



Virginia Information Technologies Agency

# Information Security Officers Advisory Group Meeting

---

June 28, 2006

expect the best



## Information Security Officers Advisory Group

### Agenda

- |       |  |  |
|-------|--|--|
| I.    | Welcome                                | Peggy Ward   |
| II.   | IT Security Policy & Standards         | Peggy Ward   |
| III.  | Partnership Update                     | Fred Duball  |
| IV.   | Infrastructure Configuration Standards | Chris Saneda<br>Lance Higley<br>Dave Matthews<br>Ben Lehman<br>Craig Drain |
| V.    | Break                                  |  |
| VI.   | Information Security Template          | Chris Saneda   |
| VII.  | Future Meeting Topics                  | Peggy Ward   |
| VIII. | Questions and Answers                  | Peggy Ward   |



Virginia Information Technologies Agency

# Welcome

## **Peggy Ward**

Chief Information Security and Internal Audit Officer

---

Information Security Officers Advisory Group

June 28, 2006

**expect the best**



# IT Security Policy and Standards Update

**Peggy Ward**

Chief Information Security and Internal Audit Officer

---

Information Security Officers Advisory Group

June 28, 2006

expect the best



# Partnership Update

## **Fred Duball**

Director, Service Management Organization

---

Information Security Officers Advisory Group  
June 28, 2006

expect the best



***NORTHROP GRUMMAN***

---

Partnership Status  
Security Services Solution  
Presenter: Fred Duball

**June 28, 2006**

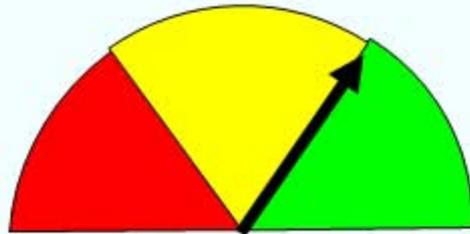


## **Agenda**

- **Partnership Status**
- **Security Solution**
  - **Current VITA / Agency Environment**
  - **Overview of NG IT Transformation (To-Be) Solution**
  - **How Transformation Projects will be Implemented**



# Program Dashboard for Week Ending 6/23/06



<i>Employee HR</i>	TimeSite Training Launched On and off boarding process underway.
<i>Current Operations (SDM)</i>	Completed last SCD Readiness Review. On schedule for SCD tasks. Continue to work Punchlist.
<i>Critical Milestones Transformation</i>	MPM loading and reviews of charters behind schedule impacted by SCD focus and budget re-plan, 3 projects in execution
<i>Financial Readiness CM</i>	Aggressive contract negotiations schedule. Uncertainty around MOU II and federal approval.

Risk Description	Potential Impact Description	Risk Mitigation Activities
------------------	------------------------------	----------------------------

Issue Description	Actual Impact Description	Resolution Activities
VITA financial systems modifications	Limited VITA financial reporting	Aggressively tackling VITA system changes
Contract negotiations schedule is aggressive	Assumed and Shared/Retained contracts not in place for SCD	VITA is focused on getting access rights for 1 Jul. NG focused on HW and Support. Both addressing Key Suppliers
MOU II and Federal Funding approval	Impacts RFS4SCD process and VITA system changes	FMS pursuing Federal approval. Proceeding as if approval received.



# Official Scorecard Based on Signed Offer Letters 6/23

Offer Type*	Total		Accept		Decline		No Response		Termed		
	Total	%	Count	%	Count	%	Count	%	Count	%	
Full Time	811	95.6%	524	64.6%	74	9.1%	197	24.3%	16	2.0%	
Part Time	1	0.1%	1	100.0%	0	0.0%	0	0.0%	0	0.0%	
Casual	36	4.2%	20	55.6%	0	0.0%	12	33.3%	4	11.1%	
<b>Total</b>	<b>848</b>	<b>100%</b>	<b>545</b>	<b>64.3%</b>	<b>74</b>	<b>8.7%</b>	<b>209</b>	<b>24.6%</b>	<b>20</b>	<b>2.4%</b>	
<b>Overall Acceptance Rate:</b>		<b>85%</b>									
Agency Name	Total		Accept		Decline		No Response		Termed		
	Total	%	Count	%	Count	%	Count	%	Count	%	
VITA Central	261	30.8%	150	57.5%	32	12.3%	73	28.0%	6	2.3%	
Department of Health	67	7.9%	36	53.7%	0	0.0%	20	29.9%	1	1.5%	
Department of Motor Vehicles	46	5.4%	23	50.0%	0	0.0%	21	45.7%	2	4.3%	
Department of Social Services	46	5.4%	33	71.7%	1	2.2%	11	23.9%	1	2.2%	
Department of Taxation	32	3.8%	23	71.9%	1	3.1%	8	25.0%	0	0.0%	
VA Department of Transportation	166	19.6%	126	75.9%	13	7.8%	24	14.5%	3	1.8%	
Other	230	27.1%	154	67.0%	17	7.4%	52	22.6%	7	3.0%	
<b>Total</b>	<b>848</b>	<b>100%</b>	<b>545</b>	<b>64.3%</b>	<b>64</b>	<b>7.5%</b>	<b>209</b>	<b>24.6%</b>	<b>20</b>	<b>2.4%</b>	
Mgmt Offers	Total		Accept		Decline		No Response		Termed		
	Total	%**	Count	%	Count	%	Count	%	Count	%	
	49	5.8%	30	61.2%	8	16.3%	10	20.4%	1	2.0%	
Years of VRS Service	Total	0 to 5	6 to 10	11 to 15	16 to 20	21 to 25	26 to 29	30+			
	Count	Count	Count	Count	Count	Count	Count	Count			
Total Count	848	215	170	94	96	76	96	101			
% of Population	100.0%	25.4%	20.0%	11.1%	11.3%	9.0%	11.3%	11.9%			
Accept Count	545	173	130	64	55	34	19	70			
% Accepted	64.3%	20.4%	15.3%	7.5%	6.5%	4.0%	2.2%	8.3%			
Decline Count	74	2	5	4	18	14	23	8			
% Decline	8.7%	0.2%	0.6%	0.5%	2.1%	1.7%	2.7%	0.9%			
No Response	209	31	29	26	23	28	50	22			
% No Response	24.6%	3.7%	3.4%	3.1%	2.7%	3.3%	5.9%	2.6%			
Termed	20	9	6	0	0	0	4	1			
% No Response	2.4%	1.1%	0.7%	0.0%	0.0%	0.0%	0.5%	0.1%			
*There are 4 in-scope employees on a Leave of Absence (LOA). The total in-scope count is 852. They will receive their offer when they return.											
**Percent of total population.											



## **Challenges In The Current VITA/Agency Environment**

- **Standardization of security system architecture and systems**
- **Conducting centralized management of security solutions**
- **Availability of full time security personnel to provide appropriate levels of accountability, responsibility, and reporting for all VITA supported agencies.**
- **Ensuring compliance with Code of Virginia 2.2-603.F that mandates agency director reporting of agency security incidents**
- **Ensuring security policy compliance**
- **Providing security metrics on the entire VITA enterprise**
- **Providing ability to audit security posture of the VITA enterprise**



## **Features of the Enterprise Security Services Solution**

- **Standardized Security Architecture**
- **Centralized management of security solutions**
- **Enterprise Security Operations Center (ESOC)**
- **Computer Security Incident Response Center (CSIRC)**
- **VITA Security Dashboard**
- **Vulnerability Assessment Program**



# Main Components of Enterprise Security Solution

## Assess and Protect

- Protection of confidentiality, availability, integrity, and physical security of information, information systems, and personnel
- Vulnerability assessments conducted by network scanning tools and human-generated analysis routines

## Support and Train

- Develop security awareness program
- Addresses all aspects of information assurance support and training
- Metrics used for continuous improvement

## Detect and Respond

- Use comprehensive threat management system to
  - Conduct forensic investigations
  - Manage incident response team activities
  - Establish security policy enforcement by finely tuning the firewalls and IDS / IPS
- Robust report generation

## Plan and Certify

- Ensure security policies and procedures are current
- Certify that security policies and procedures meet Commonwealth and Federal Government laws and directives



## **Enterprise Security Operations Center (ESOC)**

- **ESOC Located at the Southwest Enterprise Solutions Center (SWESC)**
- **Component of Northrop Grumman's CMOC Approach**
- **Delivers Real-Time, Proactive Monitoring**
  - 24x7 operations
  - Continually assesses and analyzes security posture of VITA enterprise
  - Defends Commonwealth from all activities classified as security events
  - Categorizes all events as either a threat or non-threat
- **ESOC Security Staff Duties**
  - Operate and maintain multiple systems including Enterprise IDS / IPS, Enterprise firewall management system, Enterprise vulnerability assessment system, and Enterprise logging system
  - ESOC personnel are cross-trained on CSIRC duties
- **If Determined to be an Active Incident**
  - ESOC escalates information to CSIRC for action and tracking



## **Computer Security Incident Response Center (CSIRC)**

- **CSIRC Located at the Commonwealth Enterprise Solutions Center (CESC)**
  
- **Assist the Commonwealth and Executive Branch Agencies to Comply with Code of Virginia § 2.2-603.F**
  
- **CSIRC Security Staff Duties:**
  - Responsible for all security incidents on 24x7 basis
  - Keep abreast of all industry advisories, such as US-CERT
  - Investigate security incidents, focusing on sequence, source and time of events
  - Audit logs and reports, and conduct forensic operations when necessary
  - Track, support and maintain user or machine reported incidents by entering the data into SITMS
  - CSIRC personnel are cross-trained on ESOC duties



# **Security Incident Tracking and Management System (SITMS)**

- **Single Repository of all VITA and Executive-Level Agency Security Incident Data**
  - Utilized for security incident management and remediation tracking from both machine and user-generated incidents
  
- **SITMS Database Resides on Security Storage Area Network (SAN) Located in CESC and SWESC**
  
- **SITMS is Primary Producer of Metrics**
  - Extracted for use in the VITA Security Dashboard
  - Output to appropriate personnel in report format



# **Enterprise Vulnerability Assessment System (EVAS)**

## **EVAS is a Solution Comprised of Two Subcomponents**

### **■ Component 1 – Distributed Architecture**

- Utilizes functionality of agents installed on desktops and servers to perform assessments, report deficiencies for known vulnerabilities and compliance to security policy configurations
- Assessments provide detailed compliance enforcement information, and include antivirus compliance, patch level compliance, presence of unknown hardware / software, and firewall status

### **■ Component 2 – Patch Management Platform**

- Information, such as software vendor and US-CERT alerts, is relayed to the patch management system
- Patch Management System actions generate automatic patch or configuration update, as well as report generation

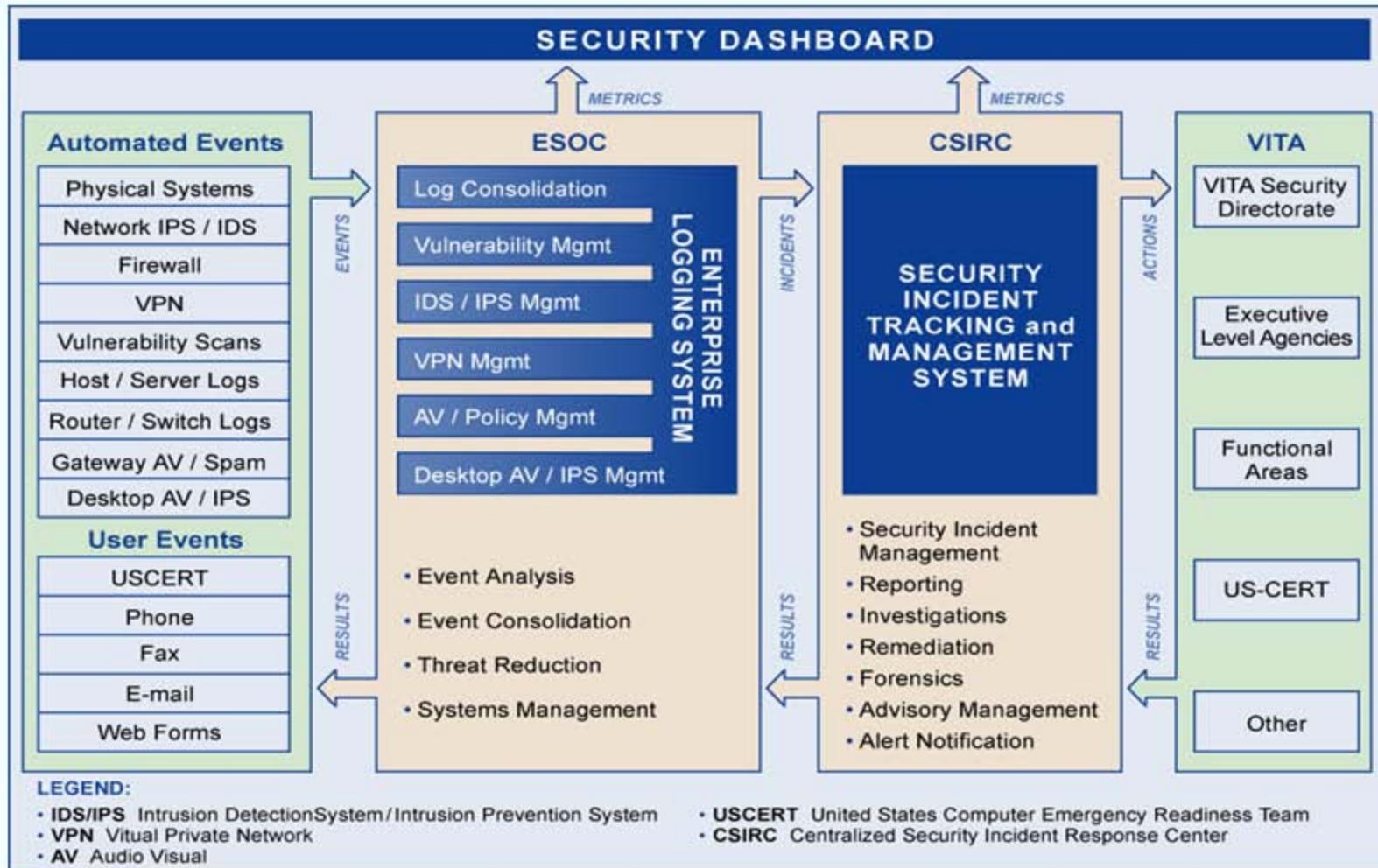


## **VITA Security Dashboard**

- **Single interface into the current security posture at any given point in time**
- **Web-accessible metric reporting capability**
- **Real-time security posture information**
- **Role-based, need-to-know access control that provides logical separation of security event information.**
  - VITA Security Directorate, executive branch agency security officers, system administrators, and other approved personnel
- **Report generation and print capabilities when needed**



# Security Services Transformation Information Flow



VITA 026\_r4



# Infrastructure Configuration Standards

**Chris Saneda**

Director, Customer Services

---

Information Security Officers Advisory Group

June 28, 2006

expect the best



## Overview – Infrastructure Configuration Standards

- Established configuration standards for most common equipment
- Striving to establish 'usable' standards
  - 1st draft based on NSA/CIS/NIST standards
    - Thorough, but too burdensome to implement
  - Settled on Center for Internet Security guideline
    - User driven organization - CIS Benchmarks are developed by teams of IT security experts from public, private, & academic sectors.
    - VITA is pursuing membership
- CIS has automatic assessment tools available for of 9 of 18 platforms for which VITA has adopted the CIS benchmark
  - Tool generates detailed assessment reports
  - Agency will review reports for mitigation or request exception
- Tools have been run at VITA Data Center
  - Pilot conducted with TAX and DMHRMRSAS location
- VITA has developed four benchmarks for platforms not covered by CIS at this time.



# CIS Benchmark for UNIX

**Lance Higley**

UNIX IT Specialist

---

Information Security Officers Advisory Group

June 28, 2006

expect the best



## CIS Benchmark for UNIX

- History – Before CIS
- Implementation
- Description of the scoring tool
- How we use the scoring tool
- Benefits
- Futures



## CIS Benchmark for UNIX

**Solaris Benchmark v1.3.0**

**June 17, 2004**

Copyright 2001-2004, The Center for  
Internet Security (CIS)

<http://www.CISecurity.org/>

## CIS Benchmark for UNIX

- History – Before CIS
  - Followed SANS Top 10 security threats
  - Installed security tools
    - tripwire, ssh, crack, sudo, tcp wrappers
  - Monthly account activity reports
  - UNIX server security policy
  - Configuration checklist from VT



## CIS Benchmark for UNIX

- Implementation
  - Began installing CIS scoring tool mid-2003
  - Phased implementation complete early 2004
  - Solaris and HP-UX servers
  - Currently running on 60+ UNIX servers

## CIS Benchmark for UNIX

- Description of the scoring tool
  - Download from CISecurity.org
  - Compressed shell archive containing
    - Solaris Benchmark PDF document
      - 78 pages of benchmark descriptions
      - 9 sections containing individual items
    - Scoring software package
      - Host based tool installed on each server



## CIS Benchmark for UNIX

- Contents of Solaris Benchmark PDF
  1. Patches and Additional Software
  2. Minimize inetd network services
  3. Minimize boot services
  4. Kernel Tuning
  5. Logging
  6. File/Directory Permissions/Access
  7. System Access, Authentication, and Authorization
  8. User Accounts and Environment
  9. Warning Banners

## CIS Benchmark for UNIX

- Contents of Solaris Benchmark PDF

- 1 Patches and Additional Software

- 1.1 Apply latest OS patches
- 1.2 Install TCP Wrappers
- 1.3 Install SSH

- 2 Minimize inetd network services

- 2.1 Disable standard services
- 2.2 Only enable telnet if absolutely necessary
- 2.3 Only enable FTP if absolutely necessary
- 2.4 Only enable rlogin/rsh/rcp if absolutely necessary
- 2.5 Only enable TFTP if absolutely necessary
- 2.6 Only enable printer service if absolutely necessary

# CIS Benchmark for UNIX

## 2.1 *Disable standard services*

### **Action:**

<script that disables standard services>  
<removed here>

### **Discussion:**

The stock `/etc/inet/inetd.conf` file shipped with Solaris contains many services which are rarely used, or which have more secure alternatives. Indeed, after enabling SSH (see Item 1.3) it may be possible to completely do away with all `inetd` based services, since SSH provides both a secure login mechanism and a means of transferring files to and from the system. In fact, the actions above will disable all standard services normally enabled in the Solaris `inetd.conf` file. The rest of the actions in this section give the administrator the option of re-enabling certain services.

## CIS Benchmark for UNIX

### ***2.2 Only enable telnet if absolutely necessary***

#### **Question:**

*Is there a mission-critical reason that requires users to access this system via telnet, rather than the more secure SSH protocol?*

If the answer to this question is yes, proceed with the action below.

#### **Action:**

```
sed 's/^#telnet/telnet/' inetc.conf >inetc.conf.new  
mv inetc.conf.new inetc.conf
```

#### **Discussion:**

*telnet* uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system.

# CIS Benchmark for UNIX

## 4.6 Use better TCP sequence numbers

### Action:

```
cd /etc/default  
awk '/TCP_STRONG_ISS=/ { $1 = "TCP_STRONG_ISS=2" }; \\  
{ print }' inetinit > inetinit.new  
mv inetinit.new inetinit  
chown root:sys inetinit  
chmod 444 inetinit
```

### Discussion:

Setting this parameter in /etc/default/inetinit causes the system to use a better randomization algorithm for generating initial TCP sequence numbers. This makes remote session hijacking attacks more difficult, as well as any other network based attack that relies on predicting TCP sequence number information.

## CIS Benchmark for UNIX

- Description of the scoring tool
  - Support for Solaris, HP-UX, AIX, Red Hat Linux, SUSE Linux, Slackware Linux
  - Host Based
    - Installs on each server to measure
  - Standard pkgadd as root
  - Software installs into /opt/CIS
  - Run script /opt/CIS/cis-scan
  - Non-invasive reading of security attributes

## CIS Benchmark for UNIX

- Description of the scoring tool
  - Results in cis-ruler-log.<date/time stamp >
    - cis-ruler-log.20060101-01:00:01.3235
  - Log contains both positive and negative log entries
  - Section numbers in the log correspond to the section numbers in the Solaris Benchmark PDF document

## CIS Benchmark for UNIX

- Sample Contents of Log

\*\*\* CIS Ruler Run \*\*\*

Starting at time 20060601-01:00:01

Positive: 1.1 System appears to have been patched within the last month.

Positive: 1.2 All inetd-based services are wrapped with TCP Wrappers

Positive: 1.3 SSH client and server are configured well.

Positive: 2.1 inetd is not listening on any of the miscellaneous ports checked in this item.

Negative: 2.2 telnet not deactivated.

Positive: 2.3 ftp is deactivated.

Positive: 2.4 rsh, rcp and rlogin are deactivated.

Ending run at time: Thu Jun 1 02:51:11 2006

Final rating = 7.73 / 10.00



## CIS Benchmark for UNIX

- Sample Contents of Log

\*\*\* CIS Ruler Run \*\*\*

Starting at time 20060601-01:00:01

Positive: 1.1 System appears to have been patched within the last month.

Positive: 1.2 All inetd-based services are wrapped with TCP Wrappers

Positive: 1.3 SSH client and server are configured well.

Positive: 2.1 inetd is not listening on any of the miscellaneous ports checked in this item.

Negative: 2.2 telnet not deactivated.

Positive: 2.3 ftp is deactivated.

Positive: 2.4 rsh, rcp and rlogin are deactivated.

Ending run at time: Thu Jun 1 02:51:11 2006

Final rating = 7.73 / 10.00

## CIS Benchmark for UNIX

### ***2.2 Only enable telnet if absolutely necessary***

#### **Question:**

*Is there a mission-critical reason that requires users to access this system via telnet, rather than the more secure SSH protocol?*

If the answer to this question is yes, proceed with the action below.

#### **Action:**

```
sed 's/^#telnet/telnet/' inetc.conf >inetc.conf.new  
mv inetc.conf.new inetc.conf
```

#### **Discussion:**

*telnet* uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system.

## CIS Benchmark for UNIX

- How we use the scoring tool
  - Checklist for new server installations
  - Simple to schedule with cron
    - `cis-ruler-log.20060101-01:00:01.3235`
    - `cis-ruler-log.20060201-01:00:00.7449`
    - `cis-ruler-log.20060301-01:00:00.21903`
    - `cis-ruler-log.20060401-01:00:01.20618`
    - `cis-ruler-log.20060501-01:00:00.24184`
    - `cis-ruler-log.20060601-01:00:01.24773`
  - Filtering out the positive with `grep`

## CIS Benchmark for UNIX

- Select only negative log entries
  - `grep "Negative" /opt/CIS/cis-ruler-log.20060101-01:00:01.3235`

### Sample Contents of Negative Entries in Log

Negative: 2.2 telnet not deactivated.

Negative: 3.3 inetd is still active.

Negative: 3.18 Web server not deactivated.

Negative: 3.19 SNMP daemon should be deactivated.

Negative: 7.9 Non-root accounts are in cron.allow.

Negative: 7.9 Non-root accounts are in at.allow.

## CIS Benchmark for UNIX

- Benefits of the benchmark
  - Detailed discussion of each security item and remediation steps
  - Comparison to industry standard security settings
  - Based on recognized best practices for configuration and operation
  - Widely accepted and reflects the consensus of expert users



## CIS Benchmark for UNIX

- Futures
  - Apache, Oracle, Linux benchmarks
  - Next Generation (NG) tool
  - Integration with commercial security assessment and security management software



## CIS Benchmark for UNIX

- Next Generation Tool (NG)
  - Version 2 supports Solaris 10
  - Java based
  - HTML formatted Report Files



# CIS Benchmark for UNIX

## Summary

Computer Name: testserver

Benchmark: The CENTER for INTERNET SECURITY Solaris Benchmark v2.0 (Solaris 10)

Scan Time: 04/27/2006 14:56:47

| Description   | Items     |           | Score         |        |
|---|-----------|-----------|---------------|--------|
|   | Passed    | Failed    | Actual        | Max    |
| 1 <u>Patches and Additional Software</u>                  | 1         | 0         | 12.500        | 12.500 |
| 2 <u>Minimize System Services</u>                         | 26        | 5         | 10.484        | 12.500 |
| 3 <u>Kernel Tuning</u>                                    | 1         | 5         | 2.083         | 12.500 |
| 4 <u>Logging</u>  | 5         | 4         | 6.944         | 12.500 |
| 5 <u>File/Directory Permissions/Access</u>                | 6         | 2         | 9.375         | 12.500 |
| 6 <u>System Access, Authentication, and Authorization</u> | 5         | 11        | 3.906         | 12.500 |
| 7 <u>User Accounts and Environment</u>                    | 6         | 7         | 5.769         | 12.500 |
| 8 <u>Warning Banners</u>                                  | 0         | 4         | 0.000         | 12.500 |
| <b>Overall Score:</b>                                     | <b>50</b> | <b>38</b> | <b>51.090</b> |        |

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.



# CIS Benchmark for UNIX

| 2 Minimize System Services  |        |
|---|--------|
| 2.1 <u>Establish Secure Baseline</u>  | Passed |
| 2.2 <u>Only enable RPC-based services if absolutely necessary</u>             | Passed |
| 2.3 <u>Only enable secure RPCs if absolutely necessary</u>                    | Passed |
| 2.4 <u>Only enable NIS server daemons if absolutely necessary</u>             | Passed |
| 2.5 <u>Only enable NIS client daemons if absolutely necessary</u>             | Passed |
| 2.6 <u>Only enable NIS+ daemons if absolutely necessary</u>                   | Passed |
| 2.7 <u>Only enable the LDAP cache manager if absolutely necessary</u>         | Passed |
| 2.8 <u>Only enable Kerberos server daemons if absolutely necessary</u>        | Passed |
| 2.9 <u>Only enable Kerberos client daemon if absolutely necessary</u>         | Passed |
| 2.10 <u>Only enable GSS daemon if absolutely necessary</u>                    | Passed |
| 2.11 <u>Only enable GUI if absolutely necessary</u>                           | Passed |
| 2.12 <u>Only enable Solaris Management Console if absolutely necessary</u>    | Failed |
| 2.13 <u>Only enable the volume manager if absolutely necessary</u>            | Passed |
| 2.14 <u>Only enable Windows-compatibility servers if absolutely necessary</u> | Passed |
| 2.15 <u>Only enable NFS server processes if absolutely necessary</u>          | Passed |
| 2.16 <u>Only enable rquotad if absolutely necessary</u>                       | Passed |
| 2.17 <u>Only enable NFS client processes if absolutely necessary</u>          | Passed |
| 2.18 <u>Only enable automount daemon if absolutely necessary</u>              | Passed |
| 2.19 <u>Only enable telnet if absolutely necessary</u>                        | Passed |
| 2.20 <u>Only enable FTP if absolutely necessary</u>                           | Passed |

# CIS Benchmark for UNIX

|   |                    |                |
|---|--------------------|----------------|
| <b>2.12 Only enable Solaris Management Console if absolutely necessary</b>  | <b>Check Type:</b> | <b>Status:</b> |
|   | OVAL5              | Failed         |
| <b>Description</b>  |                    |                |
| <p>The Solaris Management Console provides an easy-to-use administrative interface for common tasks. However, there is usually a trade-off between administrative convenience and security, so sites should consider disabling SMC and using the standard command-line administrative interfaces instead. Sites that are interested in simplified administration tools may also wish to investigate the Open Source Webmin administrative interface, which is now provided in /usr/sfw (see webmin(1M) in the /usr/sfw/man directory for more information).</p> |                    |                |
| <b>2.13 Only enable the volume manager if absolutely necessary</b>  | <b>Check Type:</b> | <b>Status:</b> |
|   | OVAL5              | Passed         |
| <b>Description</b>  |                    |                |
| <p>The Solaris volume manager automatically mounts CD-ROMs and floppy disks for users whenever a disk is inserted in the local system's drive (the mount command is normally a privileged command). Be aware that allowing users to mount and access data from removable media drives makes it easier for malicious programs and data to be imported onto your network.</p>   |                    |                |

## CIS Benchmark for UNIX

### 2.12 Only enable Solaris Management Console if absolutely necessary

#### Question:

*Is the Solaris Management Console used on this system for administrative tasks?*

If the answer to this question is yes, proceed with the actions below.

#### Action:

```
awk '$3 ~ /.NOS90wbem/ { $t = $2; $2 = $3; $3 = $t }
$3 ~ /.NOS90webconsole/ { $t = $2; $2 = $3; $3 = $t }
{ print }' /var/svc/profile/upgrade \
>/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

#### Discussion:

**The Solaris Management Console provides an easy-to-use administrative interface for common tasks. However, there is usually a trade-off between administrative convenience and security, so sites should consider disabling SMC and using the standard command-line administrative interfaces instead.**



## CIS Benchmark for UNIX

- Futures
  - **Integration with commercial security assessment and security management software**
  - **CIS Security Software Certifications**
    - Altiris**
    - Belarc, Inc.**
    - BladeLogic**
    - Cisco**
    - Elemental Security**
    - NetIQ Corporation**
    - Scalable Software**
    - Symantec**

# CIS Benchmark for UNIX

- For more information

[www.CISecurity.org/](http://www.CISecurity.org/)



The screenshot shows the website for the Center for Internet Security (CIS). The header includes the CIS logo and the text 'the CENTER for INTERNET SECURITY'. Navigation links include HOME, WHAT'S NEW, WHAT IS CIS?, BENCHMARKS/TOOLS, OTHER RESOURCES, JOIN US, TESTIMONIALS, and FAQ. A sidebar on the left contains links for 'Members Site', 'Become a CIS member!', 'CIS Members Worldwide', and 'Find Out How To Get Involved!'. The main content area features a red banner for 'CIS Benchmarks/Scoring Tools Now Available, Free of Charge!' and a table of operating systems. A yellow box on the right highlights that CIS members receive scoring tools with added features. Below that is an 'ANNOUNCEMENTS' section with a link to a June 12th, 2006 announcement about a new benchmark for Novell eDirectory 8.7.

**the CENTER for INTERNET SECURITY**

**CIS Benchmarks/Scoring Tools Now Available, Free of Charge!**

**Operating Systems**

| Benchmark                       | Version | Updated    |
|---------------------------------|---------|------------|
| Windows XP Professional SP1/SP2 | 2.01    | 09/09/2005 |
| Windows Server 2003             | 1.2     | 10/25/2005 |
| Windows 2000 Professional       | 2.2.1   | 12/17/2004 |
| Windows 2000 Server             | 2.2.1   | 12/17/2004 |
| Windows 2000                    | 1.2.2   | 02/04/2005 |

**ANNOUNCEMENTS**

June 12th, 2006 - CIS releases new Benchmark for Novell eDirectory 8.7. [Click Here](#) for more information and to download the benchmark.



Virginia Information Technologies Agency

# CIS Benchmark for Windows

**Dave Matthews**

Windows Branch Manager

---

Information Security Officers Advisory Group  
June 28, 2006

expect the best



## CIS Benchmarks for Microsoft Products

- Windows XP SP1/SP2 v2.01
- Windows Server 2003 v1.2
- Windows 2000 Professional v2.2.1
- Windows 2000 Server v2.2.1
- Windows NT v1.05
- Exchange Server 2003 v1.0
- SQL Server 2000 v1.0



## CIS Benchmark for Windows 2003

- Versions
  - Graphical User Interface (GUI)
  - Command Line Interface (CLI)
- Requires Java
- The GUI version is available with and without Java
- CIS members can access the CLI version



## CIS Benchmark for Windows 2003

- Command Line Interface (CLI)
  - Enables scripting for deployment
  - Maximize Portability
  - Maximize Inoperability



# CIS Benchmark for Windows 2003

- Definitions
  - Benchmarks: Security settings specific to a version of the operating system or application
  - Profiles: Security settings specific to the role/function of the server in the context of environment
    - Legacy
    - Enterprise
    - Specialized Security



## CIS Benchmark for Windows 2003

- Profiles:
  - Legacy: Minimum security settings, mixed environment, application interoperability
  - Enterprise: Intended for servers that do not require interoperability with legacy systems
  - Specialized Security: Used when security is tantamount to functionality, performance, and interoperability



## CIS Benchmark for Windows 2003

- Using the tool...
  - Select “Benchmark”
  - Select “Profile”
  - Answer questions
    - Legacy (8)
    - Enterprise (9)
    - Specialized Security (12)
    - Note: Default values can be modified in XML file



## CIS Benchmark for Windows 2003

- What is checked
  - Service Packs and Hotfixes
  - Auditing and Account Policies
  - Security Settings
  - Additional Security Protection
  - Note: The number of attributes checked varies with the profile selected.



## CIS Benchmark for Windows 2003

- Reports
  - User: User name, Password Age, Password Expiration for the account that ran tool
  - Service: Version and CIS feedback information
  - Benchmark: Computer name, Profile Tested, Time Tested, and Score

# CIS Benchmark for Windows 2003

- Getting Help
  - Readme files
    - List known issues
    - Areas not checked
    - Version History
  - CIS Forums
  - VITA
    - CDROM with pre-packaged script



# CIS Assessment

**Ben Lehman**

Server Assessment Project Manager

---

Information Security Officers Advisory Group  
June 28, 2006

expect the best

## CIS Assessment

- Center for Internet Security (CIS) – [www.cisecurity.org](http://www.cisecurity.org)
  - VITA Embracing CIS Standards and Best Practices
  - Security Assessment Tools
- CIS Tools Cover
  - Windows 2000 & 2003,
  - Various Flavors of Linux & Unix
  - MAC OS X
  - **No Novell Coverage**



# CIS Assessment

- Process
  - CIS Assessment Tool
    - Windows – Script with JAVA Included
    - Users of Other OS's Download from CIS Web Site
  - Assessment Tool Generates Reports
    - Use CD's to Send Reports to VITA
    - Special email (Questions & Discussion Only)  
[CISAssessment@vita.virginia.gov](mailto:CISAssessment@vita.virginia.gov)
  - Exception & Mitigation Form
    - Each Failed Item Must be Documented
    - Acceptable Risk
    - Previously Unknown Risk



## CIS Assessment

- Time Frame for Assessment
  - Non-Windows Users Can Download Assessment Tool
  - CD With Run Scripts Mailed SLD's and LAC's
  - **Target - Run Within 45 Days of Receiving the CD**
- Return Dates
  - Send Assessment Reports to VITA on CD's
  - **Target – Submit Exception/Mitigation Forms Within 30 Days of Tests**
  - **Forms Should be Mailed, Not Emailed**
- Experience
  - VITA
  - Central State Hospital



Virginia Information Technologies Agency

# VITA Security Configuration Exception Process

**Craig Drain**

Department of Taxation Information Security Officer

---

Information Security Officers Advisory Group

June 28, 2006

expect the best



# VITA Security Configuration Exception Process

---

## Contact Information

**Craig Drain**

**TAX Information Security Officer**

**[craig.drain@tax.virginia.gov](mailto:craig.drain@tax.virginia.gov)**

**804-371-0279**



## VITA Security Configuration Exception Process

---

### Discussion Areas:

- **Why do we need security standards and exceptions?**
- **Windows Security Configuration Standards**
- **Unix Security Configuration Standards**
- **Completing the Exception Form**
- **Issues and Barriers to Implementing Security Configurations**
- **TAX Experiences/Lessons Learned/Future Direction**



## VITA Security Configuration Exception Process

---

Why do we need security standards and exceptions?

- **The need for measurable baselines to measure security posture**
- **The need to implement best practice security and to mitigate threats**
- **The need to close the gap between best practice baselines and practical security to mitigate threats**
- **The need to make internal and external audits more effective**



## VITA Security Configuration Exception Process

---

### Windows Security Configuration Standard

- **Testing (using VMWare technology) with established .inf templates individually applied on development and test workstations and servers - economies in template development**
- **Utilizing NSA .inf templates by device function and customizing where necessary**
- **Comparing against CIS benchmark templates**
- **Experiences/trials and tribulations**
  - **Null Sessions - breaks various Citrix applications**
  - **Some registry settings - break SMS 2000**



## VITA Security Configuration Exception Process

---

### UNIX Security Configuration Standard

- **Testing/Implementation not as easy as Windows**
- **Beginning an initiative to test security settings with Sun Solaris on VMWare**
- **Experiences/trials and tribulations**
  - **TCP Wrappers on custom protocols - PowerBuilder based applications/services**
  - **FTP not deactivated - conversion to SSH scripts**
  - **System Accounting/Kernel auditing - space constraints; performance degradation**



# VITA Security Configuration Exception Process

## Completing the Exception Form

### Risks to the Organization

- **Issue - defining exception standards/duration relative to threat and exception duration**
  - **TAX considering internal guidelines:**
- **None - Fix Immediately;**
  - **Exception Request-30 days or less depending on VITA staff availability**



### VITA Security Configuration Standard Exception Request Form

Date of Request: \_\_\_\_\_

Requester: \_\_\_\_\_ Agency \_\_\_\_\_ System Name: \_\_\_\_\_

Baseline Configuration not Implemented: \_\_\_\_\_  
(attach configuration checklist(s) or use additional forms as needed)

Risks to the Organization:

Business/Technical Justification for not implementing the Standard:

Approved \_\_\_\_\_ Date \_\_\_\_\_  
Agency Head or Designee

#### VITA Security Services Use Only

Approved \_\_\_\_\_ Date \_\_\_\_\_ Comments: \_\_\_\_\_

Director of Security Services \_\_\_\_\_ Date \_\_\_\_\_

#### Agency Request for Appeal Use Only

Approved \_\_\_\_\_ Comments: \_\_\_\_\_

Agency Head or Designee \_\_\_\_\_ Date \_\_\_\_\_

#### VITA Executive Office Use Only (Appeal)

Appeal Approved \_\_\_\_\_ Appeal Date \_\_\_\_\_ Comments: \_\_\_\_\_

CEO or Deputy CEO \_\_\_\_\_ Date \_\_\_\_\_



## VITA Security Configuration Exception Process

---

### Completing the Exception Form

#### Risks to the Organization

- **Potential Disruption of Service - High Threat Risk**
  - **Exception Request - 90 day or less depending on VITA staff availability**
- **Potential Disruption of Service - Low/Moderate Threat Risk**
  - **Exception Request - 180 day or less depending on VITA staff availability**
- **Known Immediate Disruption of Service - Low/Moderate Threat Risk**
  - **Exception Request - 180 day or less depending on VITA staff availability**
- **Known Immediate Disruption of Service**
  - **No long term solution**
  - **Permanent exception - other mitigating control measures need to be considered**



## VITA Security Configuration Exception Process

---

### Issues and Barriers to Implementing Security Configurations

- Business/Technical Justification for not Implementing Standard
  - **Explain the business justification in detail - responsibility to clearly describe in business terms the reason (e.g, disruption of filing season and disruption of making daily deposits to the bank)**
  - **Explain the the technical justification in detail - show actual errors and results of testing (e.g., failed communication error code on batch job stream)**



## VITA Security Configuration Exception Process

---

### TAX Experiences/Lessons Learned/Future Direction

- **Issues/Hurdles to Implementing Security Configurations and Documenting Exceptions**
  - **Lack of testing environment**
    - **Complex applications dispersed among various infrastructure platforms adequately mimicking production**
  - **Time and Resource Constraints**
    - **Bringing together agency developers, testers and partnering with VITA personnel to thoroughly test applications against security configuration baselines**
    - **Time necessary to orchestrate necessary personnel for baseline implementation and testing**
  - **Budget limitations**



## VITA Security Configuration Exception Process

---

**Questions or Comments?**



# Information Security Template for High Risk Areas and Data with Specific Security Needs

**Chris Saneda**

Director, Customer Services

---

Information Security Officers Advisory Group  
June 28, 2006

expect the best



## Purpose

- The template was distributed the first week in April 2006, its purpose is to:
  - Facilitate VITA's responsibility to assist the agency in assuring data is properly safeguarded.
  - Define confidentiality requirements for sensitive data; these requirements will be passed to Northrop Grumman to ensure they also comply with agencies' data security needs.
  - Reinforce correlation between the agencies' Business Impact Analysis/Risk Assessment and identification/safeguarding sensitive data.



## Next Steps

- Determine status of agencies that have not responded (22)
- Collect and associate technical infrastructure information with agency sensitive data
- Determine gaps between data security requirements and current capability
- Determine where procedures and/or infrastructure need to be enhanced
- Develop plan to mitigate gaps



## Associated Initiatives

- Create online tool for agency/VITA updates
- Coordinate effort with other initiatives such as enterprise DR, SAS70 reporting, IT Security Policy (ITRM SEC500-02) and IT Security Standard (ITRM SEC501-01)



## Agency Template Response

We are awaiting response from the following agencies. No response indicates there is no confidential information; Agency Head will be asked to sign a document indicating such.

Charitable Gaming Commission

Virginia Employment Commission

Department of Correctional Education

Dept. of Game and Inland Fisheries

Department of Emergency Management

Department of Criminal Justice Services

State Council of Higher Education for Virginia

Frontier Culture Museum of Virginia

Dept. of Rail & Public Transportation

Center for Behavioral Rehab, Virginia

Virginia School for the Deaf and the Blind at Staunton

Comprehensive Services for At-Risk Youth and Families

Virginia School for the Deaf & Blind & Multi-Disabled at Hampton

Department of Aviation

State Board of Elections

Innovative Technology Authority

Gunston Hall

Department of Military Affairs

Chippokes Farm Foundation

Council on Human Rights

VA War Memorial

Library of Virginia



# Future Meeting Topics

## **Peggy Ward**

Chief Information Security and Internal Audit Officer

---

Information Security Officers Advisory Group

June 28, 2006

**expect the best**



# Questions and Answers

## **Peggy Ward**

Chief Information Security and Internal Audit Officer

---

Information Security Officers Advisory Group

June 28, 2006

**expect the best**