with the use of diagnostic tools for assistance ▸ Ability to fix common IT problems and complete common IT functions (i.e. deleting temporary folders to improve your computer's performance, using defrag to increase space on your hard drive, connecting via wireless, mapping a network drive) with a single click
Project Objectives	▸ Reduce the number of VITA help desk calls by allowing for agency employee self-service ▸ Provide agency employees with access to a self-help website 24/7 ▸ Improve the customer experience with IT support services

Agency Benefits from eSupport Solution

Agency Benefits
1. **Self-Service -> Greater Speed**: Agency employees will be able to reset their passwords on their own, eliminating time previously required to work through Help Desk calls 2. **Faster Ticket Submission**: Agency employees will be able to submit an online Help Desk ticket as soon as they identify an issue 3. **Greater Awareness of Status**: Agency employees will be able to check the status of a ticket online 24/7 4. **Better Service**: Help Desk personnel will be able to focus time on key issues because agency employees will be able to self-serve on several items 5. **Increased Knowledge**: Access to the Knowledge Center, support articles and FAQs will keep customers up-to-date on current problems and resolutions – Knowledge Center will continually be updated with new material

Virginia.gov Online Services | Commonwealth Sites | Help | Governor

Virginia Information Technologies Agency

eSupport

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

VITA Customer Care Center Phone Number 1-866-637-8482

eSupport Home | eSupport Survey | Useful Links

News

News Flash

- eSupport - Welcome to Self Service
- VITA - Emergency Preparedness Message from Doug McVicar June 9, 2008

Alerts & Outages

1. Resolved - VMFA - Richmond - Network Drives
2. Resolved - DMV - Norfolk - Circuit failure.
3. Resolved - DMV - Altavista - Circuit failure
4. Initial - VDACS - Richmond - Unable to access ditmvs2.state.va.us.
5. Resolved - DSS - Appomattox - Circuit Failure.

Top Solutions

Most Viewed Articles

1. eSupport - Welcome to Self Service
2. COVA - How to Report SPAM Email Messages for Filtering
3. AntiVirus - Virus information from US Department of Energy
4. BlackBerry 7520 - Typing Tips
5. NGC - Glimpse Box Issues on the Unisys Mainframe

Knowledge Center

Support Content

- Accounts and Passwords
- Hardware
- Network & Telecommunications
- News Flashes
- Resources
- Security
- Software
- Support Actions

Share Your Solution

The eSupport Team is looking for Subject Matter Experts to help us provide valuable knowledge to our Commonwealth of Virginia team. Please contact us if you are interested in helping.

Click here to share your solution

Web Ticketing

Create a Ticket

Check your Ticket

Network Password

Change your Password

Enter your question or problem below and click Search to begin:

Search

blackberry

SEARCH

Look within: All content

Search Results 1 - 5 of 37

Result Page **1** 2 3 4 5 6 7 8

Type	Article Title	Highlight	Relevance
	NGC - MTS Support Contacts *Support contacts for MTS (Mobile Technologies Services) for Northrop Grumman BlackBerry mobile devices, cell phones, pagers, calling cards, wireless modems, etc..*		97.07% More in this folder
	COVA - Unable to Send a BlackBerry Pin-To-Pin Message to Another BlackBerry *Cannot send a BlackBerry Pin-to-Pin message to another BlackBerry.*		97.07% More in this folder
	BlackBerry 7520 - Typing Tips *Users can facilitate typing on a BlackBerry 7520 with a variety of key shortcuts.*		97.07% More in this folder
	BlackBerry 7520 - How to Work with Attachments *Users can perform a variety of tasks with attachments in the BlackBerry 7520.*		97.07% More in this folder
	BlackBerry 7520 - How to Use the Web Browser *Use the Web browser in the BlackBerry 7520 to navigate the Internet anywhere.*		97.07% More in this folder

Result Page **1** 2 3 4 5 6 7 8

eSupport – Security Related Issues

- The internal eSupport site will only be available to users on the COV Domain and will contain all the aforementioned services. Because users of the external site will not have to authenticate to eSupport, we have removed the following services from the site:
  - List of critical outages impacting the Commonwealth
  - General Alerts and News Flashes
- The ability to submit and check the status of tickets require a Peregrine ESS account to ensure users only have access to tickets they have submitted
- Knowledge content available to users of eSupport is tied to their role (i.e. tech support vs. end-user). Therefore, only relevant and appropriate content will be accessible by end-users

VITA Vulnerability Assessment Program

(VAP)

Matt Slaight, Partnership Program Security Officer

16 JULY 2008

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

VAP Program

- Overview
- Defense in Depth Component
- Business case
- Objectives
- Process
- Technical description
- Schedule

Questions

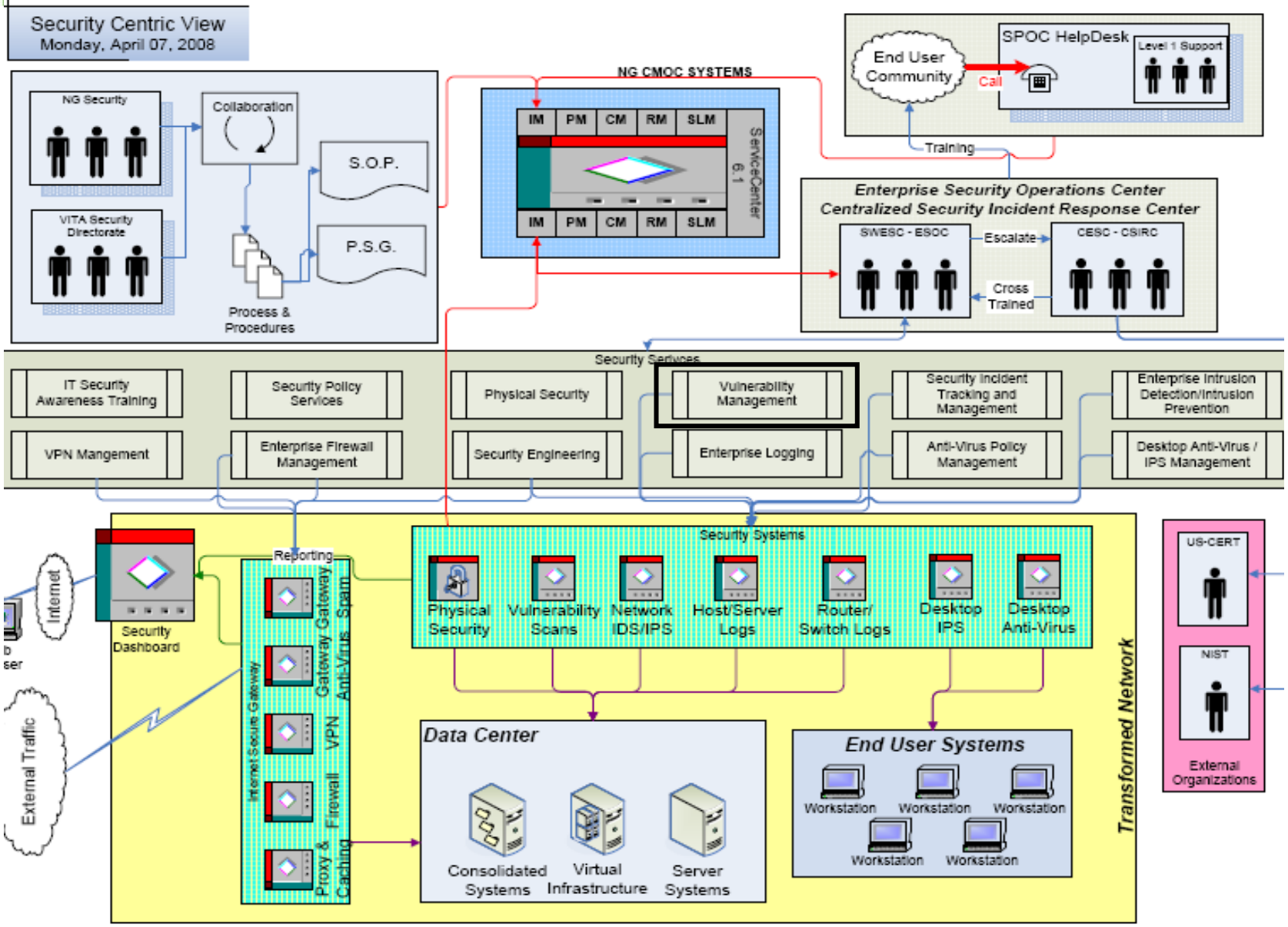
VAP Overview

- VAP is the partnership solution designed to proactively protect, detect and respond to cyber threats and vulnerabilities effecting the VITA managed infrastructure

- VAP is a COTS-based solution designed to perform assessments and report deficiencies in known vulnerabilities and to report compliance deviations to security policy configurations

- VAP is a core component of the overall “defense in depth” program designed to defend COV information assets

VAP & Defense in-depth



VAP Business Objectives

- Meet Commonwealth business and security requirements for reducing risk and maintaining compliance

- Reduce security incidents, improve security posture, and data management in the distributed environment

- Support business initiatives in accordance with applicable security standards

- Maintain the confidentiality, integrity and availability of Commonwealth Data

VAP Core processes

Vulnerability Assessment and Compliance Management is the systematic approach to accomplish the following:

- Scanning – the use of remote IT security tools to conduct scheduled automated background scanning/auditing to detect security holes (i.e., vulnerabilities) and check mandatory IT configurations for all transformed (i.e., “in-scope”) IT Partnership assets

- Analysis – the review and correlation of findings from all scanning and auditing activities to determine the security risk based on the IT security posture of vulnerabilities and non-compliant systems

- Reporting – the generation of tailored results for summary, trending, and detail analysis for IT Partnership personnel.

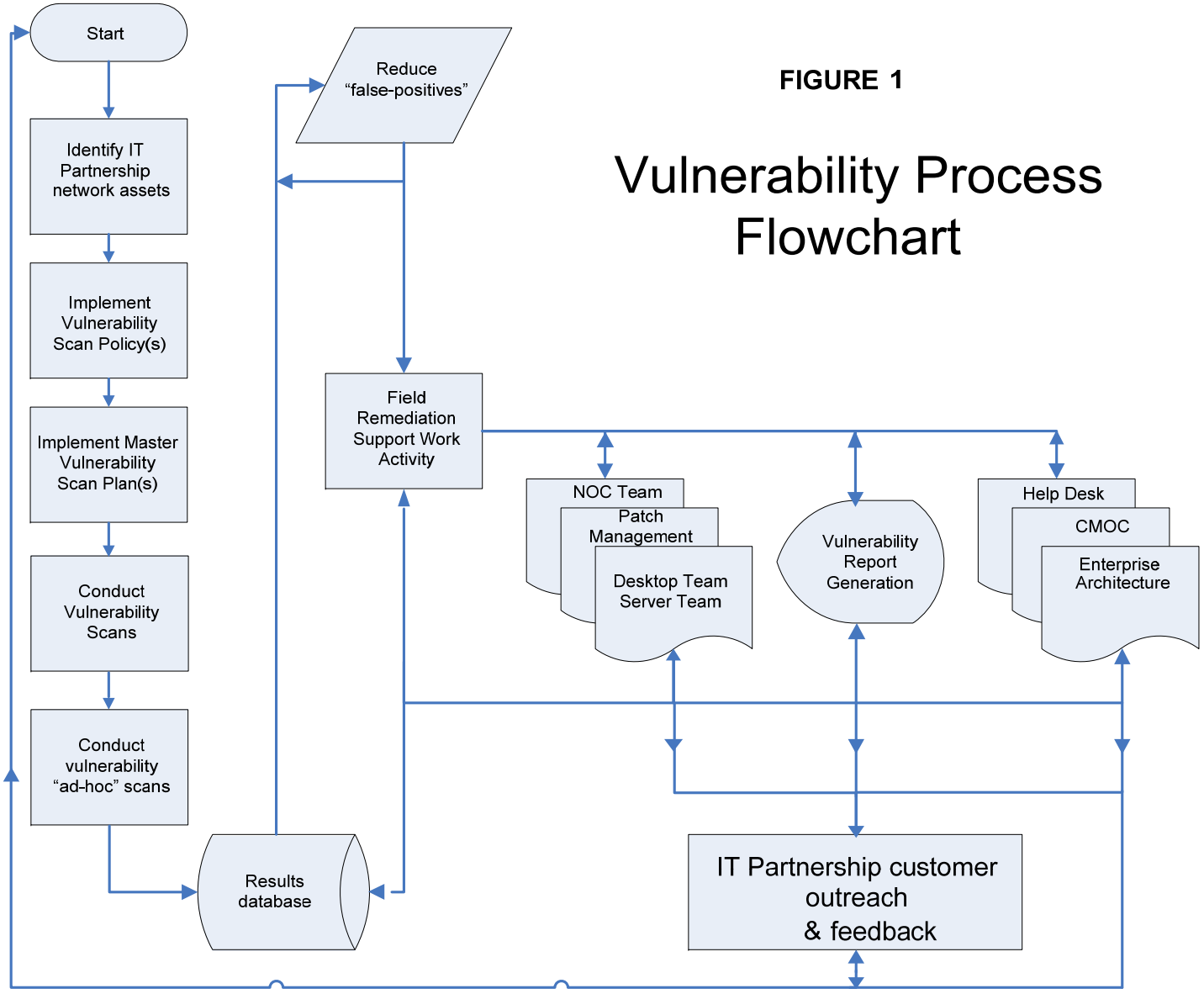
VAP operational procedures

- Scan all Transformed IT Partnership assets for vulnerabilities
- Scanning or auditing of all Transformed IT Partnership assets to ensure all workstations and servers comply with VITA security policy
- Conduct frequent periodic scans/audits
- Provide the IT Partnership with a daily “ad-hoc” scanning or auditing service support for timely remediation of vulnerability or compliance problems
- Perform false positive analysis of scan results for more accurate reporting
- Provide a report generation capability. Reports should contain summary and detailed results tailored to the appropriate field activity
- Operate all scanners securely so they do not open the network to penetration
- Customer Outreach & Feedback processes to improve efficiency and effectiveness of the Vulnerability Assessment Program (VAP)

VAP COTS Components

- **SiteProtector Application Server** - manages IDS\IPS solution components.
- **Site Protector Database** - stores all events and runs on MS SQL 2005.
- **SecureSync** - enables failover of SiteProtector and event collection.
- **Fusion Server** - estimates the network security attack impact and de-emphasizes failed attacks.
- **Agent Managers** - manages the various command and control activities, facilitates data transfer to Event Collectors, and accepts heartbeats.
- **Event Collectors** - gathers security data generated by an agent and directs the data to the SiteProtector Database.
- **Enterprise Scanner ESS1500** - The enterprise scanners will be configured to scan transformed network nodes in CESC, SWESC and in the Agencies for vulnerabilities and policy compliance.
- **Security Expressions** – is an Altiris product that will provide reporting on compliance to COV security policies

VAP Process flow



VAP schedule

- Weekly Vulnerability Scans of all Transformed subnets
- Bi-weekly IT Partnership Policy compliance scanning of desktops that reside in Transformed network segments.
- Monthly Summary Vulnerability and Compliance Reports will be shared with ISOs and VITA. These reports will posted on the PSO SharePoint Site as an interim solution until the Enterprise Security Dashboard is ready.
- Monthly detailed vulnerability and compliance reports will be sent to the service delivery team for action.
- “Ad Hoc” scans by request

In process

- Need to determine the optimum reporting process to provide ISOs scanning results
- Need to determine offline data retention period. Currently maintaining scan results on-line for 45 days

Summary

VAP

- Meets COV detect, defend, and respond objectives
- Integrated with “defense in depth” planning
- Uses state of the art technology and processes
- Some issues need resolution

QUESTIONS

Virginia Information Technologies Agency

Cyber Security Awareness Toolkit

Bob Baskette, CISSP, CCNP
Incident Management Engineer

Cyber Security starts with you

- To assist all agencies and localities in their efforts to increase Cyber Security Awareness in general and especially in October, the Virginia Information Technologies Agency has made a Cyber Security "Toolkit" available online. This Toolkit was produced by the Multi-State Information Sharing and Analysis Center (MS-ISAC) in collaboration with the U.S. Department of Homeland Security and the National Cyber Security Alliance as part of the National Cyber Security Awareness Month Campaign.

- The Toolkit is designed to help promote the delivery of a consistent cyber security awareness message and can become a cost efficient component of your Cyber Security Awareness Program. Instructions for printing and branding are also included.

- The Toolkit can be found at the following URL:
  http://www.vita.virginia.gov/security/default.aspx?id=5146

Toolkit Contents

- Citizen Awareness Banner
- Web Banner
- Bookmarks
- 2008 Cyber Security Awareness Calendar
- Cyber Bullying Brochure for Adults
- Cyber Security Brochure for Adults
- Posters

Citizens Awareness Banner

- Due to the ever increasing threats posed by malware running on citizen computers, a banner is provided for agencies to use on all Internet facing citizen and partner applications where authentication is required and personally identifiable information may be exchanged between the agency and your customers.

- HTML format for the banner

```
<h2>The security of your personal information is important to us!</h2>
<p>Diligent efforts are made to ensure the security of COV systems. Before you use this Web site to conduct business with the COV, please ensure your personal computer is not infected with malicious code that collects your personal information. This code is referred to as a <a title="keylogger" href="http://www.vita.virginia.gov/security/default.aspx?id=5344">keylogger</a>. The way to protect against this is to maintain current <a title="Anti-Virus" href="http://www.vita.virginia.gov/security/default.aspx?id=5344">Anti-Virus</a> and <a title="security patches" href="http://www.vita.virginia.gov/security/default.aspx?id=5344">security patches</a>.</p>

<p>For more information on protecting your personal information online, refer to <a title="Guide to Online Protection" href="http://www.vita.virginia.gov/security/default.aspx?id=5270">Guide to Online Protection</a>.</p>
<p><strong><a title="Online Protection Glossary" href="http://www.vita.virginia.gov/security/default.aspx?id=5344">Online Protection Glossary</a></strong></p>
```

Citizens Awareness Banner

Diligent efforts are made to ensure the security of Commonwealth of Virginia systems. Before you use this Web site to conduct business with the Commonwealth, please ensure your personal computer is not infected with malicious code that collects your personal information. This code is referred to as a keylogger. The way to protect against this is to maintain current Anti-Virus and security patches.

For more information on protecting your personal information online, refer to the Citizens Guide to Online Protection.

Online Protection Glossary

- **Keylogger =** Keystroke logging (often called keylogging) is a diagnostic tool used in software development that captures the user's keystrokes. Such systems are also highly useful for law enforcement and espionage—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures.

- **Anti-Virus =** Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware). Antivirus software typically uses two different techniques to accomplish this:
  - Examining files to look for known viruses matching definitions in a virus dictionary
  - Identifying suspicious behavior from any computer program which might indicate a malicious software infection.

- **Security patches =** If a patch is a piece of data used to update a software product, then a security patch is a change applied to an asset to correct the weakness described by a vulnerability. This corrective action will prevent successful exploitation and remove or mitigate a threat's capability to exploit a specific vulnerability in an asset. Security patches are the primary method of fixing security vulnerabilities in software.

- **Malware =** Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Citizens Guide to Online Protection

- Because only you can control the information you choose to release, you are the single best person to protect your personal information.
  - Keep anything with any personal or account information in a safe place
  - Only provide your information to trusted sources.
  - Always be skeptical when providing your personal information.
  - If you can't verify the legitimacy of the government entity, business or person requesting your information by calling the parent organization and verifying their contact with you, or if you don't understand why a certain piece of information is needed, do not provide it.

- Online Risks
  - E-mail and fraudulent Web sites
    - If you should ever receive an e-mail that appears to be suspicious, do not reply to it or click on the link it provides. Simply delete it. To report a suspicious e-mail that uses the Commonwealth of Virginia's name or the name of one of its agencies, you can forward it to VITAsecurityservices@vita.virginia.gov.
  - Malware
    - Spyware, viruses, worms and trojans are all malicious programs that are loaded onto your computer without your knowledge and commonly referred to as malware. Whether the goal of these programs is to capture or destroy information, to attack other computers or to swamp your computer with advertising, you don't want them.
    - Viruses and worms spread by infecting computers and then replicating. Spyware and trojans disguise themselves as a legitimate application and embed themselves into your computer, to monitor your activity, collect information and deliver it back to online criminals.

Web Banner

CYBER SECURITY AWARENESS MONTH
CYBER SECURITY
STARTS WITH "YOU"
Think Before You Click
Keep your software and operating system up-to-date.
Keep your data safe and secure.
Use hard-to-guess passwords.

Bookmarks

IS YOUR PC UP-TO-DATE?

New vulnerabilities and problems are found every day in programs and operating systems.

Most successful attacks on computer systems exploit known vulnerabilities.

Keep It Up-to-Date

- Install software and operating system patches so that attackers cannot take advantage of known problems or vulnerabilities.
- Take advantage of the many updated software programs and updates for operating systems.
- Check with your organization's policies and procedures before enabling automatic update options on your system.

Patch it to PROTECT IT!

DID YOU LOCK YOUR COMPUTER?

When you leave your computer unlocked, it is vulnerable to anyone's access. Someone using your computer with your log-on credentials can access all your files and documentation without you knowing.

Lock It When You Leave It

- Do you lock your car or house when you leave it? Of course you do, because your car, the place where you live, and the things inside are valuable to you.
- Do you lock your computer when you leave it? Your workstation or laptop may have valuable data on it — or your system account could provide access to confidential data.

Protect your information. DO YOUR PART!

Hi. I'M CYBER SECURE.

A cyber security program is only as strong as the people who implement it.

Do your part to protect yourself and others — protect your computer. Keep your firewall, anti-virus and anti-spyware programs up-to-date.

Be More Secure

- Install a firewall to protect your system against malicious network or Internet traffic.
- Install anti-virus software to protect your system against viruses, worms, Trojans, keyloggers, and other malicious programs.
- Install anti-spyware software to protect you against unwanted software that monitors your computer use or Internet behavior.

ARE YOU?

IS "PASSWORD" A GOOD PASSWORD?

No — It's not. Do your part to protect information in your care with hard-to-guess passwords.

Default passwords, names and dictionary words, even in other languages, can be guessed or cracked.

Create Strong Passwords

- Create passwords that are at least 8 characters long.
- Use a combination of upper and lower case letters, numbers, and special characters whenever possible.
- Use a passphrase to help you remember it.
- Don't use names of your family or friends.

BE CREATIVE!

Cyber Bullying Brochure for Adults

- The Cyber Bullying Brochure is a Parent's Guide to dealing with CyberBullies

- The brochure provides information on
  - What is a Cyberbully?
  - Who Are Cyberbullies?
  - Who Are the Victims of Cyberbullies?
  - Why Can Cyberbullying be Worse Than Physical Bullying?
  - Warning Signs that your Child may be a Victim of a Cyberbully
  - What to do if a Cyberbully Targets your Child

- Additional Sites for more Information About Cyberbullying
  - MS-ISAC: www.msisac.org/awareness/news/2007-01.cfm
  - Cyberbully.org: www.cyberbully.org
  - McGruff.org: www.mcgruff.org/advice/cyberbullies.php
  - Power in You: www.powerinyou.org/?id=MzI2
  - Bully Online: http://www.bullyonline.org/related/cyber.htm
  - Staying Safe Online: groups.msn.com/StayingSafeOnline/cyberbullies.msnw
  - National Crime Prevention Council:
  - www.ncpc.org/media/cyberbullying.php

- Brought to You By The Multi-State Information Sharing and Analysis Center

Cyber Security Brochure for Adults

- Guidelines for Information Security and Internet Usage

- The Internet has become a ubiquitous part of how we communicate. With the increasing volume and complexity of cyber security threats, we must understand what these threats are and how we can protect ourselves and the information in our care. By protecting yourself and the systems entrusted to you, you are protecting your co-workers, your entire organization's network and data and, ultimately, the citizens who are depending on you.

- Topics discussed in the Cyber Security Brochure
  - Use and Regularly Update Firewalls, Anti-virus, and Anti-spyware Programs
  - Install and Patch Operating Systems, Browsers, and Other Programs
  - Understand Passwords and Authentication
  - Lock Your Workstation and Laptop Whenever You Leave It
  - Backup Important Files Regularly
  - Be Cautious When Using the Internet
  - Be Cautious About Messaging Security - E-mail and Instant Messaging (IM)
  - Review Your Computer Security
  - Know How to Respond to a Cyber Incident
  - Remember that Cyber Security is Everyone's Responsibility

- Brought to You by the Multi-State Information Sharing and Analysis Center

MS-ISAC Posters

MS-ISAC Posters

Internet Safety Month - September

- September has been designated as Internet Safety Month by the Virginia General Assembly

http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HJ587

- United States Department of Justice has an on-line Internet Safety Program located at:

http://www.ojp.usdoj.gov/newsroom/events/internet_safety.htm

Cyber Security Awareness Month -OCTOBER

Governor Kaine has signed a proclamation designating October 2008 as Cyber Security Month – PLAN YOUR EVENTS NOW!

- The United States Department of Homeland Security National Cyber Security Division is sponsoring events during the month of October designed to increase awareness of the need to protect the nation's critical infrastructures and key resources from cyber threats and vulnerabilities

http://www.us-cert.gov/press_room/ncsamonth.html

Additional Cyber Security Awareness Resources

- The National Cyber Security Alliance provides simple, straight forward cyber security and safety resources to the public so that everyone will have the required knowledge to avoid cyber criminals

  http://www.staysafeonline.org/

- Project SafetyNet VA is a joint effort, led by Attorney General Bob McDonnell, to educate and elevate awareness among Virginia's children and parents about the dangers of the Internet through innovative initiatives. The Attorney General's Youth Internet Safety Advisory Committee meets regularly to implement these educational initiatives and is comprised of leaders representing education, law enforcement, parents, faith-based organizations and the technology industry

  http://www.oag.state.va.us/ProjectSafetyNetVA/index.html

Questions ???

For questions or more information, please contact VITA Security Services at:
VITASecurityServices@VITA.Virginia.Gov

Thank You!

Virginia Information Technologies Agency

Update on IT Security Policy, Standards & Guidelines

Cathie Brown, CISM, CISSP
Deputy Chief Information Security Officer

IT Security Policy (SEC 500-02 R.5)

- 30 Days on ORCA (5/30/08-6/30/08)
- 23 Comments Received
- Submitted to ITIB for Approval
- Publish in July, 2008

IT Security Standard (SEC 501-01 R.4)

- 30 Days on ORCA (6/01/08-7/01/08)
- 193 Comments Received
- Submitted to ITIB for Approval
- Publish in July, 2008

IT Systems Security Guideline (SEC 515-00)

- 30 Days on ORCA (5/13/08-6/10/08)
- 24 Comments Received
- Submitted to CIO for Approval
- Publish in July, 2008

Thank You For Your Comments!

- George Mason University
  - Kathy Adcock
  - Robert Nakles
- Department of Rehabilitative Services
  - Richard Benke
- Norfolk State University
  - Andrea Di Fabio
- Radford University
  - Monta Elkins
- Department of Medical Assistance Services
  - Theresa Fleming

Thank You For Your Comments!

- Department of Environmental Quality
  - Chandra Griffin
- Supreme Court of Virginia
  - David Hines
- Department of Motor Vehicles
  - Bevan Hurlbert
- Department of Juvenile Justice
  - Robert Jenkins

Thank You For Your Comments!

- Southwestern Virginia Mental Health Institute
  - Bracken Jones
- Department of Alcohol Beverage Control
  - James Lewis
- Virginia Retirement Services
  - Michael McDaniel
- Virginia Department of Transportation
  - Henry Moriconi
  - Thomas Wood

Thank You For Your Comments!

- Virginia Employment Commission
  - Christopher Nicholls
- Virginia Highlands Community College
  - Shannon O'Neill
- James Madison Univeristy
  - Darlene Quackenbush
- Thomas Nelson Community College
  - Catherine Szpindor
- Ronaoke County
  - Diane Wilson

Revisions

- Aligns with changes to the Code of Virginia for Data Breach Notification
- Documents additional and revised requirements
- Includes a new section for Application Security
- Eliminates exemption for academic and research systems

Scope & Compliance

- Revision: **Remove language in the scope section that excluded "Academic Instruction and Research" systems.**
  - Rationale: **All systems must be protected based on the sensitivity of the data rather than the type of system.**

- Revision: **Compliance date of January 1, 2009; except July 1, 2009 for systems previously excluded under Academic and Research.**
  - Rationale: **To provide sufficient amount of time to bring academic and research systems into compliance.**

Roles & Responsibilities

- Revision: **Agencies with multi-geographic locations or specialized business units should consider designating deputy ISOs as needed.**
  - Rationale: **Recommended as a best practice and implemented successfully in DMHRSAS.**

- Revision: **The ISO is not a System Owner or a Data Owner except in the case of compliance systems for IT Security.**
  - Rationale: **To recognize there are situations where it is appropriate for the ISO to own the system or data.**

IT System & Data Classification

- Revision: **Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Agency Head…**
  - Rationale: **To clarify that there is information classified as sensitive with respect to availability or integrity that is appropriate for posting on a publicly accessible medium.**

Application Security

- Revision: **New Application security requirements define the high level specifications for securely developing and deploying Commonwealth applications.**
  - Rationale: **Due to the increase in attacks against application vulnerabilities, this section has been added to enhance security for applications.**

Logical Access Control

- Revision: **Users are accountable for any activity on the system performed with the use of their account.**
  - Rationale: **To impress upon users they are responsible and should protect their credentials.**

- Revision: **Prohibit the use of guest and shared accounts on sensitive IT systems.**
  - Rationale: **Recognize there are systems without sensitive data where guest and shared accounts may be valid.**

Logical Access Control

- Revision: **Prohibit the displaying of user's last name in the logon screen.**
  - Rationale: **Recommended as best practice and in accordance with Center for Internet Security configuration standards.**

- Revision: **Configure applications to clear cached data and temporary files upon exit of the application or logoff of the system.**
  - Rationale: **To protect against the use of cached credentials to allow unauthorized access.**

Password Management

- Revision: **Require passwords on mobile devices issued by the agency such as PDA's and smart phones.**
  - Rationale: **To recognize the need to better protect data on mobile devices.**

- Revision: **Require the users of sensitive IT systems, to include network systems, to change their passwords after a period of 42 days.**
  - Rationale: **To maintain consistency with Center for Internet Security configuration standards.**

Data Storage Media Protection

- Revision: **Prohibit the connection of any non-COV owned data storage media or device to a COV-owned network, unless the connection is to a segmented guest network. This prohibition is at the agency's discretion and need not apply to an approved vendor providing operational IT support services under contract.**
  - Rationale: **To protect the COV-owned network while acknowledging the needs of access by personal devices to a guest network and IT support service via a vendor.**

Data Storage Media Protection

- Revision: **Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case… approved by the Agency Head.**
  - Rationale: **To protect information in agency email from being stored in an external email system, while recognizing there may be a valid need to forward email internally between accounts.**

Data Storage Media Protection

- Revision: **Procedures to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered… where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.**
  - Rationale: **To protect against the potential for data leakage due to lost or stolen backup tapes.**

Personnel Security

- Revision: **Temporarily disable physical and logical access rights when personnel are not working for a prolonged period in excess of 30 days due to leave, disability or other authorized purpose.**
- Revision: **Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.**
  - Rationale: **To limit the potential for unauthorized access.**

Email Communications

- Revision: **Email shall not be used to send sensitive data unless there is encryption… The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.**
  - Rationale: **To address the use of email disclaimers.**

Data Breach Notification

- Revision: **Clarification of terms (Personal Information and redacted) and requirements have been revised in order to align with the Code of Virginia §18.2-186.6**.
  - Rationale: **To maintain consistency with the Code of Virginia.**

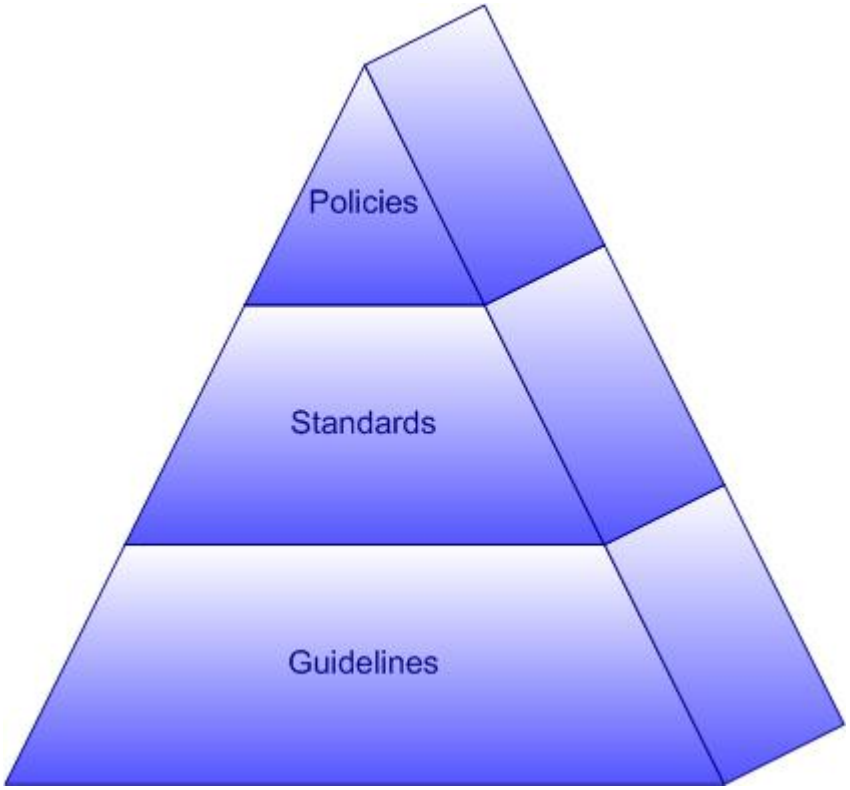
Data Breach Notification

- Revision: **In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to section E of Code of Virginia §18.2-186.6, the individual or entity shall notify without reasonable delay, the Office of the Attorney General and all consumer reporting agencies…**
  - Rationale: **To align with requirements in the Code of Virginia.**

Other Revisions Included

- Business Impact Analysis
- IT System and Data Classification
- IT System and Data Backup and Restoration
- Malicious Code Protection
- Password Management
- IT Security Incident Handling
- Glossary

?Questions?



Thank you!

Virginia Information Technologies Agency

Commonwealth Security Annual Report

Peggy Ward
Chief Information Security and Internal Audit Officer

Information Security Report

§ 2.2-2009. (Effective until July 1, 2008) Additional duties of the CIO relating to security of government information.

C. The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.

Secretariat: Finance

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DOA	NO	YES	YES	ADEQUATE	YES	NO
DPB	Extension Expired	Yes	YES	INADEQUATE	YES/UPD	NO
TRS	YES	YES	NO	ADEQUATE	YES	NO
TAX	YES	YES	YES	INADEQUATE	YES	YES

Secretariat: Administration

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
SCB	YES	NO	NO	INADEQUATE	YES	NO
CHR	NO	YES	NO	NOT SURVEYED	YES	NO
SBE	YES	NO	YES	INADQUATE	YES	NO
EDR	YES	YES	YES	NO PROGRAM	YES/UPD	NO
DGS	YES	YES	NO	ADEQUATE	YES	NO
DHRM	YES	YES	NO	INADEQUATE	YES/UPD	NO
DMBE	NO	YES	YES	NO PROGRAM	YES	NO

Virginia Information Technologies Agency

Secretariat: Commerce & Trade

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
BOA	YES	YES	YES	INADEQUATE	YES	NO
DBA	NO	YES	YES	INADEQUATE	YES	NO
VEDP/VTA	NO	YES	NO	INADEQUATE	YES	NO
VEC	YES	YES	YES	INADEQUATE	YES/UPD	NO
DHCD	YES	YES	NO	INADEQUATE	YES	NO
DOLI	NO	YES	YES	INADEQUATE	YES	NO
DMME	YES	YES	YES	INADEQUATE	YES	YES
DPOR	YES	YES	YES	INADEQUATE	YES	NO
VRC	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
VRA	NO	NO	NO	NOT SURVEYED	NA	NO
VNDIA	NO	NO	NO	NOT SURVEYED	NA	NO
VHDA	NO	NO	NO	NOT SURVEYED	NA	NO
TIC	NO	NO	NO	NOT SURVEYED	NA	NO

Secretariat: Health & Human Resources

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
VDA	YES	YES	YES	NO PROGRAM	YES	NO
DHP	YES	YES	NO	ADEQUATE	YES	NO
VDH	YES	YES	YES	INADEQUATE	YES	YES
DMAS	YES	YES	YES	INADEQUATE	YES	NO
DMHMRSAS (CBR)	YES	YES	YES	INADEQUATE	YES	NO
DRS (VBPD, VDBVI, VDDHH, WWRC)	YES	YES	NO	ADEQUATE	YES	NO
DSS (CSARYF)	YES	YES	YES	INADEQUATE	YES/UPD	NO
TSF	NO	NO	NO	NOT SURVEYED	NO	NO

Secretariat: Education (excluding Higher Ed)

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DOE	YES	YES	NO	INADEQUATE	YES	NO
FCMV	NO	YES	NO	NO PROGRAM	NO	NO
GH	NO	YES	NO	NO PROGRAM	NO	NO
SCHEV	EXTENSION EXPIRED	YES	NO	INADEQUATE	YES	NO
JYF	YES	YES	YES	INADEQUATE	YES	NO
LVA	YES	YES	YES	INADEQUATE	YES	NO
VMFA	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
SMV	NO	YES	NO	INADEQUATE	YES	NO
VCA	NO	NO	NO	INADEQUATE	YES	NO

Secretariat: Education (Higher Ed only)

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
CNU	YES	YES	NO	ADEQUATE	NA	N/A
VMI	YES	YES	NO	ADEQUATE	NA	N/A
VCCS	YES	YES	NO	ADEQUATE	NA	YES
GMU	YES	YES	YES	INADEQUATE	NA	YES
JMU	YES	YES	NO	ADEQUATE	NA	YES
LU	YES	YES	YES	INADEQUATE	NA	YES
NSU	NO	YES	NO	INADEQUATE	NA	NO
ODU	YES	YES	YES	INADEQUATE	NA	YES
RU	YES	YES	NO	INADEQUATE	NA	YES
VSU	YES	YES	YES	INADEQUATE	NA	NO
UMW	YES	YES	YES	INADEQUATE	NA	NO

Secretariat: Agriculture & Forestry

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
VADACS (DCG)	YES	YES	YES	NO PROGRAM	YES	NO
DOF	YES	YES	YES	INADEQUATE	YES	N/A

Secretariat: Natural Resources

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DCR	YES	YES	YES	INADEQUATE	YES	NO
DEQ	YES	YES	YES	INADEQUATE	YES	YES
DGIF	NO	YES	YES	INADEQUATE	YES	NO
DHR	YES	YES	YES	INADEQUATE	YES	NO
MRC	YES	YES	YES	INADEQUATE	YES/UPD	NO
VMNH	NO	YES	NO	INADEQUATE	YES	NO

Secretariat: Transportation

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
DOAV	NO	YES	YES	INADEQUATE	YES	NO
MVDB	NO	YES	NO	INADEQUATE	YES	NO
DMV	YES	YES	YES	INADEQUATE	YES	NO
DRPT	YES	YES	YES	INADEQUATE	YES	NO
VDOT	YES	YES	YES	INADEQUATE	YES	YES

Secretariat: Technology

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
CIT	YES	YES	YES	Adequate	YES	NO
VITA	YES	YES	YES	Adequate	YES	YES

Secretariat: Public Safety

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
ABC	YES	YES	YES	INADEQUATE	YES	YES
CASC	NO	NO	NO	NO PROGRAM	NO	NO
DOCE	NO	YES	NO	INADEQUATE	YES	NO
DOC	YES	YES	YES	ADEQUATE	YES	NO
DCJS	YES	YES	NO	INADEQUATE	YES	NO
DFS	YES	YES	YES	NO PROGRAM	N/A	N/A
VDEM	NO	YES	YES	INADEQUATE	YES	NO
DFP	NO	YES	YES	INADEQUATE	NO	NO
DJJ	YES	YES	YES	INADEQUATE	YES	NO
DMA	NO	NO	NO	INADEQUATE	YES	NO
VSP	YES	YES	YES	INADEQUATE	YES	N/A
DVS	NO	YES	NO	NO PROGRAM	YES	NO

Other

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
GOV	Extension Expired	YES	NO	INADEQUATE	YES	NO
OAG	NO	YES	YES	INADEQUATE	NA	NO

Independent Agencies

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DRP Plan Rec'd	CAP's Rec'd
VCSP	NO	NO	NO	ADEQUATE	N/A	NO
LOTTERY	NO	YES	YES	INADEQUATE	N/A	NO
VRS	NO	YES	YES	ADEQUATE	N/A	NO
SCC	NO	YES	YES	NO PROGRAM	N/A	NO
VOPA	NO	NO	NO	NO PROGRAM	N/A	NO
IDC	NO	YES	YES	NO PROGRAM	N/A	NO
VWCC	NO	NO	NO	INADEQUATE	N/A	NO

Questions?

Upcoming Events

UPCOMING EVENTS

IS Orientation

Wednesday, July 30th, 1 to 3:30 pm @ CESC
Thursday, August 14th, 9:30 am to 12:00 pm @ CESC

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

To register email VITASecurityService@VITA.Virginia.gov

UPCOMING EVENTS!

NEXT ISOAG MEETING!

August 20th, 1:00 – 4:00 pm

- Monitoring Acceptable Use of the Internet In The COV – Jim Austin, VDOT
- Altiris – Longwood University (Invited)

@ CESC

UPCOMING EVENTS

Commonwealth Information Security Council Meeting

Monday, July 21, 12:00 - 2:00 p.m. @ CESC with Committee meetings from 2:00 - 3:30 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 VITASecurityServices@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

CIO – CIA Communication Exchange

Tuesday, July 22, 9 – 11:30 am

VDOT Auditorium, 1221 E Broad ST

UPCOMING EVENTS

COVITS 2008

Commonwealth of Virginia Innovative Technology Symposium

September 7 – 9, 2008
Williamsburg Marriott

Early Bird Registration ends August 8th, 2008

Don't miss this opportunity to see the latest in digital government solutions, keep abreast of current policy issues and network with key government executives, technologists and industry specialists.

www.govtech.com/events/COVITS2008

Any Other Business ??????

ADJOURN

THANK YOU FOR ATTENDING!!