Virginia Information Technologies Agency

Commonwealth Collaboration

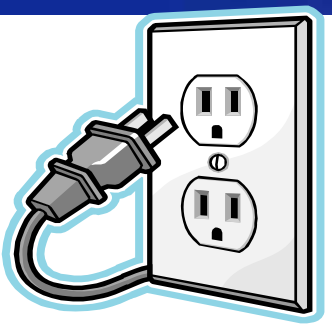
Peggy Ward,
Chief Information Security Officer
of the Commonwealth of Virginia

FISSEA 2008 Conference
Security through Innovation and Collaboration

Information Security – WHY?

- Increasing dependency on technology for daily living in both our personal and professional lives!
- More and more Internet activity: government services, employment, shopping, banking, real estate, friends!
- Good Business is Secure Business!

Information Security – WHY?



The most secure computer is one that is unplugged!

But unplugging will not help the work get done and besides, it creates unhappy users!

There is constant balancing act between speed / ease and security

Information Security – WHY?

!Threats!

Honeynet Statistics for 2/21 – 2/27 2008

- **1,145 Unique Infected Computers Seen**
- **500,696 Attacks from 1,145 Computers**
- **113 of Unique Pieces of Malware Collected**
- **56 Countries of Origination**

Information Security – WHY?

Why Information Security?

1. Approximately how many computers on the Internet are infected with spyware?

   a. 25%
   b. 45%
   c. 60%
   d. 80%

2. What is the single best thing you can do to protect your computer against spyware?

   a. Disable Active-X in Internet Explorer
   b. Protect your computer with a firewall
   c. Install anti-spyware and keep it updated
   d. Only browse websites that you know & trust

From SANS Institute Security Newsletter for Computer Users

Information Security – WHY?

1. d. While expert opinions vary, most sources agree that 80% is a reliable estimate for how many computers connected to the internet are infected with spyware.

2. c. Anti-spyware is as important as antivirus software for protecting your computer.

From SANS Institute Security Newsletter for Computer Users

What to Do?

!Collaborate!

Collaboration allows us to leverage our ideas, knowledge and resources to strengthen the information security posture of the Commonwealth of Virginia and nationally as well!

Commonwealth Collaborations

Three Collaboration Spheres

- Top Down Collaboration
- Internal Commonwealth Collaboration
- External Information Security Collaboration

Top Down Collaboration – General Assembly

The General Assembly provides a legislative foundation!

In addition to dependency on Information Technology in our personal and professional lives, there are also the General Assembly Legislative requirements codified in the Code of Virginia to motivate us!

Top Down Collaboration – General Assembly

§ 2.2-603.F Authority of agency directors.

The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.

Top Down Collaboration – General Assembly

§ 2.2-2009 Additional duties of the CIO relating to security of government information

A. develop policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information.

B. develop policies, procedures, and standards that shall address the scope of security audits and the frequency of such security audits.

Top Down Collaboration – General Assembly

§ 2.2-2009 Additional duties of the CIO relating to security of government information

C. 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.

F. promptly receive reports from directors of departments in the executive branch of state government made in accordance with § 2.2-603 and shall take such actions as are necessary, convenient or desirable to ensure the security of the Commonwealth's electronic information.

Top Down Collaboration – Governor

Governor's Executive Order 43 (2007)- *Protecting the Security of Sensitive Individual Information in Executive Branch Operations*

"…I hereby empower the Secretary of Technology to coordinate and oversee all efforts within the executive branch, in every secretariat, agency, institution, board, commission, and other entity to ensure compliance with established Commonwealth Information Security Policies and Standards so that protection of sensitive individual information is appropriate and that privacy is respected to the maximum extent possible."

Governor's Proclamation

Governor Kaine issued a proclamation designating October 2007 as Cyber Security Awareness Month

Top Down Collaboration – APA

Auditor of Public Accounts (APA) issued the report:

Review of Information Security In The Commonwealth of Virginia as of December 1, 2006

as required by Senate Joint Resolution 51 (SJR 51)

http://www.apa.virginia.gov/reports/SJR06.pdf

Top Down Collaboration – APA

- Senate Joint Resolution No. 51 was passed by the 2006 General Assembly.
- Directed the Auditor of Public Accounts to report on the adequacy of the security of state government databases and data communications from unauthorized uses.
- The report, published 12/01/2006, summarized the current state of information security programs implemented at state agencies including institutions of higher education in the Commonwealth of Virginia.

Top Down Collaboration – APA

Criteria Used

- **Best Practices as defined by:**
  - ISO (International Standards Organization)
  - NIST (National Institute of Standards and Technology)
  - ISACA (Information Systems Audit and Control Association)
  - COBIT (Control Objectives for Information and Related Technologies)
  - (GAO) US Government Accountability Office
- **COV IT Information Security Policy (SEC500-02) and Standard (SEC501-01)**

Top Down Collaboration – APA

Results December 2006

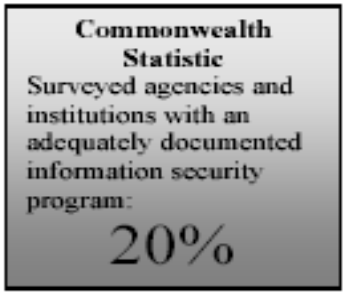
" The information security programs in the agencies and institutions of the Commonwealth are generally inadequate and do not address the business needs to adequately control information as well as risks associated with not controlling information."

104 agencies and institutions reviewed

- **17% had no information security program**
- **63% had inadequately documented programs**

= 80% !

- **20% had adequately documented programs**



Top Down Collaboration – APA

- **Recommendation #1:**

  VITA develop a plan to communicate infrastructure information and standards to agencies and provide assistance to agencies as they develop there IS programs.

- **Recommendation #2:**

  The General Assembly may wish to consider granting the CIO authority over the other branches of government's information security programs.

Top Down Collaboration – APA

- **Recommendation #3:**

  The CIO and ITIB should consider supplementing the COV SEC501-01 Standard with the additional processes identified in the report.

- **Recommendation #4:**

  In order to create proper information security plan, agencies require sufficient resources with appropriate expertise to develop such a plan. Using a centralized entity, such as VITA, to help allows the COV to leverage its cost and resources with information security expertise to assist agencies, especially small to medium-sized agencies.

Top Down Collaboration – CIO & CISO

The Chief Information Officer (CIO) of the Commonwealth has designated the Chief Information Security Officer (CISO) of the Commonwealth to develop the Commonwealth Information Security Policies, Standards and Guidelines (PSG) for his review and approval and that of the Information Technology Investment Board.

Top Down Collaboration – CIO & CISO

PSG Development and Implementation

Each PSG, as developed or revised, is vetted with the Commonwealth Information Security Council and then placed on the Online Review and Comment Application for 30 days allowing all interested parties to comment and provide suggested revisions. A response is prepared for each comment received.

Where additional plans or actions are needed by the Commonwealth Information Security Community, the compliance date is placed 6 -12 months in the future.

Top Down Collaboration – CIO & CISO

Commonwealth Information Security Policy & Standards
http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs

Information Security Policy
IT Security Policy (SEC500-02) (07/19/2007)

Information Security Standards

IT Security Standard (SEC501-01) 7/01/2007

IT Security Audit Standard (SEC502-00) 7/01/2006

Use of Non-Commonwealth Computing Devices to Telework (SEC511-00) 7/01/2007

Data Removal from State Electronic Equipment Standard (SEC2003-02.1) 3/08/2004 (New Version March 2008!)

Top Down Collaboration – CIO & CISO

COV Information Security Guidelines

Contingency Planning Guideline (SEC508-00) 4/18/07

Data Protection Guideline (SEC507-00) 7/02/07

Internet Privacy Guidelines (SEC2001-02.1) 2/27/2001

IT Security Threat Management Guideline (SEC510-00) 7/01/2007

Logical Access Control Guideline (SEC509-00) 4/18/07

Risk Management Guideline (SEC506-01) 12/11/2006

Risk Assessment Instructions- Appendix D (SEC506-01) 12/14/2006

Top Down Collaboration – CIO & CISO

COV Information Security Templates

Corrective Action Plan Template

Exception Request Form - COV IT Security Policy and Standard

Interoperability Security Agreement Template

IT Security Audit Plan Template

Risk Assessment Report Template

Security Roles and Responsibilities Template

System Inventory and Definition Template

Internal Commonwealth Collaboration

Examples:

- Commonwealth Information Security Council
- Commonwealth Information Officers Advisory Group
- Information Security Officer's Orientation
- Cyber Security Tools

Internal Commonwealth Collaboration – IS Council

Commonwealth Information Security Council

Formed: April, 2007

Eleven Information Security Officers have come together to strengthen the information security posture of the Commonwealth.

Visit their website at

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

Internal Commonwealth Collaboration – IS Council

The Council has formed committees around the following four initiatives and others have volunteered to assist them:

- Encryption
- Identity and Access Management
- Making Information Security an Executive Management Priority
- Small Agency Outreach

All branches of State Government are represented by the membership. Meetings are monthly or more frequently as needed.

Internal Commonwealth Collaboration – IS Council

A Few Accomplishments:

- Published weekly information security articles for Executives during Cyber Security Month, October, 2007 in the *Leadership Communiqué* – the Agency Heads e-newsletter from the Governor's office.
- Had a Cyber Security Article Published in Capitol Connections Magazine featuring the Secretary and Deputy Secretary of Technology as well as the CISO.
- Finalized a Business Impact Analysis Template and Tools and provided to the Virginia Department of Emergency Management for optional use in Continuity Planning across the Commonwealth
- Surveyed the Information Security Community to focus efforts and are formulating target plans to address stated issues and opportunities.

Internal Commonwealth Collaboration – IS Council

A Few More Accomplishments:

- Drafted a Commonwealth of Virginia Identity and Access Management Trust Model
- Provided input on Data Breach Notification Requirements & Early Adoption
- Developing a Non Disclosure Agreement term and condition for statewide use in contracts
- Developing a Secure Communication Portal for the Information Security Community

Internal Commonwealth Collaboration – ISOAG

Information Security Officers Advisory Group (ISOAG)

Who?

Open to all government personnel interested in information security in the Commonwealth. Currently 256 persons have joined from the judicial, legislative and executive branches of state government as well as independent agencies and localities!

Internal Commonwealth Collaboration – ISOAG

What?

- Analysis of Threats & Software Updates
- Training Opportunities
- Monthly Cyber Security Tips customized for Virginia
- Topical updates such as changes to PCI
- Invitation to the monthly ISOAG meetings

How? Send an email with your contact information to VITASecurityServices@VITA.Virginia.Gov

Internal Commonwealth Collaboration – ISOAG

Monthly Meetings Summary

	FY 08* (7/07 – 2/08)	FY 07 (7/06 – 6/07)
# of attendees	621	604
# of Mtgs	9	8
Avge # attendees	77.6	67

* Still in progress; YTD

Information from past meetings is available at
http://www.vita.virginia.gov/security/default.aspx?id=323

Internal Commonwealth Collaboration – ISOAG

March's Meeting: March 19, 1:00 pm – 4:00 pm CESC Chester, Virginia

- FRAC/FIPS 501 - Mike McAllister, Office of Commonwealth Preparedness
- Web Enterprise Initiatives - Gov's Office (INVITED)
- Commonwealth Information Security Council Information Security Survey – COV IS Council
- CAM/APM Roles - Debbie Secor & Mike Melton (INVITED)
- Compliance Management Tool - Benny Ambler, VITA
- Commonwealth Information Security Annual Report - Cathie Brown, VITA
- Information Security Audit Language - Cathie Brown, VITA
- Web App Hacking Demo - Tripp Sims, VITA
- 2008 Legislation Related to Security - Peggy Ward, VITA

Internal Commonwealth Collaboration – ISO Orientation

What?

Small group overview of the IT Security Program in the Commonwealth focusing on the Commonwealth Collaboration Opportunities as well as the COV IT Security Policy, Standards and Guidelines!

Who?

All Commonwealth ISO's, back-up ISO's, IT Auditors and interested IT persons!

When?

Monthly!

How?

Send an email expressing interest to: **VITASecurityServices@VITA.Virginia.Gov**

Internal Commonwealth Collaboration – ISO Orientation

Started: March 27, 2007

As of February, 2008 we have had 84 persons attend representing 50 organizations including all branches of State government as well as local government.

Internal Commonwealth Collaboration – Cyber Security Tools

Web Based Cyber Security Tools from many sources!

Toolkit

Located at: http://www.vita.virginia.gov/security/default.aspx?id=5146

Contents:

1. Citizen's Awareness Banner

Due to the ever increasing threats posed by malware running on citizen computers, it is suggested that Commonwealth government entities utilize the "Citizen's Awareness Banner" on all Internet facing citizen & partner applications where authentication is required, or where any personally identifiable information may be exchanged between the agency & your customers.

More Content in the Toolkit!

2. Citizen's Guide to On-Line Protection

The Guide to Online Protection' includes: Glossary of terminologies, Links to Anti-Virus, Anti-Spyware, & Firewall guides, Secure computing practices & more! The Guide is easily maintained & will continue to be developed with more content as the security landscape changes & new threats & defenses come to light.

Internal Commonwealth Collaboration – Cyber Security Tools

and some more….

3. Cyber Security web banner

4. Security Awareness Posters, bookmarks, etc. (MS-ISAC) that can be printed and used for end user awareness

5. Videos and other materials around "Faux Paws" the Techno Cat for children's internet safety courtesy of Commonwealth Information Security Council member, Aaron Mathes, Office of the Attorney General

Internal Commonwealth Collaboration – Cyber Security Tools

Monthly Cyber Security Awareness Tips

The Commonwealth in concert with the Multi-State Information Sharing & Analysis Center provides a monthly newsletter featuring cyber security awareness information targeted at the end user. The newsletter provides security awareness information for everyone to use both at work and at home to will find valuable in protecting against cyber attacks. It is provided via the web but also in word to the persons on the ISOAG list so they can brand and customize it if they choose.

http://www.vita.virginia.gov/communications/publications/cybersecuritytips/default.aspx?id=117

Internal Commonwealth Collaboration – Cyber Security Tools

Web based Incident Reporting!

Report information technology security incidents to the Chief Information Officer of the Commonwealth as required by Code of Virginia §2.2-603.F "Authority of agency directors" at https://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm

Reporting allows the Commonwealth to have a holistic picture of the Commonwealth's information security posture including issuing alerts.

Guidance on what to report is provided at: https://www.vita.virginia.gov/security/default.aspx?id=317

External Commonwealth Collaboration

Examples:

- **InfraGard**
- **Multi State – Information Sharing & Analysis Center (MS-ISAC)**
- **Information Risk Executive Council (IREC)**
- **Public Private Partnership with Northrop Grumman (NG)**

External Commonwealth Collaboration -InfraGard

InfraGard

http://www.infragard.net/

The Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996 as a local effort to gain support from the IT industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

External Commonwealth Collaboration – MS-ISAC

MS-ISAC

http://www.msisac.org/

The Multi State – Information Security Analysis Center (MS-ISAC) is a voluntary & collaborative organization with participation from all 50 states & the District of Columbia. The mission of the MS-ISAC, consistent with the objectives of the National Strategy to Secure Cyberspace, is to provide a common mechanism for raising the level of cyber security readiness & response in each state & with local government as well as for gathering information on cyber threats to critical infrastructure & providing two-way sharing of information between & among the states & local governments. The U.S. Department of Homeland Security has officially recognized the MS-ISAC as the national center for the states to coordinate cyber readiness & response.

External Commonwealth Collaboration – IREC

IREC

We have a Commonwealth-wide membership with the Information Risk Executive Council (IREC) that allows every Commonwealth of Virginia state and local government employee interested in Information Security to register and be a member! The tools & papers include those around topics such as Information Security Awareness, Identity & Access Management, Information Protection & more!

External Commonwealth Collaboration – NG

Problem: Virginia had an aging, inefficient infrastructure and numerous operational security risks

- 90+ autonomous IT shops
- 60% of equipment 8 to 10 years old
- Unacceptable risk for hacking & security incidents
- Virginia's data center building rated a security risk

External Commonwealth Collaboration – NG

Solution: Virginia established the nation's largest state government public-private partnership to modernize and secure the IT infrastructure

- Created November 2005 with Northrop Grumman Corporation
- Valued at $1.9 billion over 10 years
- Included $270 million up-front capital investment, job creation and modernization initiatives
- Includes desktop and print, help desk, e-mail, security, network, mainframe and server, as well as facilities

External Commonwealth Collaboration – NG

IT Infrastructure Partnership benefits

Service Commencement Date: July 1, 2006

- Standardized security architecture
- Enterprise Security Operations Center – central monitoring and management
- New, modern data center facility with operational redundancy and hardened security
- Dedicated disaster recovery facility – Lebanon, Va.

External Commonwealth Collaboration – NG

IT Infrastructure Partnership benefits

- Single, statewide network and Internet Secure Gateway
- Standard, consistent use of security tools and policies across infrastructure and PCs (firewalls, admin. rights, encryption, anti-virus, etc.)
- Standard infrastructure support and planned refresh
- Strengthened security of IT assets and Commonwealth data

Contact Information

Peggy Ward
Chief Information Security & Internal Audit Officer
Commonwealth of Virginia
Virginia Information Technologies Agency

Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, Virginia 23836

804.416.6014 Voice
804.416.6359 Facsimile
Peggy.Ward@VITA.Virginia.Gov

http://www.vita.virginia.gov/security/