



Virginia Information Technologies Agency

Commonwealth Information Security Advisory Group (ISOAG) Meeting

March 14, 2007



ISOAG March 2007 Agenda

- | | |
|--|--------------------|
| I. Welcome | Peggy Ward, VITA |
| II. Commonwealth Enterprise Solutions Center (CESC) Tier III Data Center | Dana Taylor , NG |
| III. CESC Physical Security | Ralph Bell, NG |
| IV. Server Virtualization/Shared DASD Security | Dana Taylor , NG |
| V. CESC Data Center Information Security | Trey Stevens, NG |
| VI. Encryption Solution Ordering Specifics | Don Kendrick, VITA |
| VII. SJR 51 Action Plan | Cathie Brown, VITA |
| VIII. IT Legislation | Peggy Ward, VITA |
| VIII. Other Business | Peggy Ward, VITA |

Facilities Overview

Commonwealth Enterprise Solutions Center

Presented by: Dana Taylor



Basic Data Center Infrastructure

- Floor Plan
- Amenities
- **Electrical**
- **Mechanical**
- **Questions and Answers**

Meeting Tier III

“ the key to Tier III is concurrent maintainability...”

Uptime Institute

- **The Data Center is 50,000 sq ft**
- **100 Watts per sq ft (corner to corner)**
- **Raised floor is 48”**
- **All equipment have dual source power**
- **Security Cameras**
- **Access control (including Portal with Bio)**
- **CMOC (Consolidated Management Operations Center)**
- **Fire Protection - Pre-Action Sprinklers and VESDA**
- **Cable management**
 - Server PODs Via overhead Cable tray
- **Two separate Dmarc Locations (3 Rooms each)**

- **Separation of VITA and Northrop Grumman**
- **Central Monitoring (CMOC)**
- **Expandability**
- **Testing and Burn In Labs**
- **Security Operations Center (SOC)**
- **Hot Cold Isles**
- **Floor Layout (Alpha Numeric floor grid)**

Page Intentionally Omitted

Page Intentionally Omitted

Page Intentionally Omitted

400A516 Page Intentionally Omitted

GENERATOR PARALLELING GEAR



GENERATOR



SPECIAL SYSTEMS

- **VESDA (Very Early Smoke Detection Apparatus)**
- **Elevated Cable Tray**
- **Access Control and CCTV**
- **Local and Remote Monitoring**
- **Signal Reference Grid**
- **Emergency Power Off**

Page Intentionally Omitted

Typical Computer Room Air Conditioning Unit (CRAC)

Multiple CRAC units installed for initial Data Center operation



Page Intentionally Omitted

Page Intentionally Omitted

Page Intentionally Omitted

Page Intentionally Omitted

CESC Physical Security Overview

Ralph Bell



Page Intentionally Omitted

Page Intentionally Omitted

Pegasys P2000 Security Management System

The Pegasys P2000 technology has been utilized as the security platform for many agencies and critical infrastructures in the Commonwealth of Virginia including:

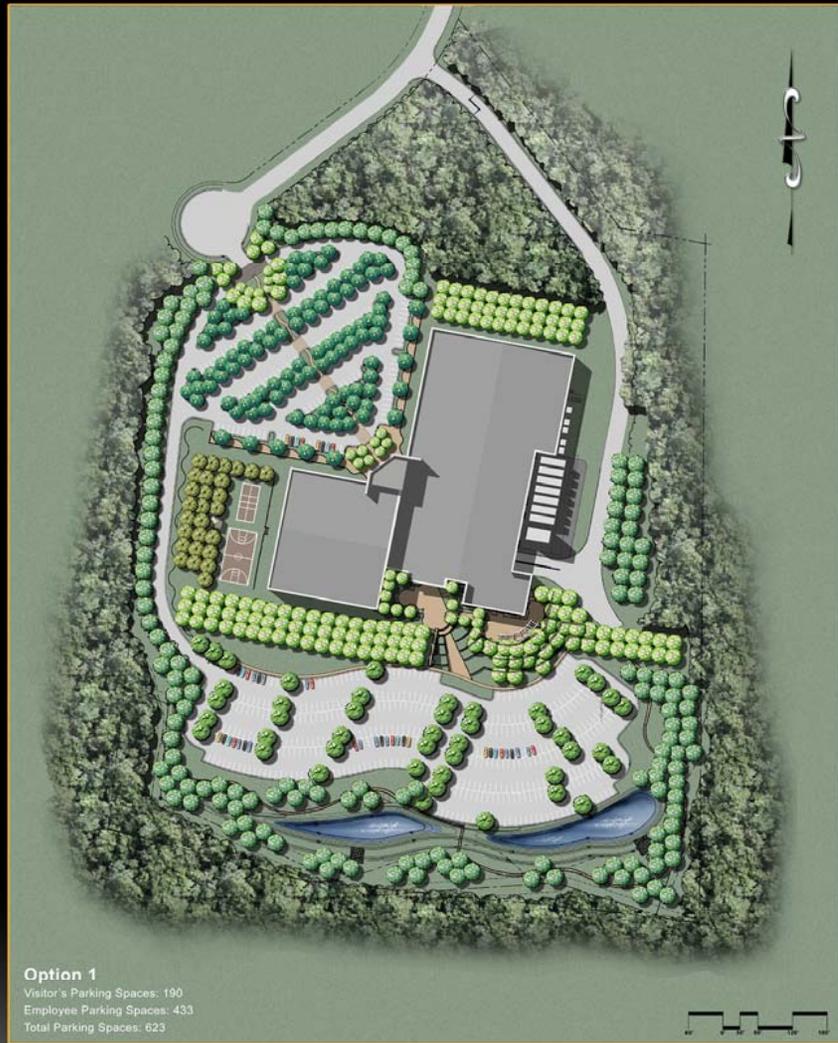
- § Virginia Department of Transportation**
- § Virginia Department of General Services - including**
 - Capitol
 - Supreme Court
 - Division of Consolidated Laboratory Services
- § Virginia State Police**
- § The Chesapeake Bay Bridge Tunnel Authority**
- § Virginia Department of Public Rail & Transportation**
- § Virginia Department of Emergency Management**
- § Virginia Forensic Laboratories**

Page Intentionally Omitted

Page Intentionally Omitted

Page Intentionally Omitted

Security Walk Through



Richmond Enterprise Solution Center



Meadowville Technology Park
Chesterfield County, Virginia



NORTHROP GRUMMAN

Server Virtualization/ Shared DASD Security

Dana Taylor

VMware Infrastructure Security Components

- § VirtualCenter
- § The virtual machines
- § The virtualization layer, consisting of the VMkernel and the virtual machine monitor
- § The ESX Server service console
- § The ESX Server virtual networking layer
- § Virtual storage

Isolation is a Virtualization Benefit

- § ESX Server can be deployed in a variety of scenarios, including *Restrictive Multi-customer Deployment*
- § Virtual machines are isolated from the host machine and other virtual machines running on the same hardware
- § They share physical resources such as CPU, memory and I/O devices, but cannot “see” any device other than virtual devices made available to it by the virtual machine monitor
- § Data does not leak across virtual machines. Applications only communicate over configured network connections

VirtualCenter

- § Centralized management of the VMware Infrastructure
- § Sophisticated system of roles and permissions
- § Allows fine-grained determination of authorization for administrative and user tasks, based on user or group and inventory item, such as clusters, resource pools, and hosts
- § Allows only the minimum necessary privileges to be assigned in order to prevent unauthorized access

Page Intentionally Omitted

Virtual Storage

- § Centralized management of the VMware Infrastructure
- § Sophisticated system of roles and permissions
- § Allows fine-grained determination of authorization for administrative and user tasks, based on user or group and inventory item, such as clusters, resource pools, and hosts
- § Allows only the minimum necessary privileges to be assigned in order to prevent unauthorized access

Page Intentionally Omitted

Page Intentionally Omitted

Page Intentionally Omitted

Page Intentionally Omitted

Questions?

Contact Information:

§ Mike Shaffer – VITA Service Delivery Manager

§ mike.shaffer@vita.virginia.gov

§ Don Norwine – Server Functional Area Lead

§ don.norwine@ngc.com

§ Jennifer Breitzmann – Server Functional Area

§ jennifer.breitzmann@ngc.com



Logical Security - Networks

Trey Stevens

Security Engineer



NORTHROP GRUMMAN

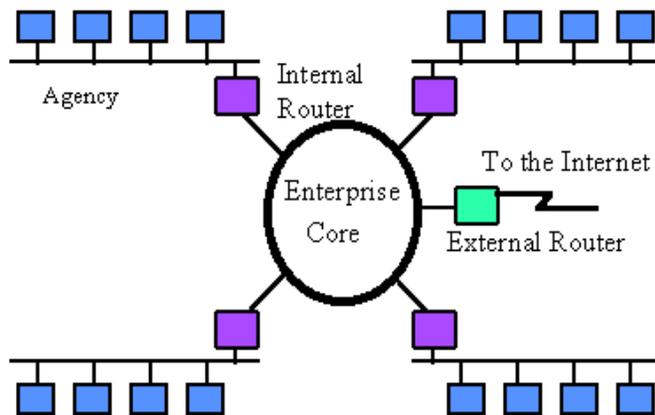
Premise

Agencies have expressed concern that in the new shared environment, where all of their resources are physically beside systems outside of their control, that data security may suffer.

Network segmentation

- Agencies will be logically separated in several different ways
 - TCP/IP range
 - VLAN separation
 - Firewalls

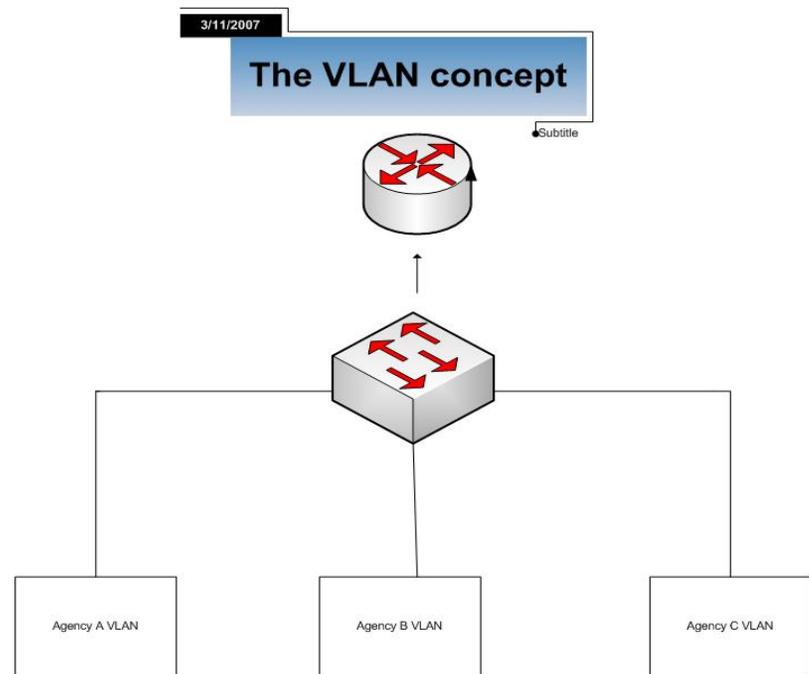
TCP/IP range



Each agency will be allocated their own range of addresses. Based on the nature of TCP/IP, these ranges cannot communicate with one another without going through a router/firewall.

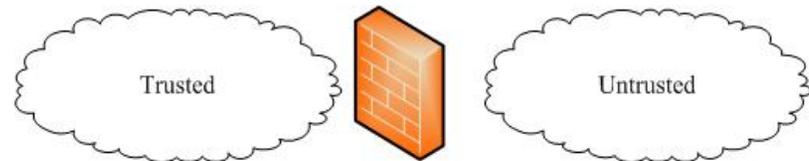
VLAN's

- Virtual Local Area Network's are a very flexible type of LAN in which machines located in the same physical area are not necessarily on the same LAN broadcast domain.
- Virtual LANs (VLANs) are used as a means to identify and then segment traffic at a very granular level.



Firewalls

- Firewalls will be used to protect specific resources, thereby reducing the risk of unauthorized access to sensitive information.
- In addition to user containment, internal firewalls contain attacks to prevent damages from spreading in the event that an attack occurs.

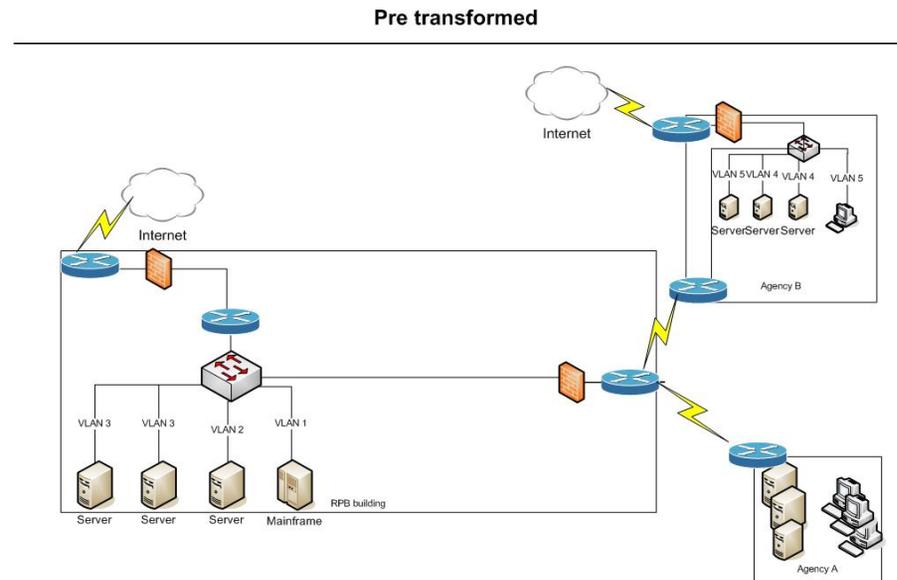


Defense in depth

- Physical security maintained in a Tier 3 data center as described by Dana Taylor.
- Layer 2 switch security with VLAN's
- Layer 3 security with firewalls
- Additional security not discussed such as NIDS/NIPS and HIDS

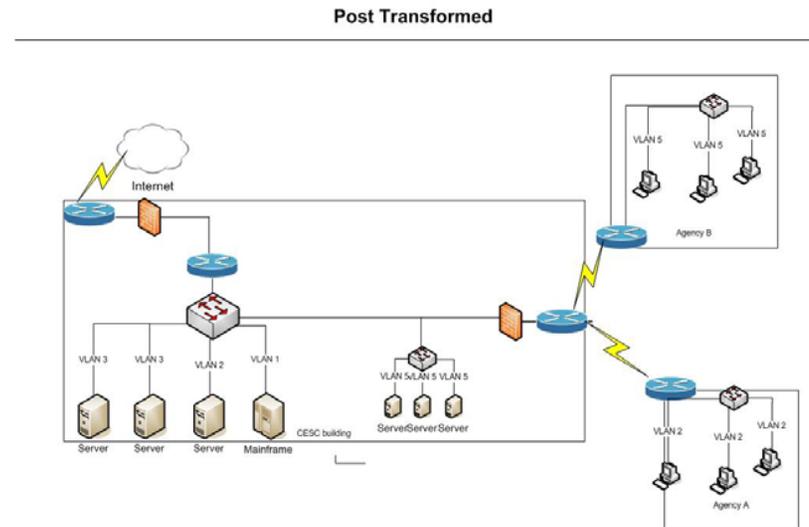
Before Transformation

- Before Transformation, Agencies may have differing degrees of logical separation.
- For example, Agency A in this diagram is basically a 'flat' network with all computers and servers on the same subnet. Agency B in this diagram is utilizing VLAN separation internally and also has its own Internet connection.
- Agencies connect back to RPB for resources



Post Transformation

- Post Transformation, each agency will have a degree of logical separation which will be honored all the way back to the data center ensuring agencies can access their assets but no one else can.
- Internet access will be collapsed providing fewer points of entrance
- Agencies connect back to the CESC for resources



Questions?



Guardian Edge - Encryption Plus

Don Kendrick

Senior Manager of Security Operations



NORTHROP GRUMMAN



SJR 51 Action Plan

Cathie Brown, CISM, CISSP

ISOAG Meeting

expect the best



SJR 51 Recommendation #1

- Develop a plan to communicate infrastructure information & standards to agencies that VITA supports.
- Provide assistance & expertise to agencies as they develop their information security programs.
- Assume responsibility for ensuring that the infrastructure meets the agency's needs & mitigate threats & vulnerabilities through Northrop Grumman's standards.



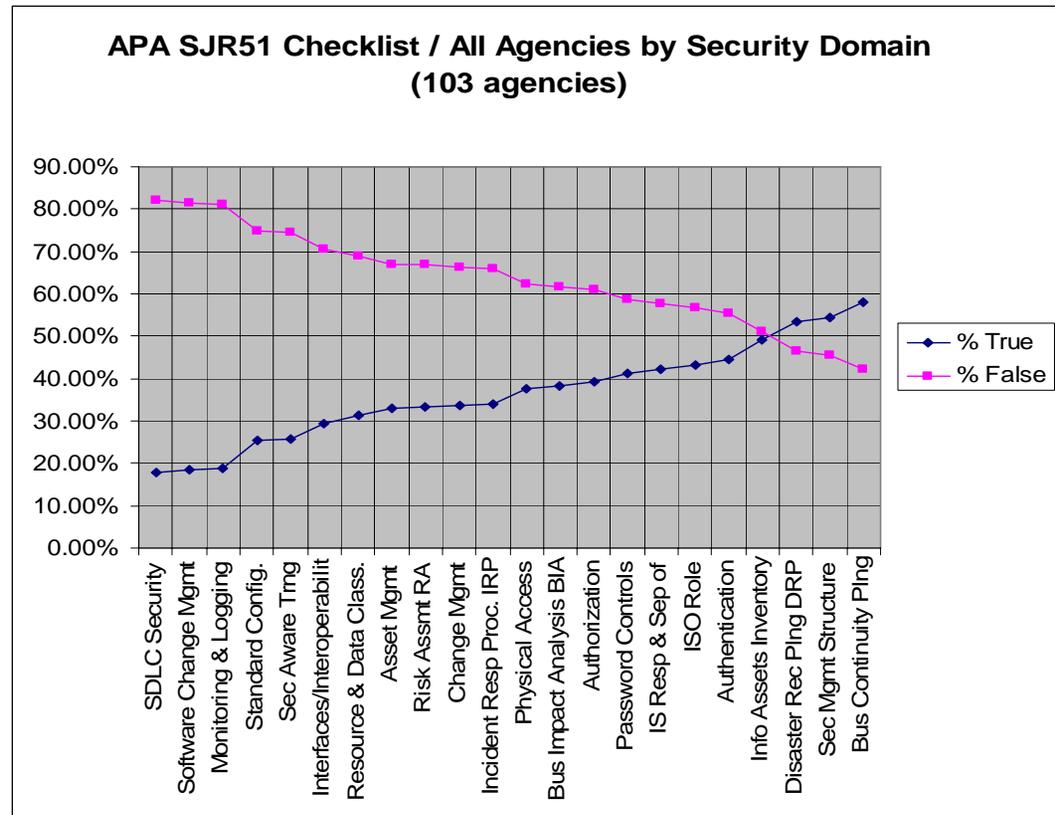
Action Plan

- Analyze SJR51 data to define areas of need
- Identify communication vehicles
- Promote COV Information Security:
 - Standards and Guidelines
 - Configuration Standards (CIS and NG)
 - Information Assurance Program
- Compliance with COV Information Security Standard (ITRM SEC501-01)

Data Analysis: Security Domains

Top 5 areas based on analysis of Security Domains

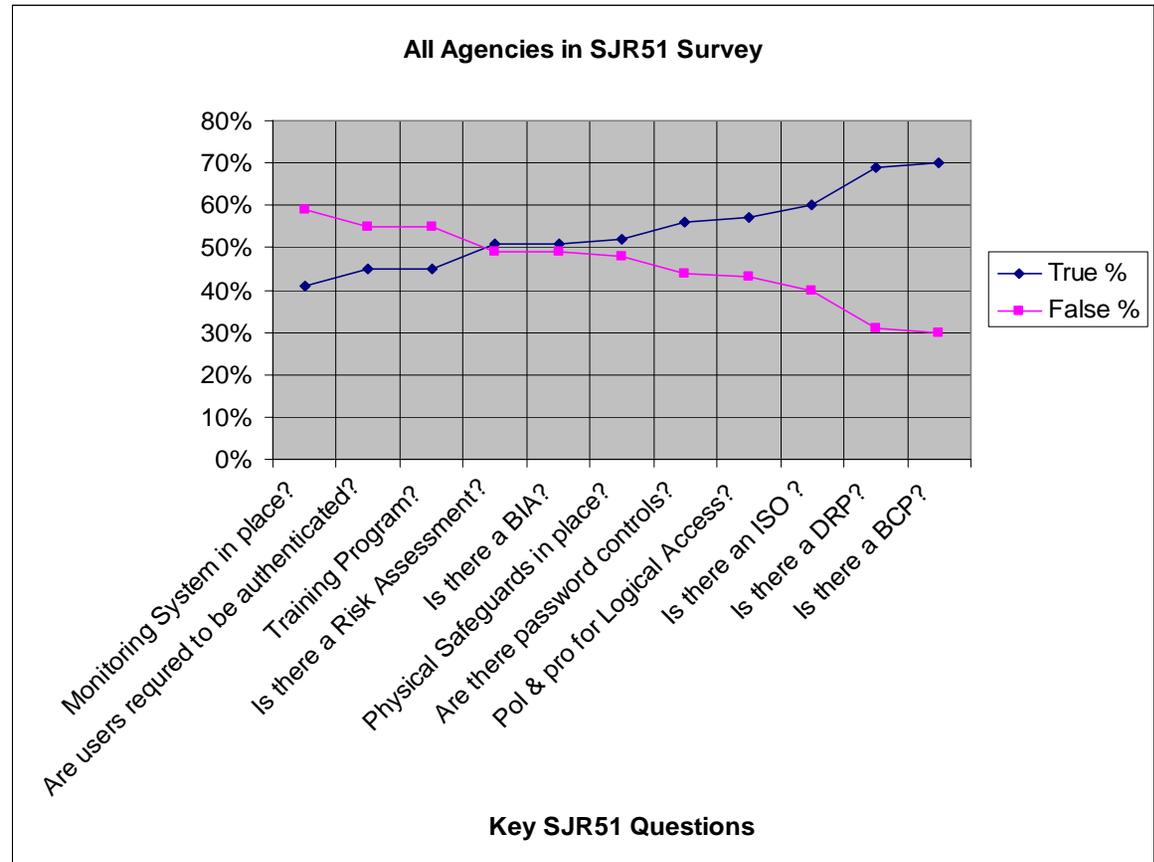
1. SDLC Security
2. Software Change Mgmt
3. Monitoring & Logging
4. Standard Config.
5. Security Awareness Training



Analysis: Key Questions

Top 5 areas based on key questions

1. Monitoring System?
2. Users required to authenticate?
3. Training Program?
4. Risk Assessment?
5. BIA?





Communication Vehicles

- ISOAG Meetings
- AITR Meetings
- New ISO Orientation
- Information Security Council
- CAM Small Agency Council
- Leadership Communique
- SoTech Communications



Promote COV Information Security

- Proposed schedule for Guidelines

| Guidelines | Publish on Web | Present at ISOAG Meeting |
|----------------------------------|----------------|--------------------------|
| Data Protection Guideline | Mar-07 | Apr-07 |
| Logical Access Control Guideline | Mar-07 | Apr-07 |
| Contingency Planning Guideline | Mar-07 | Apr-07 |
| Threat Management Guideline | Apr-07 | May-07 |
| System Security Guideline | Jun-07 | Jul-07 |
| Personnel Security Guideline | Jul-07 | Aug-07 |
| IT Security Audit Guideline | Sep-07 | Oct-07 |



Configuration Standards

- Center for Internet Security (CIS) configuration standards adopted
- 1,037 Windows servers tested from 24 agencies
- Focus remediation efforts on top 6 failures
 1. Interactive Logon Message
 2. Password History Enforced
 3. Account Lockout Duration Set
 4. Maximum Event Log Size Not Set
 5. Complex Passwords Not Set
 6. Minimum Password Length Not Set or Insufficient



NG Infrastructure Standards

| | In Compliance | Working On Plan to Comply | Exception Submitted |
|------------------------------|---------------|---------------------------|---------------------|
| Server Backup | 65 | 6 | 2 |
| Rotate Backup Tapes | 61 | 10 | 2 |
| User Passwords | 57 | 13 | 3 |
| Admin Passwords | 48 | 22 | 7 |
| OS Patches | 62 | 12 | 1 |
| Virus Patches | 65 | 11 | 1 |
| Test Server Restore | 33 | 21 | 25 |
| Network Monitoring Passwords | 62 | 13 | 2 |
| RAID Configuration | 40 | 32 | 2 |
| Enable Firewall on LT | 41 | 25 | 3 |
| | 63% | 19% | 6% |

- Currently meeting with SLDs individually on plans to bring agencies into compliance with standards



Information Assurance Program

- Collect information on sensitive systems
- Collect IT Security Audit Plans on sensitive systems
- Collect technical data on infrastructure
- Analyze current security controls
- Document recommendations, if any
- Provide letters of assurance to customer Agencies



Compliance with Information Security Standard

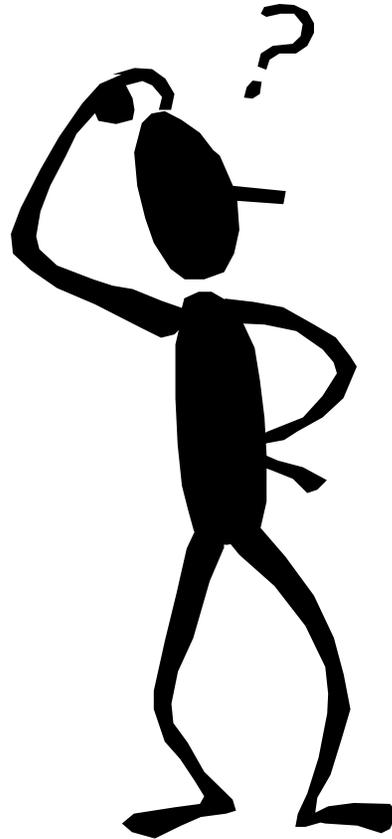
- Designate ISO & backup ISO
- Perform BIA
- Inventory & classify IT systems and data
- Perform Risk Assessment for sensitive systems
- Require IT Security Audits for sensitive systems
- Document and exercise contingency/DR plans
- Implement security configuration standards
- Incorporate IT security requirements in SDLC of IT applications
- Document formal account management practices
- Define appropriate data protection practices
- Safeguard the physical facilities
- Establish access control, security awareness training and acceptable use policies for personnel security
- Prepare for response to IT security incidents



Recommendation #3

- The CIO & ITIB should consider supplementing the Commonwealth's SEC 501 standard with the additional processes identified in this report.
- 15 processes identified
- Each process will be considered as the IT Security Standard is revised or as guidelines are published.

QUESTIONS





Virginia Information Technologies Agency

2007 General Assembly Session IT Legislation Update

Peggy Ward





Bills Failed

HB 1603S - Multiline telephone systems; owner or operator thereof ability to identify location from 9-1-1 call.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HB1603S1>

HB 2140/SB 1244 - Identity theft; notification of breach of information system.

<http://leg1.state.va.us/cgibin/legp504.exe?071+sum+HB2140>

<http://leg1.state.va.us/cgibin/legp504.exe?071+sum+SB1224>

HB 2306/SB 1342 - Public institutions of higher education; operational authority.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2306>

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB1342>

HB 2870 - Cellular phones; encouraged to program w/ICE #'s

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2870>



Bills Failed - Continued

HB 2973 - Unsolicited bulk electronic messages; changes scope of State's spam law

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB2973>

HB 3148 - Compromised Data Disclosure Act

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+HB3148>

SB 1123 - Auditor of Public Accounts; review security governmental databases containing personal information.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+SB1123>



Bills Passed

HB 1603S - Multiline telephone systems; owner or operator thereof ability to identify location from 9-1-1 call.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HB1603S1>

HB 1885 - Voice-over-Internet protocol service; revises definition.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HB1885ER>

HB 2196 - Chief Information Officer; powers and duties.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HB2196ER>

HB 2198 Electronic health records; requires those purchased by state agency to adhere to accepted standard.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HB2198ER>

HB 2946 - Chief Information Officer; powers and duties; information technology recycling.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HB2946ER>



Bills Passed - Continued

SB 845 - State agencies; Chief Information Officer to develop policies, etc. relating to security data.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+sum+SB845>

SB 1004 - Telecommuting; use of personal computers.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+SB1004ER>

SB 1111 - Freedom of Information Act; closed meetings and security of public buildings.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+SB1111ER>

HJ 587 - Internet Safety Month; designating as September 2007, and each succeeding year thereafter.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+HJ587E>



SB 1004 – SUBSTITUTE!

Telecommuting; use of personal computers.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+SB1004ER>

Telecommuting; use of personal computers. A. In accordance with the statewide telecommuting and alternative work schedule policy, to be developed by the Secretary of Administration pursuant to § [2.2-203.1](#), the head of each state agency shall establish a telecommuting and alternative work policy under which eligible employees of such agency may telecommute, participate in alternative work schedules, or both, to the maximum extent possible without diminished employee performance or service delivery. ... ***The policy shall promote use of Commonwealth information technology assets where feasible but may allow for eligible employees to use computers, computing devices, or related electronic equipment not owned or leased by the Commonwealth to telecommute, if such use is technically and economically practical, and so long as such use meets information security standards as established by the Virginia Information Technologies Agency, or receives an exception from such standards approved by the CIO of the Commonwealth or his designee.*** The policy shall be updated periodically as necessary. *Patron:* Devolites Davis



SB 1029 – SUBSTITUTE!

Chief Information Officer; to incorporate computer security into 4-year strategic plan.

<http://leg1.state.va.us/cgi-bin/legp504.exe?071+ful+SB1029ER>

Powers of the Chief Information Officer (CIO); information security. Requires the CIO of the Commonwealth to monitor trends in information security and incorporate computer security into the four-year strategic plan for information technology.

Patron: O'Brien



SB 1029 – SUBSTITUTE!

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\(3\)](#), limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions. Patron: O'Brien*



Virginia Information Technologies Agency

Other Business





Data Handling Standardization

- Work effort underway to provide standards for handling of data irrespective of form (electronic, paper, video, audio, etc.)
- First meeting was March 12
- Framework is in design & efforts of other states are being assessed.
- Freedom of Information Advisory Council was contacted.



Upcoming Events

Virginia Digital Government Summit

March 15, 2007 Richmond Marriott

<http://www.govtech.net/events/index.php/VirginiaDGS2007>



UPCOMING EVENTS!

ISOAG MEETING DATES

Wednesday, April 25, 2007

9:00 - 12:00 @ TBD

Tentative Agenda Items:

Executive Order 43 – Secretary Chopra

Telework – Karen Jackson (to be invited)

Remote Access – Chad Wirz

Information Security Council – Peggy Ward



Any other Topics?



ADJOURN

**THANK YOU FOR
YOUR TIME AND
THOUGHTS**

!!!