



Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

April 8, 2008

April Showers



Bring



May
Flowers!





ISOAG April 2008 Agenda

- | | | |
|-------|---|---|
| I. | Welcome and Opening Remarks | Peggy Ward, (VITA) |
| II. | Messaging In Transformation | Don Drew, (COV IT Infrastructure Partnership) |
| III. | Virginia Interactive Services & Security | Lynn DuBard, (Virginia Interactive) |
| IV. | COV IS Council 1 Year Report | Marie Greenberg, (SCC)/John Willinger, (DMHMRSAS) |
| V. | Commonwealth Annual Report Data Points | Ed Miller, (VITA) |
| VI. | COV IT Security Policy & Standard Exception Process | Cathie Brown, (VITA) |
| VII. | Web Security | Michael Watson, (VITA) |
| VIII. | Roles and Responsibilities Sec 501 | Peggy Ward, (VITA) |



Messaging Encryption

April 8, 2008



NORTHROP GRUMMAN

Messaging Encryption

What is the solution?

- The encryption solution for the new Enterprise Messaging System is an internal Public Key Infrastructure (PKI).
- Encryption requires certificates from either a private or public source. Our solution is to provide them from an internal private source.
- We are using the Microsoft Active Directory integrated PKI.
- The purpose of this solution is to enable the sending of encrypted messages to internal and external users on an as needed basis.

Messaging Encryption

Who can use it?

- Anyone who is a member of the COV domain and can log on the COV domain is eligible to use the Enterprise Messaging Encryption solution.
- Windows XP and Outlook 2003 workstations are required to use this solution.
- Outlook Web Access users also are able to send encrypted mail.

Messaging Encryption

How do you use it?

- There is an internal website that can be accessed once you have logged into the COV Domain.
- The user will request a certificate and then will download the certificate following the instructions provided on the website.
- When the certificate is downloaded on your workstation, you are now able to send encrypted mail
- For every person that a user wants to send encrypted mail to, they will have to send the recipient their public key. Each user has a specific public key that is used for every recipient that they want to encrypted mail to.
- The user will need to “select” each message that they want to encrypt.
- There is an external website that can be accessed that requires the user to log on to in order to download their certificate. This is the way that Outlook Web Access users would acquire their certificate.

Messaging Encryption

Things to be aware of

- If a user sends an encrypted message, the recipient must have the key in order to read the message.
- Each individual user has their own specific key
- This solution is only available to users who have migrated to the COV domain.

Messaging Encryption

Further Questions

?????????

Virginia Interactive Security

April 2008

Presented by
Lynn DuBard

Overview

The following information is covered in this presentation:

- Services offered by Virginia.gov
- SOX
- PCI DSS
- Sensitive Data
- Acceptable Use
- Social Engineering
- Verizon Business – Security Solutions Powered by CyberTrust (*formerly known as CyberTrust*)

Virginia Interactive is Virginia.gov

- Virginia.gov is a public private partnership established between the Virginia Information Technologies Agency (VITA) and Virginia Interactive. Virginia Interactive, a subsidiary of [NIC](#), manages the commonwealth's portal and brands and markets eGovernment websites and services as Virginia.gov.
- The primary goal of Virginia.gov is to positively transform the relationships between citizens and government by utilizing the Internet to provide a more efficient method for obtaining information and services.

Virginia.gov's Services

- Web development
- Marketing
- Web design
- Enterprise solutions
 - Payment portal
 - Google
 - Online store
 - Event registration
 - Live help
- Accessibility, Usability and Commonwealth Policies, Standards and Guidelines
- Portal management

SOX – Sarbanes Oxley

Introduction

- The Sarbanes Oxley Act requires public companies to commit to a number of different activities and that their outside auditors will certify to their compliance with these requirements.
- Depending on the section, civil and criminal penalties can apply for violations of this act.

SOX – Sarbanes Oxley

Section 404 requirements

- Corporate has centralized as much of this requirement as possible, but there are requirements that each business unit must also meet.
- Section 404 requirements are subject to change. They must be reviewed by NIC at least annually and changes made to ensure that our internal controls meet current business needs.

SOX – Sarbanes Oxley

Compliance due dates

Compliance Topics	Due Dates	Portal
Login Review & Change Management	Feb 28, May 31, Aug 31, Nov 30	Virginia
Password Testing and Firewall Review	Apr 30	Virginia

SOX – Sarbanes Oxley

Key controls

- The following items are key controls for Sarbanes-Oxley and evidence will need to be provided upon request:
 - Computer room access must be restricted.
 - GM must review monthly accounts receivable aging report.
 - Data backup and recovery practices need to be in place.
 - GM must approve all payroll changes.

PCI DSS

Introduction

- The Payment Card Industry (PCI) is a consortium of the four major credit card companies. This organization was created for the purpose of developing a uniform set of security principles for those organizations which process credit card transactions.
- There are many rules governing the structure of credit card processors and those who service these companies.



PCI DSS

Structure

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

PCI DSS

Indicating compliance

- Have an outside security scanner scan our networks each quarter to assess whether we have vulnerabilities that need to be patched.
- Annually submit a questionnaire that asks detailed questions about our compliance for each area.
- The corporate data center or CDC is beginning the process of having an outside assessor verify our compliance with the standard. Once this process is complete, the CDC will be listed on a list of certified service providers.
- This step is will be required for VI once we reach 2,000,000 credit card transactions annually.

Sensitive Data

Company / Portal Policy Excerpts

- Sensitive data as defined by VI includes the following:
 - Credit card numbers, expiration dates and ccv values
 - Bank account numbers
 - Social security numbers
 - Driver's license numbers
 - Other State identification numbers

When they are stored with other defining personal information, such as

- Name
- Address
- Birth date
- Routing number
- Other information that would match the sensitive data to an individual.

Everything we do as a company depends heavily on the protection of sensitive data

Sensitive Data

Company Policy Excerpts

- In some States, legislation has been passed expanding the definition of sensitive or personal information. In those states, the State definition should be treated as expanding the definitions above to match the broader State definitions.

Actions to Protect Sensitive Data

- The company policy also identifies what actions must be taken to protect sensitive data that is in our custody:
 - Sensitive data should not be stored longer than required for business necessity.
 - Sensitive data fields should be encrypted by strong methods using a minimum key length of 128 bits or longer, where practicable.
 - Sensitive data should not be transmitted by any insecure means.
 - Decryption keys should be securely stored and not embedded in the application nor stored on the same server as the data itself.
 - When user interfaces require displaying credit card information, truncating or masking the sensitive data is required

Sensitive Data

3rd Party Data

- VI is accountable for sensitive data that is passed on to third parties. Our portal policy states:
 - Sensitive data should be transferred to business partners only in situations where required by business necessity.
 - In the case of credit card information, these partners must have a signed agreement with VI stating that they are compliant with any regulations or guidelines required by industry standards, which is reviewed no less often than yearly.
 - If sensitive data must be transferred to a business partner, for example, for payroll processing, insurance or similar purposes, care must be taken to insure that those partners are aware of the proper methods for handling the data.

Acceptable Use

Introduction

- VI provides equipment to its employees for the purpose of conducting business. *An important question for each employee is for what purposes can this equipment be used?*
- The company has a policy regarding what is acceptable use of company equipment and company networks that defines these actions.
- *Disciplinary actions can be taken for violation of this policy up to and including termination of employment.*

Social Engineering

Introduction

- Security training often focuses on primarily technical issues. Most security breaches come from a source that is almost non-technical.
- Employees who provide information to others who are not authorized to receive this information may be the largest source of security breaches.



Social Engineering

Common Approaches

- Some of the most well known are:
 - Shoulder surfing
 - Dumpster diving
 - Posing
 - Phishing
 - Pharming
- Always beware of unsolicited requests by email, phone or even in person for information to be provided.
- If in doubt, always confirm by an independent means that the request is valid.
- Get management assistance if there is any doubt about the request.
- Assume we are a TARGET.



Corporate / Portal Security

As an organization grows, the technology industry recognizes that it is a “Best Practice” to implement a Corporate Security Program.

- **Corporate Security Program**

- Layers of protection
- CyberTrust SMP
- Laptop encryption
- Sensitive data discovery

- **Security as a Marketing Tool**

Why focus on Security?

Be a Secure Partner

It is important to be able to recognize and minimize vulnerabilities

- System and network scanning
- Sensitive data awareness and protection
- Assessment by an independent 3rd party security company

Meet and Exceed Expectations

Meet and exceed laws and industry standards that apply to our business

- SOX and PCS DSS
- NACHA / ACH Rules
- State and Federal Privacy Laws

Be proactive instead of reactive.

Security Focus Areas

Application Development

- It is important to make security a key component of the Application Development lifecycle. Consider the following items:
- Security training for developers
- Vulnerability scans performed before applications are moved into production
- Code reviews and separation of duties

Technology Infrastructure

- Security is a key component in the Technology infrastructure
- Layered approach
- Core financial applications – Virginia Payment Portal, VPP
- Use of application firewalls
- Upgraded VPN capabilities on our network
- Implementation of systems and network patches on a regular basis

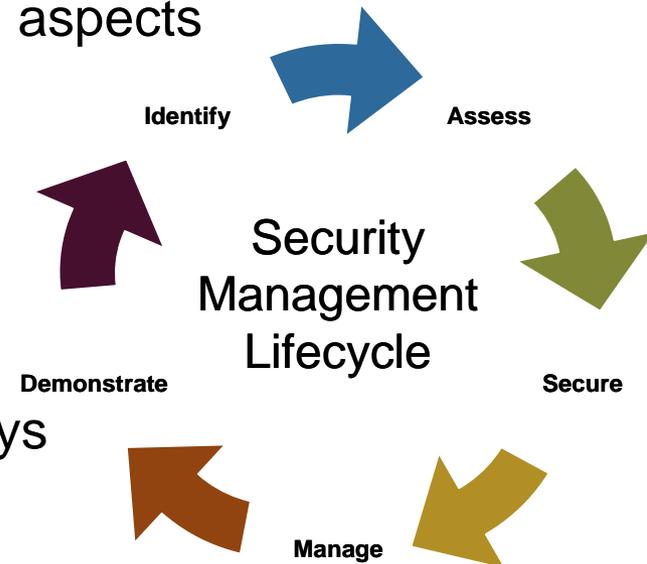
Layers of Protection

Layer		Approach
Compliance / Industry Best Practices	SOX PCI DSS NACHA/ACH Rules	State and Federal Statutes CyberTrust SMP Best Practices
PC Tier	Laptop Encryption Desktop Risk Assessment Secure Remote Access/VPN	
Network	Firewalls IDS/IPS Load Balancers Security Metric Scanning CyberTrust Scanning Trip Wire Enterprise Manager	Web Application Firewalls Nessus/NMAP Scans Logging/Review VPNs E-mail Filters Spam AV
Web/Application Tier	AppScan Encryption Mod_Security Third Party App Segmentation Manual Review for Sensitive Data	Virtualization Secure Web Dev. Training Language Selection Logging / Review Automated Scripts for Sensitive Data/WebSense CPS
Database Tier	Encryption Manual Review for Sensitive Data Logging/Review	Database Platform Selection Automated Scripts for Sensitive Date/WebSense CPS

CyberTrust

CyberTrust Security Management Program (SMP) Certification

- Reviews both administrative and technical aspects
- 164 Essential Practice Controls
 - Policies
 - Procedures
 - Standards
 - Configurations
 - Technical components
- Vulnerabilities are identified in 6 major ways
 - External
 - Internal
 - Desktop
 - Email
 - Wireless
 - Phone lines



Security Program

- **Laptop Encryption Solution**

- Microsoft BitLocker
- AES 256 bit whole disk encryption
- Reduces risk due to lost or stolen laptops
- Smartcard readers on all laptops

- **Sensitive Data Discovery Tool**

- Websense CPS
- Configured to include policies for all current laws and industry standards including PCI, SOX and HIPAA
- Supports multiple platforms and file types

Security as a Marketing Tool

- **Emphasize the Layered approach**
 - Resources (Portal, Corporate and Third Parties)
 - Technology (Application, System and Network)
- **Emphasize our compliance efforts**
 - SOX, PCI DSS and NACHA / ACH Compliance
 - CyberTrust SMP Certification
- **Be the front line in speaking with Partners**
 - Know what is considered sensitive data
 - Educate partners about the risks associated in working with sensitive data
 - Explore alternatives rather than using sensitive data, where possible

Questions?

Lynn DuBard

General Manager

ldubard@virginiainteractive.org

804 692 0599


Virginia.gov

Commonwealth Information Security Council

Commonwealth Information Security Council -The Beginning

Formed: April, 2007

Eleven Information Security Officers from different state agencies meet monthly; discussing ways to strengthen the information security posture of the Commonwealth.

Visit our website at

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

Purpose

- The Commonwealth Information Security Council recommends strategic direction on Commonwealth information security and privacy-related initiatives.
- The purpose of the Council is to increase, through education, the understanding of key business processes of customer Agencies and of VITA; to obtain consensus and support for enterprise-wide security initiatives; to identify key areas for process improvement; and to coordinate Agency business processes with VITA (Directorate) processes.

Council Objectives

- The core objectives of the Commonwealth Information Security Council are:
 - **To foster the adoption of consistent and complete information security policies, standards and procedures to protect Commonwealth-wide information resources,**
 - To encourage efficient allocation of information security resources,
 - To respond to changes in the environment which call for corresponding changes in the Commonwealth information security infrastructure,

Objectives - continued

- **To recommend and sponsor information security awareness, communication and education programs to develop an information security conscious culture across the Commonwealth,**
- To serve as agency sponsors of the Commonwealth information security program, providing both credibility and visibility,
- **To provide a forum to discuss and assess pending legislation, regulation and/or requirements that have the potential to impact Commonwealth or individual agency information security practices, thereby enabling the Commonwealth to take proactive steps to address such mandates.**

IS Council -The Early years

The Council has formed committees around the following four initiatives and ISOs from various agencies 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.

IS Council – The Early Years

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.

IS Council – The Early Years

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

The next Generation

- Boldly go where no other council has gone before!
- Seek out new problems and solutions.
- Leap over tall buildings with a single bound... oops wrong show!

Thank you



Compliance with § 2.2-2009

Ed Miller

Manager Information Security Assurance





§ 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.



Data Points for § 2.2-2009 Compliance

- In order to assess compliance with § 2.2-2009, VITA is leveraging as much information as possible from what is currently available.
- COV ITRM SEC policies and standards (500-02, 501-01 and 502-00) already require Executive and Independent agencies to submit certain information to VITA on a scheduled basis.



Data Points for § 2.2-2009 Compliance

- Designation of an Information Security Officer
- Submission of an IT Security Audit Plan for sensitive systems
- Submission of the Corrective Action Plans to address audit findings on a quarterly basis
- For customer agencies of the IT Infrastructure Partnership – submission of an IT Disaster Recovery Plan



Data Points for § 2.2-2009 Compliance

- Number and type of IT Security Policy & Standard Exceptions
- IS orientation attendance. Although not required, it does demonstrate commitment to developing an adequate security plan for an agency.
- Results of APA's Senate Joint Resolution 51 follow-up report to be issued around August, 2008.



Data Points for § 2.2-2009 Compliance

- Reported security incidents & data breaches relative to timeliness of reporting as well as the severity, handling, response and resolution of the incident.
- The results & remediation efforts for all security audits, SAS70 audits, and vulnerability or infrastructure assessments, in addition to any IT Security Audit findings reported by the APA, internal audits or other auditing engagements.



Data Points for § 2.2-2009 Compliance

- Agencies that have deficiencies will be notified and given opportunities to come into compliance. This is the first such notice.
- The CIO will report to the Governor, ITIB, APA and affected Cabinet Secretaries, any agencies with unacceptable results by the end of calendar year 2008.



Data Points for § 2.2-2009 Compliance

- The following tables for each Secretariat document the current status of some of the data points that will be monitored:
 - ISO Confirmation
 - IT Security Audit Plan Submission
 - Corrective Action Plans
 - IS Orientation / Training attendance
 - IT DR Plan submission
 - APA's 2006 SJR51 Rating



Secretariat: Administration

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



Secretariat: Agriculture and Forestry

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



Secretariat: Commerce & Trade						
Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR Plan Rec'd	CAP's Rec'd
BOA	YES	YES	YES	INADEQUATE	YES	N/A
DBA	NO	YES	YES	INADEQUATE	YES	NO
VEDP/VTA	NO	YES	NO	INADEQUATE	YES	NO
VEC	YES	YES	YES	INADEQUATE	YES/UPD	N/A
DHCD	YES	YES	NO	INADEQUATE	YES	NO
DOLI	NO	YES	YES	INADEQUATE	YES	NO
DMME	YES	YES	NO	INADEQUATE	YES	NO
DPOR	YES	YES	YES	INADEQUATE	YES	NO
VRC	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
VRA	NO	NO	NO	NOT ASSESSED	N/A	NO
TIC	NO	NO	NO	NOT ASSESSED	N/A	NO



Secretariat: Education (excluding Higher Ed)

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR Plan Rec'd	CAP's Rec'd
DOE	YES	YES	NO	INADEQUATE	YES	NO
FCMV	NO	YES	NO	NO PROGRAM	NO	NO
GH	NO	NO	NO	NO PROGRAM	NO	NO
SCHEV	EXTENSION EXPIRED	YES	NO	INADEQUATE	YES	NO
JYF	YES	NO	YES	INADEQUATE	YES	N/A
LVA	YES	YES	YES	INADEQUATE	YES	N/A
VMFA	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
VSM	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 DR Plan Rec'd	CAP's Rec'd
CNU	YES	YES	NO	ADEQUATE	N/A	N/A
VMI	YES	YES	NO	ADEQUATE	N/A	N/A
VCCS	YES	YES	NO	ADEQUATE	N/A	N/A
GMU	YES	YES	YES	INADEQUATE	N/A	NO
JMU	YES	YES	NO	ADEQUATE	N/A	Q1
LU	YES	YES	YES	INADEQUATE	N/A	Q1, Q2, Q3
NSU	NO	YES	NO	INADEQUATE	N/A	NO
ODU	YES	YES	YES	INADEQUATE	N/A	Q2
RU	YES	YES	NO	INADEQUATE	N/A	N/A
VSU	YES	YES	YES	INADEQUATE	N/A	N/A
RBC	YES	NO	NO	INADEQUATE	N/A	Q3
UMW	YES	YES	YES	INADEQUATE	N/A	N/A



Secretariat: Executive (Governor)						
Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR Plan Rec'd	CAP's Rec'd
GOV	EXTENSION EXPIRED	YES	YES	INADEQUATE	YES	NO
OAG	NO	YES	YES	INADEQUATE	N/A	NO



Secretariat: Finance

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR Plan Rec'd	CAP's Rec'd
DOA	NO	YES	NO	ADEQUATE	YES	NO
DPB	EXTENSION EXPIRED	NO	YES	INADEQUATE	YES/UPD	NO
TAX	YES	YES	YES	ADEQUATE	YES	N/A
TRS	YES	YES	NO	INADEQUATE	YES	NO



Secretariat: Health & Human Resources

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR Plan Rec'd	CAP's Rec'd
VDA	YES	YES	YES	NO PROGRAM	YES	N/A
DHP	YES	YES	NO	ADEQUATE	YES	N/A
VDH	YES	YES	NO	INADEQUATE	YES	Q1, Q2
DMAS	YES	YES	YES	INADEQUATE	YES	NO
DMHMRSAS (CBR)	YES	YES	YES	INADEQUATE	YES	N/A
DRS (VBP, VDBVI, VDDHH, WWRC)	YES	YES	NO	ADEQUATE	YES	N/A
DSS (CSARYF)	YES	YES	NO	INADEQUATE	YES/UPD	N/A
TSF	NO	NO	NO	NOT ASSESSED	NO	NO



Secretariat: Natural Resources

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



Secretariat: Public Safety

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR Plan Rec'd	CAP's Rec'd
ABC	YES	YES	NO	INADEQUATE	YES	Q1, Q2
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	YES	NO PROGRAM	YES	NO



Secretariat: Technology

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



Secretariat: Transportation

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR 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	N/A
DRPT	YES	YES	YES	INADEQUATE	YES	N/A
VDOT	YES	YES	YES	INADEQUATE	YES	Q1, Q2
VPA	NO	NO	NO	ADEQUATE	N/A	NO



Independent Branch Agencies

Agency	Audit Plan Rec'd	ISO Confirmed	Attended IS Orientation	2006 SJR51 Rating	IT DR 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	NO	YES	NO PROGRAM	N/A	NO
VCU-HSA	NO	NO	NO	NOT ASSESSED	N/A	NO
VOPA	NO	NO	NO	NO PROGRAM	N/A	NO
VWCC	NO	NO	NO	INADEQUATE	N/A	NO



Compliance with § 2.2-2009

- Questions?



Requesting Exceptions IT Security Policy and Standards

Cathie Brown, CISM, CISSP

Deputy, Chief Information Security Officer



Security Exception FAQ's

- When do I request an exception?
- How do I request an exception?
- What information do I put on the exception request form?
- What's the process once the exception form is submitted?
- How long is an exception good for?
- What happens when an exception expires?
- Can you show an example?



When do I request an exception?

- When the agency will not meet a requirement in one or more of the following security policy or standards:
 - IT Security Policy (SEC500-02)
 - IT Security Standard (SEC501-01)
 - IT Security Audit Standard (SEC502-00)
 - Removal of COV Data from Electronic Media Standard (SEC514-03)
 - Use of Non-COV Devices to Telework Standard (SEC511-00)



How do I request an exception?

- Download the exception request form
<http://www.vita.virginia.gov/uploadedFiles/Library/ITSecurityPolicyStandardExceptionRequestForm.doc>
- Send to VITA by either
Submitting the completed form to
VitaSecurityServices@vita.virginia.gov
 - **The agency head sends OR is copied** on the email submission, or
 - Attach a scanned copy of the form **signed by the agency head** to the email
- OR
Mailing or faxing the completed form **signed by the agency head**
 - VITA CS&RM, 11751 Meadowville Lane, Chester VA 23836
 - Fax (804) 416-6359



What information do I put on the form?

- Agency Name
- Contact for Additional Information
- Requirement from which an exception is requested
 - Include the section of the Policy or Standard
- Provide the Business or Technical Justification
- Describe the scope including quantification and requested duration (not to exceed one (1) year)
- Describe all associated risks
- Identify the controls to mitigate the risks
- Identify any unmitigated risks
- **Agency Head approval**



What's the process after submitting the form?

- Form reviewed for completeness
 - All sections are filled out
 - Agency Head has approved or been copied on email
- Technical Review
 - May request additional information
 - Evaluate for alternative solutions
- Based on review
 - Recommend approval, alternative solution or denial or
 - Recommend to Agency to re-write the exception request to reflect additional information or alternative solution
- Exception is approved or denied
- Signed form is scanned
- Email completed form as 'approved' or 'denied' to the contact with copy to Agency Head



How long is an exception good for?

- Maximum amount of time an exception is valid is 1 year
 - In some cases, timeframe may be less
 - There are no blanket exceptions
- As circumstances and configurations change, exceptions must be reviewed
 - Assess if the exception is still required
 - Assess if controls are still adequate
 - Update information



What happens when an exception expires?

- Existing exceptions are reviewed on a weekly basis for expiration dates
- Once an exception has expired an email with a copy of the exception is sent to the Agency
 - Requesting an update or
 - Requesting a new exception if still needed
- Our goal is to send the notification emails 30 days before expiration
- Exceptions approved for postponing the implementation of COV Security Policy and/or Standard or for postponing remedial action of NG Self Assessments will not be renewed
 - A status letter will be requested



Can you show an example?

COV IT Security Policy & Standard Exception Request Form

Agency Name: Department of Virginia State Agency

Contact for Additional Information: State Agency ISO

Requirement to which an exception is requested:

SEC501 5.2.2 #16 –Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.

SEC501 5.2.2 #17. Require that local administrator rights, or the equivalent on non-Microsoft Windows based IT systems, be granted only to authorized IT staff.



Example (continued)

1. **Provide the Business or Technical Justification:**

In order to be productive, members of this group need to be able to install, configure, patch, and upgrade certain software products on development machine(s).

We are requesting local administrator accounts to be utilized for installation and updates of software that falls outside the scope of Partnership support. Additionally should a need arise for administrative privileges which falls outside of install/update we will utilize the "runas" command as outlined in Microsoft's "How To: Secure Your Developer Workstation"

[<http://msdn2.microsoft.com/en-US/library/aa302367.aspx>].



Example (continued)

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

The following list of state agency employees requires both admin and regular user accounts on their PCs:

See attached list. Duration requested for 1 year.

3. Describe all associated risks:

Local Administrators have complete and unrestricted access to the computer, which can allow the download of spyware/malware to the device and alter configuration settings or remove security software.



Example (continued)

4. Identify the controls to mitigate the risks:

Additionally the following controls will help mitigate the risks:

- Individuals who are granted this privilege must be trusted to use the privilege in a responsible manner.
- Although there is no guarantee that loss of data or system failure will not occur on the pc which this affects, the individual should be properly trained in the installation and use of the software tools involved to minimize this risk, and pc restore can be applied if failure does occur.
- The use of regular user accounts will be used unless tasks are necessary that require local admin privileges.

5. Identify any unmitigated risks:

A user with administrative privileges can download and install malicious code and/or disable security software protecting the computer.



Example (continued)

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

Agency Head

Date



Comments and/or Questions





Web Application Security

Michael Watson

Incident Management Director

Commonwealth Security



Web Application Security

- The System
 - What parts of the system and/or process could an attacker exploit?
- The Application
 - What parts of the application could an attacker exploit?
- How can we protect the Application?



The System

- The Attack of Then
 - Patches
 - Attempt to take over a system using security vulnerabilities
 - Misconfigured Services
 - Websites inadvertently allow anyone to upload files
 - Security Controls not in Place
 - Allows attackers to gain access to what should be protected resources



The Application

- The Attack of Now
 - Data Injections
 - Cross Site Scripting - XSS (other site scripting as well)
 - Remote Code Execution
 - Data Leakage



What is a web application?

- From CGI to Web 2.0
 - CGI – Common Gateway Interface
 - Simple form based application to send data
 - Scripting/Scripting Frameworks
 - JavaScript/PHP – Became popular due to CGI's lack of session management and authorization controls.
 - Application Frameworks
 - Java/.Net – Scripting languages did not scale and had performance problems.



Policy and Procedures

- Establish standards of review for applications
 - 3rd Party Developers
 - Include security in the requirements design
 - Home Grown Development
 - Integrate security into the development life cycle
 - COTS – Commercial Off The Shelf
 - Test the final configuration for vulnerabilities
 - Be aware of holes that may be exposed via a COTS application (i.e. SQL)
- Secure Coding Practices



How to Protect the Application

- Types of Attacks
 - Data Injections
 - Cross Site Scripting - XSS (other site scripting as well)
 - Remote Code Execution
 - Data Leakage/Exposure



Data Leakage/Exposure

- Protecting the Data
 - Encryption – SSL, TLS, etc.
 - End point compromise renders encryption ineffective
- Protecting the Inputs
 - Crossover with Data Injection
 - Display unintended data
- Proper Access Controls
 - Least Privilege
 - Defense In Depth



Data Leakage In Real Life

- Lasell College alerted 20,000 current and former students and staff that their personal information was illegally accessed by a college employee. The employee, a member of the Department of Information Technology, gained unauthorized access to a database containing names and Social Security numbers. The college became aware of the incident in early February after investigating suspicious activity.
 - “We deeply regret this situation and are taking steps to investigate what has happened and to put measures in place to improve the protection of our data and to limit the data we keep to what we really need,” said Chief Information Officer Deborah Gelch.



Data Injections

- Never trust data from the client
- Scrub the input
 - Validate and check data integrity
 - Make sure that the data entered is what you expect
 - Don't use JavaScript to validate
 - Make sure that the different data formats are checked
 - BASE64 Encoding, UUEncode, Hex Encoding, etc.
 - Avoid taking commands from input fields
- Use least privilege
 - Restrict database and file permissions to only the accounts that need them
 - Use separate accounts for those who need to read and those that need to write

SQL Injection Example

- Form using SQL to obtain data associated with an email address
 - `SELECT field FROM table WHERE field='jdoe@vita.gov';`
- Modified query to display all data
 - `SELECT field FROM table WHERE field='something' OR 'x'='x';`
 - Similar queries are used to map a database's schema.
- Drop a table
 - `SELECT field FROM table WHERE field='something';
DROP TABLE table;_--';`



SQL Injection Incidents

- Widespread web attacks started since January
 - TrendMicro Affected
 - Computer Associates
- Beginning to become coordinated injections
 - Probe and then attack all at once



XSS Scripting

- Facilitates Phishing
 - Allows creation of links that look like they are from an authorized website
- Can reference exploit code
- Always use DNS names in publications and references to links
- Commonly overlooked when developing applications

XSS Example

- IFRAME JavaScript
 - `<IFRAME SRC="javascript:alert('XSS');"></IFRAME>`
- DIV Tag
 - `<DIV STYLE="width: expression(alert('XSS'));">`
- Page Generated
 - `http://www.xx.state.xx.us/homelandsecurity/Search/Search.asp?col=pasearch&qt=%22%3E%22%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E&charset=iso-8859-1&qp=url%3A%2Fwww.xx.state.xx.us%2Fxx%2F`
- Sites Affected in the last month
 - ATT, paypal, usatoday



Remote Code Execution

- Attempts to exploit known vulnerabilities
- Attackers obfuscate code
 - Encoded data
- Packages of remote code available for sale
 - MPACK
- Typically hosted on remote systems
 - Referenced by XSS, SQL Injected links, etc.



Use Best Practices

- Code Reviews
- Vulnerability Scans
- Data Validation and Integrity Checks
- Least Privilege



COV IT Security Standard 501 Roles and Responsibilities

Peggy Ward

Chief Information Security & Internal Audit Officer



Roles and Responsibilities matrix

- **Overview:**

- We took each requirement of the IT Security Standard 501 and laid it into an excel spreadsheet.
- These requirements were identified by the words require, document, provide, identify, implement, establish, designate, etc.
- For each requirement we identified the responsibility for carrying out that requirement.
- The Agency is ultimately responsible for complying with all of the requirements.
- However, if a COV agency has an infrastructure service provider (ISP), we identified responsibility for each requirement as the agency, the agency and ISP, agency with ISP or ISP.



Roles and Responsibilities matrix – Examples

2.2.2 Requirements	Each Agency Head shall fulfill the following responsibilities:		
1	As required by Section 2.3 of the COV <i>IT Security Policy</i> (ITRM Policy SEC500-02), via e-mail to VITASecurityServices@vita.virginia.gov, designate an Information Security Officer (ISO) for the agency, and provide the person’s name, title and contact information to VITA no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO.	Agency	
2.6.2 Requirements	For each Agency-owned IT system classified as sensitive, the Agency shall fulfill the following responsibilities:		
1	Conduct a formal RA of the IT system, as needed, but not less than once every three years.	Agency with ISP	ISP provide technical advice
3.4.2 Requirements	For every IT system identified as sensitive, each Agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems and data in accordance with Agency requirements. At a minimum, these plans shall address the following:		
1	Secure off-site storage for backup media	ISP	



Roles and Responsibilities matrix

- **A couple of notes:**
 - All new requirements are listed in blue and have a compliance data of 7/1/08
 - Please note Infrastructure Service Provider (ISP) where applicable
- **A copy of the Roles and Responsibilities matrix can be found on our web site at:**
<http://vita.virginia.gov/security/default.aspx?id=323>



QUESTIONS?





Virginia Information Technologies Agency

Upcoming Events





UPCOMING EVENTS

IS Orientation

Wednesday, April 9th, 1:00 – 3:30 p.m. @ CESC

Wednesday, May 28th, 2:30-5:00 pm @ CESC

IS 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 ISO's and interested IT persons!

To register email VITASecurityServices@VITA.Virginia.gov



UPCOMING EVENTS

Commonwealth Information Security Council Meeting

Friday, April 11, 9:00 - 11:00 a.m. @ CESC with
Committee meetings from 11:00 - 12:00

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

The US Department of Homeland Security's National Cyber Security Division and the Multi-State Information Sharing and Analysis Center invite you to participate in the next session of the National Webcast Initiative:

~ Application Security ~

Wednesday, April 23rd, 2008
2:00pm - 3:00pm (Eastern)

<http://www.msisac.org/webcast/2008-04/>



UPCOMING EVENTS!

NEXT ISOAG MEETING!

Wednesday, May 21st 1:00 – 4:00

@ CESC



Any Other Business ???????





ADJOURN

THANK YOU FOR ATTENDING!!

