Federal Desktop Core Configuration

presented by:
Stephen Quinn
National Institute of Standards and Technology

Agenda

- Federal Desktop Core Configuration History

- Security Content Automation Protocol Interlude

- SCAP and FDCC

- FDCC Web Site and Tools

- FDCC High Impact Settings and Frequently Asked Questions

OMB Deep Dive Working Group

Acknowledgements

- Office of Management and Budget
- US Air Force
- Microsoft
- National Institute of Standards and Technology
- Defense Information Systems Agency
- National Security Agency
- Department of Homeland Security

Federal Desktop Core Configuration

FDCC

- Common core Microsoft Windows configuration driven by OMB
- Leverage USAF Standard Configuration Desktop initiative
  - Deployed and tested across half a million Windows XP systems
- Based on the DISA, NSA, NIST, USAF, and Microsoft existing guidelines for securing Windows XP and Vista
- Includes applications beyond Operating System
  - Windows XP/Vista Firewall
  - Internet Explorer 7

OMB Memo M-07-11

Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR FOR MANAGEMENT

March 22, 2007

M-07-11

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson
Deputy Director for Management

SUBJECT: Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

To improve information security and reduce overall IT operating costs, agencies who have Windows XP ™ deployed and plan to upgrade to the Vista™ operating system, are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

The recent release of the Vista™ operating system provides a unique opportunity for agencies to deploy secure configurations for the first time when an operating system is released. Therefore, it is critical for all Federal agencies to put in place the proper governance structure with appropriate policies to ensure a very small number of secure configurations are allowed to be used.

DoD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista™ operating system, and to deploy standard secure desk tops for Windows XP™. Information is more secure, overall network performance is improved, and overall operating costs are lower.

Agencies with these operating systems and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008. Agencies are requested to submit their draft implementation plans by May 1, 2007 at fisma@omb.eop.gov. With your endorsement we will work with your CIOs on this effort to improve our security for government information. If you have questions about this requirement, please contact Karen Evans, Administrator, E-Government and Information Technology at (202)395-1181 or at fisma@omb.eop.gov.

Corresponding OMB Memo to CIOs:

• Requires, **"Implementing and automating enforcement of these configurations;"**

•"NIST has established a program to develop and maintain common security configurations for many operating systems and applications, and **the "Security Content Automation [Protocol]" can help your agency use common security configurations.** Additionally, NIST's revisions to Special Publication 800-70, "Security Configuration Checklist Program for IT Products," will provide your agency additional guidance for implementing common security configurations. For additional information about NIST's programs, please contact Stephen Quinn, at Stephen.Quinn@nist.gov."

OMB Memo M-07-18

Ensuring New Acquisitions Include Common Security Configurations

"The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista)."

"Applications designed for normal end users shall run in the standard user context **without elevated system administration privileges.**"

"The National Institute of Standards and Technology (NIST) and the Department of Homeland Security continue to work with Microsoft to establish a virtual machine to provide agencies and information technology providers' access to Windows XP and VISTA images. The images will be **pre-configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.** "

Producing an FDCC Virtual Machine Image

Implement FDCC settings on virtual machine images

Use SCAP to verify FDCC settings were implemented correctly

- Windows XP
- Windows Vista
- Windows XP Firewall
- Windows Vista Firewall
- Internet Explorer 7.0

Reconcile any "failed" SCAP tests

Record any exceptions
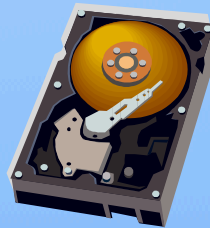
FDCC Virtual Machine Image
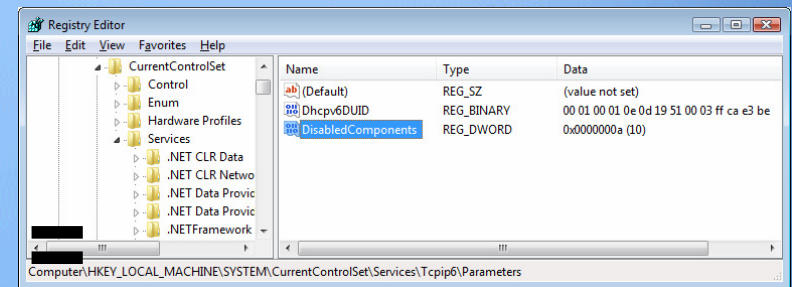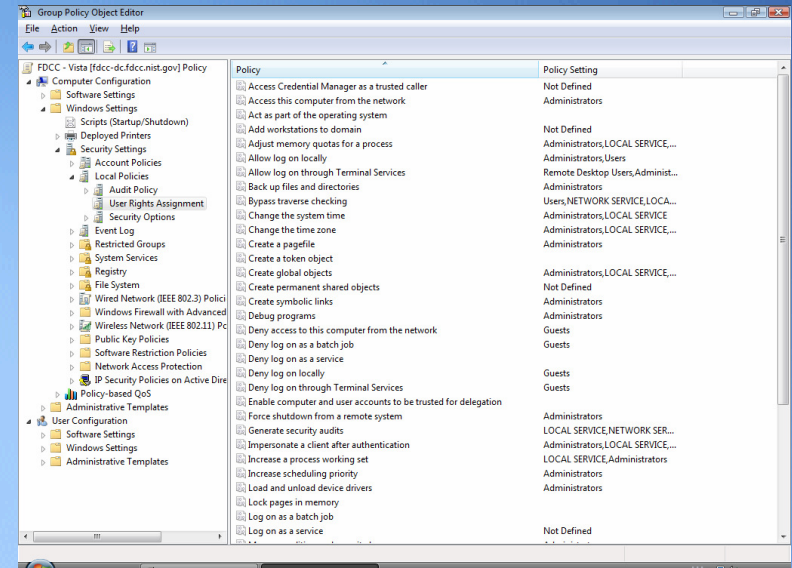
What is SCAP?

How

Standardizing the format by which we communicate

Protocol

CVE

OVAL
CVSS

SCAP

CPE

CCE

XCCDF
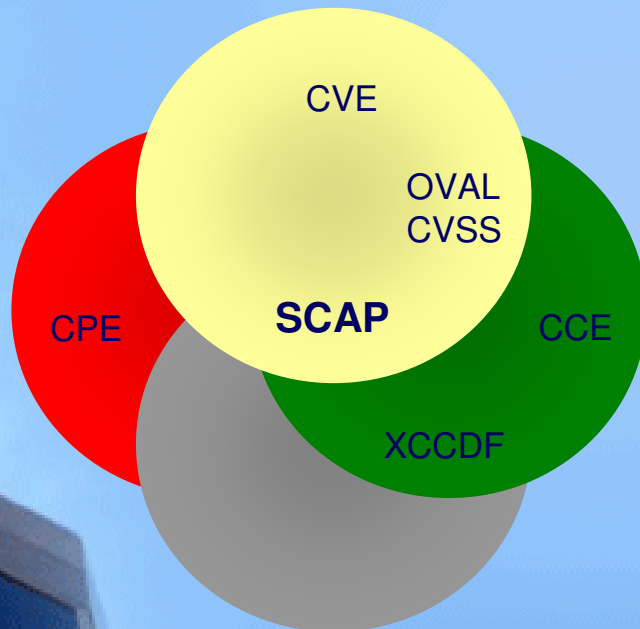
What

Standardizing the information we communicate

Content

Sponsored by
DHS National Cyber Security Division/US-CERT

National Vulnerability Database
a comprehensive cyber vulnerability resource

NIST
National Institute of
Standards and Technology

http://nvd.nist.gov

- 50 million hits per year
- 20 new vulnerabilities per day
- Mis-configuration cross references
- Reconciles software flaws from US CERT and MITRE repositories
- Produces XML feed for NVD content

Security Content Automation Protocol (SCAP)

Standardizing How We Communicate

MITRE	**CVE**	**Common Vulnerability Enumeration**	Standard nomenclature and dictionary of security related software flaws
MITRE	**CCE**	**Common Configuration Enumeration**	Standard nomenclature and dictionary of software misconfigurations
MITRE	**CPE**	**Common Platform Enumeration**	Standard nomenclature and dictionary for product naming
NATIONAL SECURITY AGENCY	**XCCDF**	**eXtensible Checklist Configuration Description Format**	Standard XML for specifying checklists and for reporting results of checklist evaluation
MITRE	**OVAL**	**Open Vulnerability and Assessment Language**	Standard XML for test procedures
FIRST	**CVSS**	**Common Vulnerability Scoring System**	Standard for measuring the impact of vulnerabilities

Cisco, Qualys, Symantec, Carnegie Mellon University

Existing Federal Content
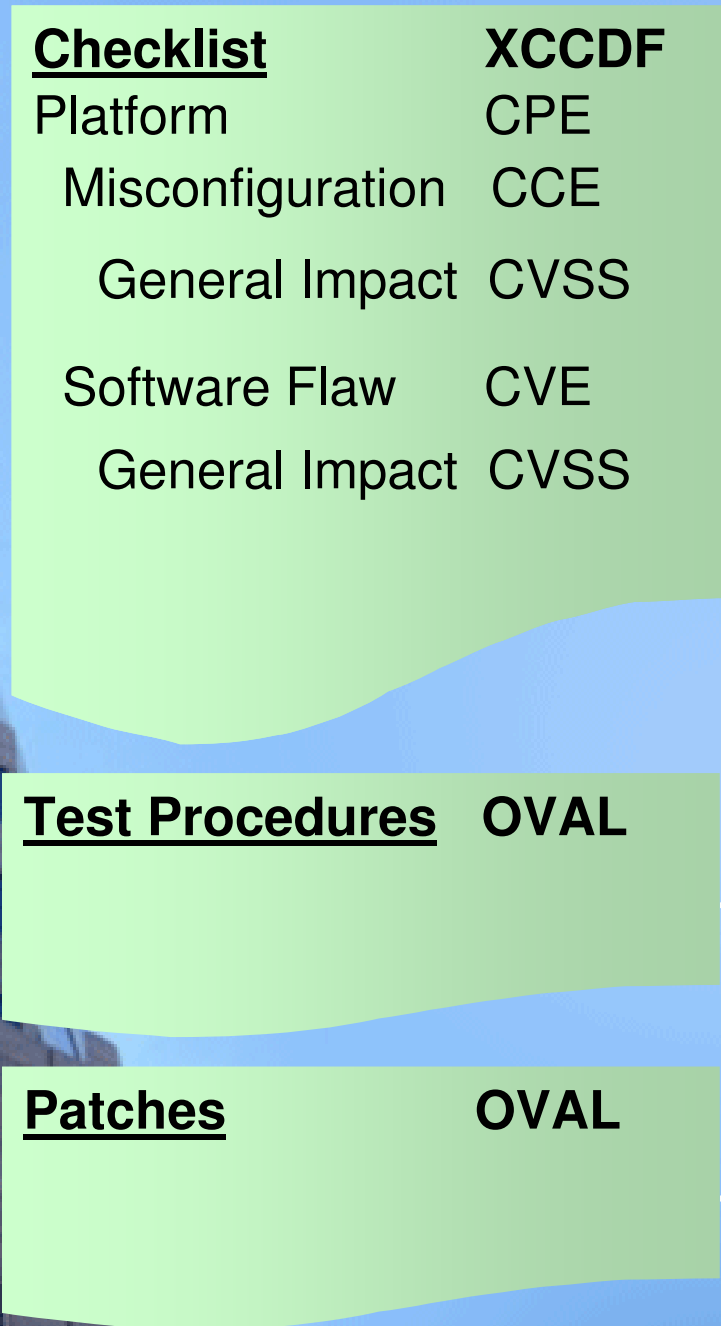## *Standardizing What We Communicate*

- In response to NIST being named in the Cyber Security R&D Act of 2002
- Encourages vendor development and maintenance of security guidance
- Currently hosts 112 separate guidance documents for over 125 IT products
- Translating this backlog of checklists into the Security Content Automating Protocol (SCAP)
- Participating organizations: DISA, NSA, NIST, Hewlett-Packard, CIS, ITAA, Oracle, Sun, Apple, Microsoft, Citadel, LJK, Secure Elements, ThreatGuard, MITRE Corporation, G2, Verisign, Verizon Federal, Kyocera, Hewlett-Packard, ConfigureSoft, McAfee, etc.

- Over 4 million hits per month
- About 20 new vulnerabilities per day
- Mis-configuration cross references to:
  - NIST SP 800-53 Security Controls (All 17 Families and 163 controls)
  - DoD IA Controls
  - DISA VMS Vulnerability IDs
  - Gold Disk VIDs
  - DISA VMS PDI IDs
  - NSA References
  - DCID
  - ISO 17799
- Reconciles software flaws from:
  - US CERT Technical Alerts
  - US CERT Vulnerability Alerts (CERTCC)
  - MITRE OVAL Software Flaw Checks
  - MITRE CVE Dictionary
- Produces XML feed for NVD content

How SCAP Works

Checklist   **XCCDF**

Platform   CPE

  Misconfiguration   CCE

   General Impact CVSS

  Software Flaw   CVE

   General Impact CVSS

Test Procedures   **OVAL**

Patches   **OVAL**

COTS/ GOTS Tools

Specific Impact CVSS
Results

Specific Impact CVSS
Results

Traceability within SCAP Checklists

Keyed on SP800-53
Security Controls

```
<Group id="IA-5" hidden="true">
  <title>Authenticator Management</title>
    <reference>ISO/IEC 17799: 11.5.2, 11.5.3</reference>
    <reference>NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10,
      15.1.11, 15.1.12, 15.1.13, 16.1.3, 16.2.3</reference>
    <reference>GAO FISCAM: AC-3.2</reference>
    <reference>DOD 8500.2: IAKM-1, IATS-1</reference>
    <reference>DCID 6/3: 4.B.2.a(7), 4.B.3.a(11)</reference>
</Group>
```

Traceability to Mandates

```
<Rule id="minimum-password-length" selected="false"
      weight="10.0">
    <reference>CCE-100</reference>
    <reference>DISA STIG Section 5.4.1.3</reference>
    <reference>DISA Gold Disk ID 7082</reference>
    <reference>PDI IAIA-12B</reference>
    <reference>800-68 Section 6.1 - Table A-1.4</reference>
    <reference>NSA Chapter 4 - Table 1 Row 4</reference>
    <requires idref="IA-5"/>
    [pointer to OVAL test procedure]
</Rule>
```

Traceability to Guidelines

Rationale for security
configuration

Federal Risk Management Framework

FIPS 199 / SP 800-60

SP 800-37 / SP 800-53A

Monitor
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness

Categorize
Information System

Define criticality / sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Select
Security Controls

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate
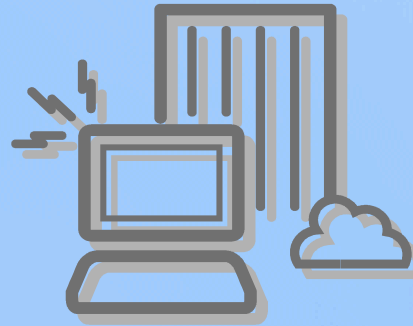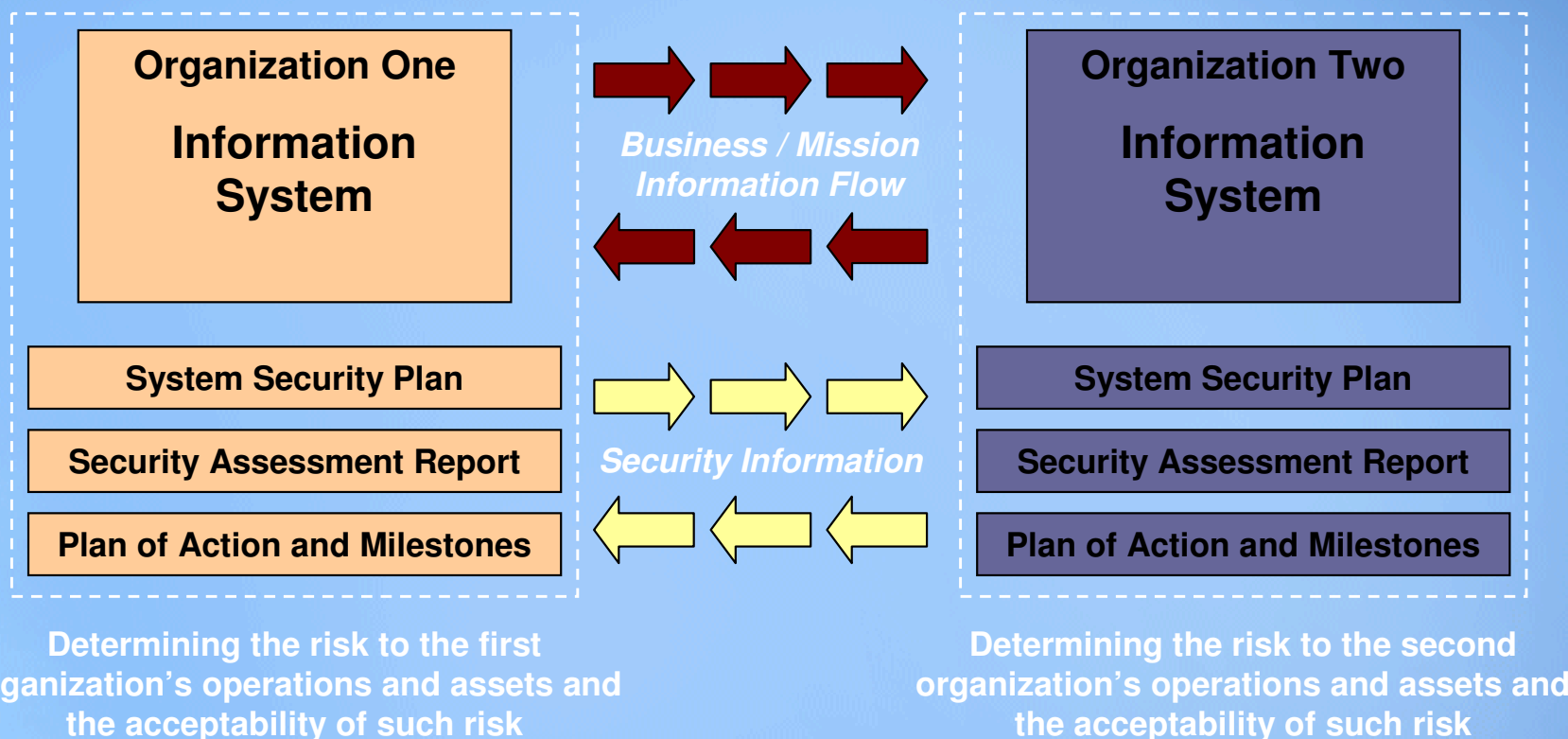
SP 800-37

Authorize
Information System

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-53 / SP 800-30

Supplement
Security Controls

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-53A

Assess
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-70

Implement
Security Controls

Implement security controls; apply security configuration settings

SP 800-18

Document
Security Controls

Document in the security plan, the security requirements for the information system and the security controls planned or in place

Controls with Automated Validation Support

Tool Set	Automation	Control Count	Control Percent	Control Example
Framework Tools	Full Automation	-	-	-
	Partial Automation	49	30%	PL-2 System Security Plan
Security Content Automation Protocol	Full Automation	31	19%	AC-11 Session Lock
	Partial Automation	39	24%	AC-8 System Use Notification
Future Automation Techniques or No Automation		44	27%	AC-1 Access Control Policy and Procedures
	Total Controls	163	100%	

Integrating IT and IT Security Through SCAP

Vulnerability Management

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System

CVE

Misconfiguration

OVAL
CVSS

Asset Management

CPE

SCAP

CCE

Configuration Management

XCCDF

Compliance Management

Security Visibility Among Business/Mission Partners

Organization One — Information System	Business / Mission Information Flow	Organization Two — Information System
System Security Plan	Security Information	System Security Plan
Security Assessment Report		Security Assessment Report
Plan of Action and Milestones		Plan of Action and Milestones

Determining the risk to the first organization's operations and assets and the acceptability of such risk

Determining the risk to the second organization's operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin…establishing levels of security due diligence and trust.

Stakeholder and Contributor Landscape: Industry
Product Teams and Content Contributors

Stakeholder and Contributor Landscape: Federal Agencies
SCAP Infrastructure, Beta Tests, Use Cases, and Early Adopters

DHS		**OMB**	
NSA		**IC**	
OSD		**DISA**	
DOJ		**EPA**	
Army		**NIST**	
DOS			

Producing an FDCC Virtual Machine Image

Implement FDCC settings on virtual machine images

Use SCAP to verify FDCC settings were implemented correctly

- Windows XP
- Windows Vista
- Windows XP Firewall
- Windows Vista Firewall
- Internet Explorer 7.0

Reconcile any "failed" SCAP tests

FDCC Virtual Machine Image

Record any exceptions
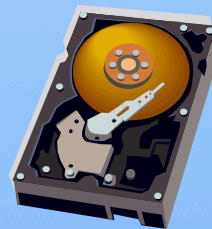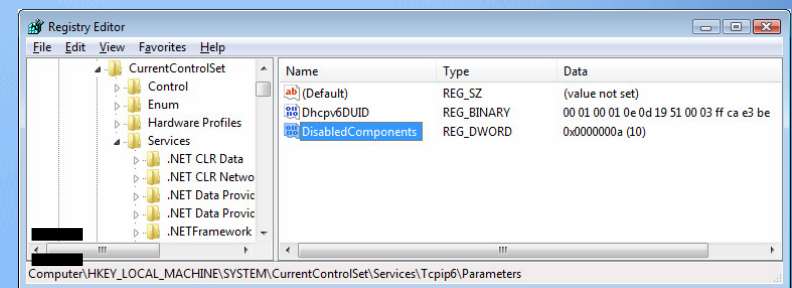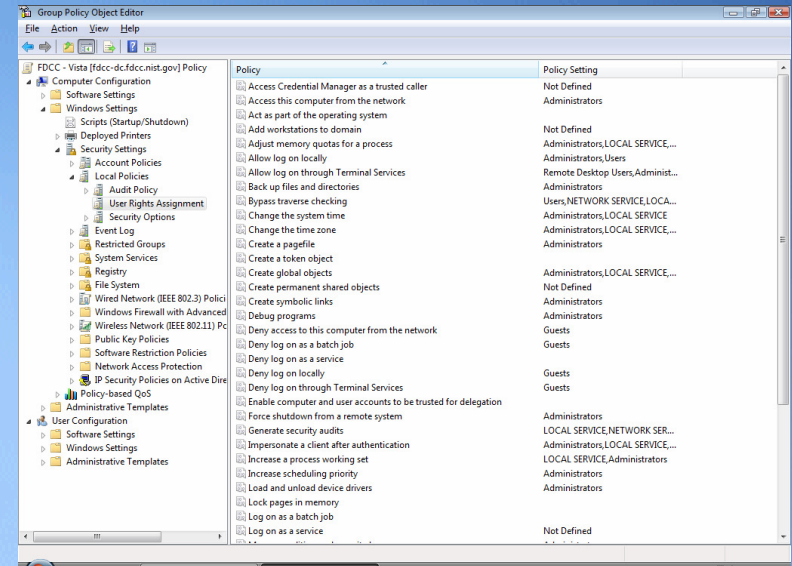
OMB 31 July 2007 Memo to CIOs

Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations

July 31, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
              Administrator, Office of E-Government and Information Technology

SUBJECT: Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations

The Office of Management and Budget recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008."

As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," a virtual machine would be established "to provide agencies and information technology providers' access to Windows XP and VISTA images." The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc. The website also includes frequently asked questions and other technical information for adopting the Federal Desktop Core Configurations (FDCC).

Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST's Security Content Automation Protocol (S-CAP) to help evaluate providers' self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations. Related resources (e.g., group policy objects) are also provided to help facilitate agency adoption of the FDCC.

For additional information about this initiative, please call 1-800-FED-INFO. Additional information about the S-CAP can be found at: http://nvd.nist.gov/scap.cfm.

"As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," **a virtual machine would be established "to provide agencies and information technology providers' access to Windows XP and VISTA images."** The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc."

"Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and **use NIST's Security Content Automation Protocol (S-CAP) to help evaluate providers' self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations."**
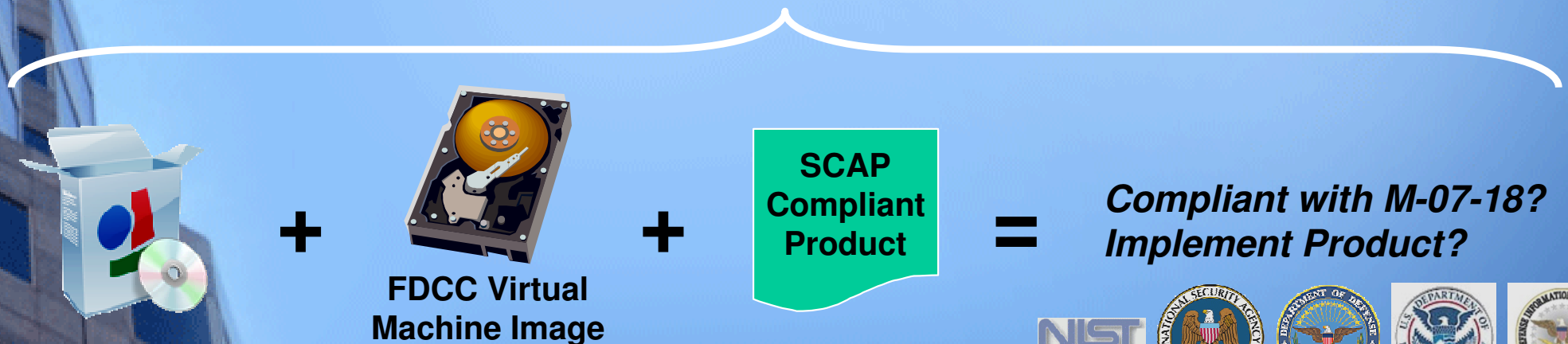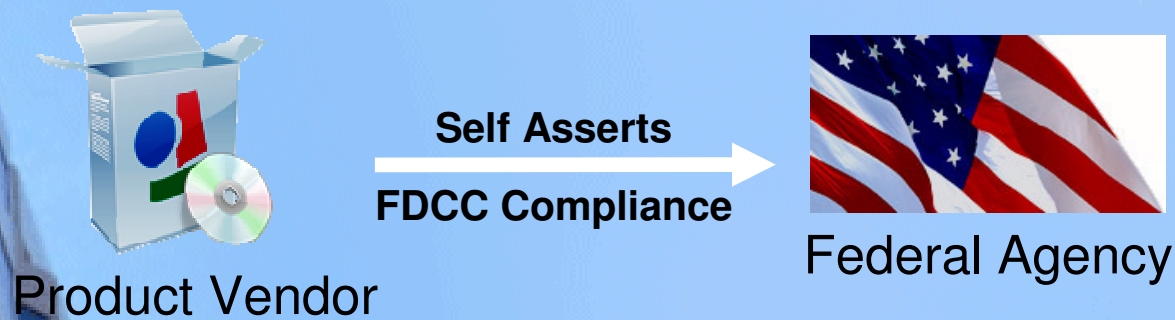
Accomplishing FDCC with SCAP

Operations Teams	Product Teams	Function
●	●	Test to ensure products do not change the FDCC settings
●		Assess new implementations for FDCC compliance
●		Monitor previous implementations for FDCC compliance
●		Generate FDCC compliance and deviation reports

Quote from OMB Memo *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*
"**Information technology providers** must use S-CAP validated tools, as they become available, to **certify their products** do not alter these configurations, and **agencies** must use these tools **when monitoring** use of these configurations. "

The Relationship Between FDCC and SCAP Product Compliance

http://fdcc.nist.gov

Frequently Asked Questions

Technical FAQs

This frequently asked questions (FAQ) document addresses subjects associated with the March 2007 OMB-mandated Federal Desktop Core Configuration (FDCC). Topics include the FDCC, laboratory testing of the FDCC, agency testing of the FDCC, use of the SCAP to evaluate computers for FDCC compliance, deploying the FDCC, and reporting deviations to the FDCC. This FAQ should be considered an addition to the Managing Security Risks Using Common Configurations FAQ.

Federal Desktop Core Configuration

1. **What is the Federal Desktop Core Configuration (FDCC)?**
   The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FD...
   operating system soft...
   Desktop Core Config...
   2007 memorandum fr...
   a corresponding mem...
   Chief Information Off...

2. **What operating sys...**
   Currently, FDCC setti...
   Pack 2) and Microsof...

3. **Where can I obtain...**
   systems other than...
   In general, NIST sugg...
   (SP) guide if one exist...
   not available, Federal ...
   (checklists.nist.gov) t...
   Defense Information ...
   guide that could be us...
   do not exist, Federal ...
   Regardless which guid...
   deployed information ...
   recommended checkli...

4. **How was the FDCC...**
   The Windows Vista F...
   Security Guides for b...
   Vista Security Guide ...
   NSA, and NIST. The ...
   DISA, NSA, and NIS...
   The Windows XP FD...
   Security-Limited Fun...
   DoD customization o...
   Internet Explorer 7.0.

FDCC Laboratory Testing

1. **What was the objective of the recent NIST test effort?**
   In support of OMB and Fede...
   DISA, Microsoft, and third-p...
   laboratory testing to verify a...
   written FDCC policy.

2. **What version of Microsof...**
   Internet Explorer 7.0 was tes...

3. **What if I use a browser ...**
   While settings for other brow...
   to use other Web browser so...
   7.0. If agencies are using Int...
   Internet Explorer 7.0.

4. **Were any Microsoft Offic...**
   Microsoft Office is not instal...
   included in GPOs. The Micro...
   represented in the FDCC doc...
   before laboratory testing. Mi...
   testing after publication of th...

5. **To comply with the FDC...**
   the Microsoft Windows F...
   No. The FDCC baseline reco...
   the Microsoft Windows Firev...
   system installation. However,...
   firewall software instead of t...

6. **Is Microsoft Defender an...**
   included in the FDCC set...

FDCC Agency Testing

1. **What are Virtual PCs (VPC), and what is the difference between a VPC and a Virtual Hard Disk (VHD)?**
   Virtual PC (VPC) is a Microsoft product that allows users to run a virtual instance of an opera...
   instance of an opera...
   (VHD) can utilize th...
   USB ports) in the sa...
   the VHD appears as ...

2. **Why are VHDs be...**
   VHDs are very usefu...
   can be installed on a...
   operating systems, V...
   the purposes of ensu...
   malfunctioned with t...
   over a single physica...

3. **When will VHDs e...**
   According to Micros...
   VHDs will be publish...
   http://csrc.nist.gov/f...

4. **What can be dow...**
   The FDCC technical ...
   policy documentatio...
   content files.

5. **Can I use the VHD...**

Security Content Automation Protocol

1. **What is SCAP?**
   NIST recently established a suite of interoperable and automatable security standards known as the Security Content Automation Protocol (SCAP). By virtue of using XML-ba...
   readable. Specific...
   host SCAP refere...
   http://nvd.nist.gov...

2. **How are the SC...**
   As part of the iter...
   that both VHDs a...
   and test complian...
   tools were able to...
   settings were pro...
   used for testing ...
   determine if newl...

3. **What settings ...**
   There are a small...
   at this time. Thes...

4. **Where can I ob...**
   FDCC SCAP con...

FDCC Deployment

1. **What are some settings that will impact system functionality that I should test before I deploy the OMB mandated FDCC baseline in an operational environment?**
   There are a number of settings that will impact system functionality and agencies should test thoroughly before they are deployed in an operational environment.

   - Running the system as a standard user - some applications may not work properly because they require administrative access to the operating system and application directories and registry keys.
   - Minimum 12 characters password and change every 60 days - this may impact system usability and interoperability with some enterprise single sign-on password management systems.
   - Wireless service - the wireless service is disabled and this will prevent the use of Wi-Fi network interfaces that depend on the built-in wireless service.
   - FIPS 140-2 setting - impacts browser interoperability with Web sites that do not support the FIPS 140-2 approved algorithms. This can usually be

http://fdcc.nist.gov/download_fdcc.html

Information Technology Laboratory - Computer Security Division
Computer Security Resource Center - CSRC

NIST
National Institute of
Standards and Technology

| Focus Areas | Publications | Site Map | Search |

Federal Desktop Core Configuration
FDCC

- DOWNLOAD PAGE -

FDCC
- Home
- Disclaimer
- Contact

NIST Resources
- NIST Security Configuration Checklist for IT Products
- Security Content Automation Protocol
- Guidance for Securing Microsoft Windows Vista
- Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
- Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
- NIST Systems Administration Guidance for Windows 2000 Professional
- FISMA Implementation Project
- National Vulnerability Database

WARNING NOTICE

Do not attempt to implement any of the settings without first testing them in a non-operational environment. These recommendations should be applied only to Windows XP Professional SP2 and Vista systems and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The security policies have been tested on Windows XP Professional SP2 and Vista systems with a Windows 2003 server and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003.

The draft download packages contain recommended security settings; they are not meant to replace well-structured policy or sound judgment. Furthermore, these recommendations do not address site-specific configuration issues. Care must be taken when implementing these settings to address local operational and policy concerns.

These recommendations were developed at the National Institute of Standards and Technology, which collaborated with DHS, DISA, NSA, USAF, and Microsoft to produce the Windows XP and Vista FDCC baseline. Pursuant to title 17 Section 105 of the United States Code, these recommendations are not subject to copyright protection and are in the public domain. NIST assumes no responsibility whatsoever for their use by other parties, and makes no guarantees, expressed or implied, about their quality, reliability, or any other characteristic. We would appreciate acknowledgement if the recommendations are used.

Download Packages

Please read the Download FAQ

| Documentation | GPOs | VHD Files | SCAP Content |

Documentation
2007.07.31
FDCC Documentation Release 1.0 - Draft [xls, 100K]

SHA-1 Digest:
2CB88444394B73E69EF41175897809A1232588A0

SHA-256 Digest:
D6ECF963F4D2FA4AB92BA79D1527768DDF5ACCC875872496DE4C4C23E283CD17

GPOs
2007.07.31
FDCC GPO Release 1.0 - Draft [zip, ~3 MB]

SHA-1 Digest:
B46C514BFABD312FA9C1AC149AFA04D2D15215FC

SHA-256 Digest:
682B097721E068170AD7CE883BC70045803FE6A00A8C97A60A194C13CEFCDA5C

VHD Files
2007.07.31
Windows XP FDCC VHD Release 1.0 (Click to download) - Draft [zip, ~1.8GB]

Note:
Internet Explorer 6 and 7 have a download limitation of 2 GB and 4 GB respectively. Other browsers do not appear to have this limitation.

SHA-1 Digest:
E50E4F3B40920D595FA0481B3AF7E72C76203249

SHA-256 Digest:
1F20C16989CF30B5187EA95CD07BA629CF18F0F41D89E87B8EC8DB9CD768858E

Windows Vista FDCC VHD Release 1.0 - (Click to download) - Draft [zip, ~4.5GB]

Note:
Internet Explorer 6 and 7 have a download

SCAP Content
2007.07.31
FDCC SCAP Content

Windows XP SP2

Windows XP Firewall

Internet Explorer 7.0

Windows Vista

Windows Vista Firewall

The preceding files are intended for use with "SCAP FDCC scanning capable" tools.

FDCC Security Settings

FDCC Security Settings

Group Policy Objects (GPOs)

Both

Vista

XP
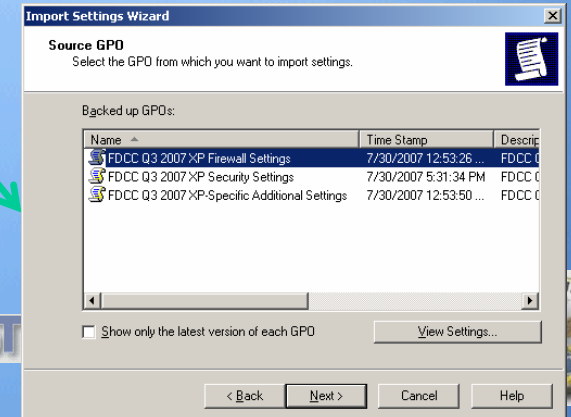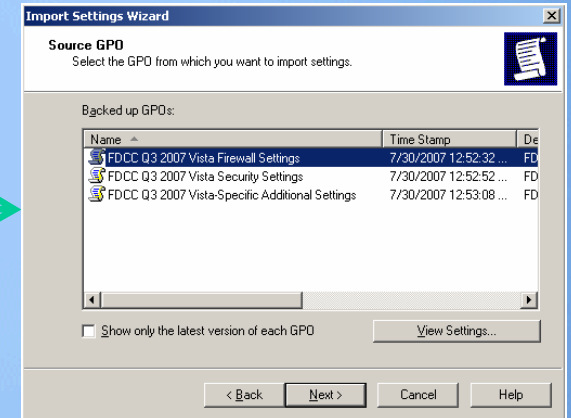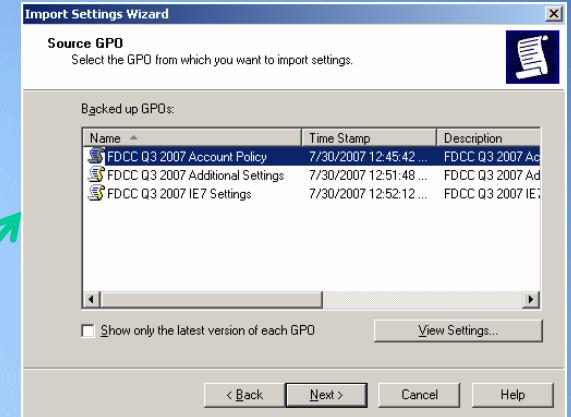
GPOs Test Environment

Windows Server 2003
- AD/DNS -
- GPOs -

Windows Vista
Client

Windows XP
Client

FDCC GPOs

Group Policy Management Console – gpmc.msc

Group Policy Object Editor – gpedit.msc

Download FDCC VHD Files

NTFS Disk Space Requirement:
Vista: 4.5 GB + 10 GB + Swap
XP: 1.8 GB + 3.5 GB + Swap

Vista FDCC VPC

1. Microsoft Virtual PC 2007
2. fdcc_admin
3. P@ssw0rd123456

SCAP Content

http://nvd.nist.gov/scapchecklists.cfm

Microsoft Windows Vista	SCAP-WinVista.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest	secure elements	ThreatGuard	Includes a Federal Desktop Core Configuration profile
Microsoft Windows XP Professional	SCAP-WinXPPro.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest	NIST National Institute of Standards and Technology	ThreatGuard	Includes a Federal Desktop Core Configuration profile. The FISMA compliance policies are complete. The DISA policies are substantial but still under development by Mitre.

Microsoft Windows Vista Firewall	SCAP-WinVistaFirewall.zip (v0.12) released 7/31/2007 SHA1 Digest SHA256 Digest	secure elements	Patches are located in the OSs zip files.	Includes a Federal Desktop Core Configuration profile
Microsoft Windows XP Firewall	SCAP-WinXPFirewall.zip (v0.18) released 7/31/2007 SHA1 Digest SHA256 Digest	secure elements	Patches are located in the OSs zip files.	Includes a Federal Desktop Core Configuration profile

Microsoft Internet Explorer Version 7.0	SCAP-IE7.zip (v0.95) released 7/31/2007 SHA1 Digest SHA256 Digest	MITRE	ThreatGuard	Includes a Federal Desktop Core Configuration profile

File Explorer window — SCAP-WinVista

Name	Date modified	Type	Size
SCAP-WinVista-CPE.xml	7/27/2007 7:17 PM	XML File	6 KB
SCAP-WinVista-OVAL-v90.xml	7/30/2007 9:00 AM	XML File	1,222 KB
SCAP-WinVista-Patches.xml	7/18/2007 12:12 PM	XML File	104 KB
SCAP-WinVista-XCCDF.xml	7/30/2007 7:03 PM	XML File	765 KB
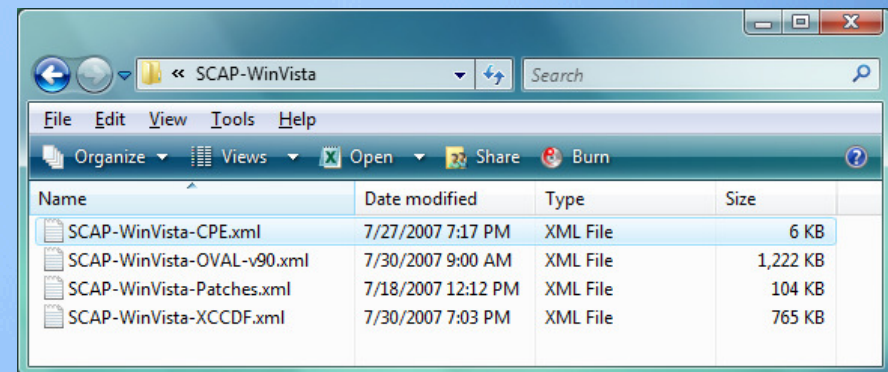
Verify and Test
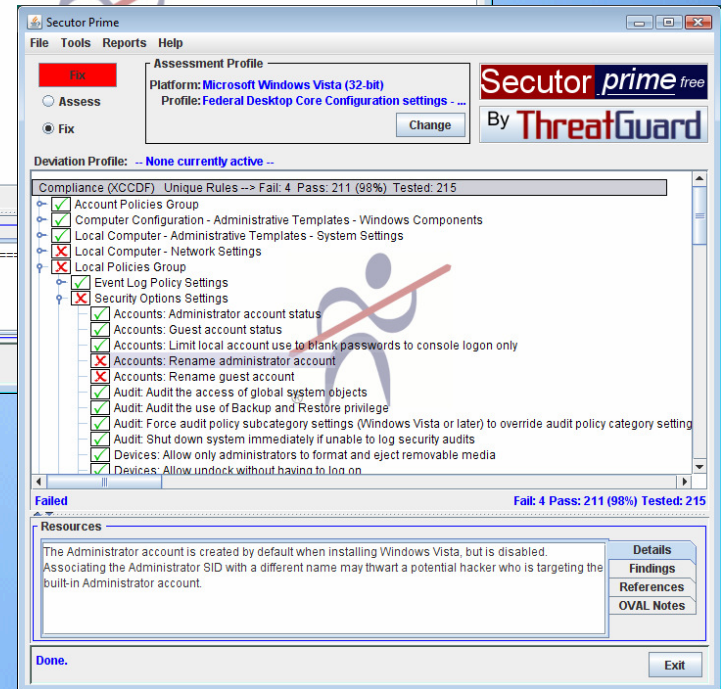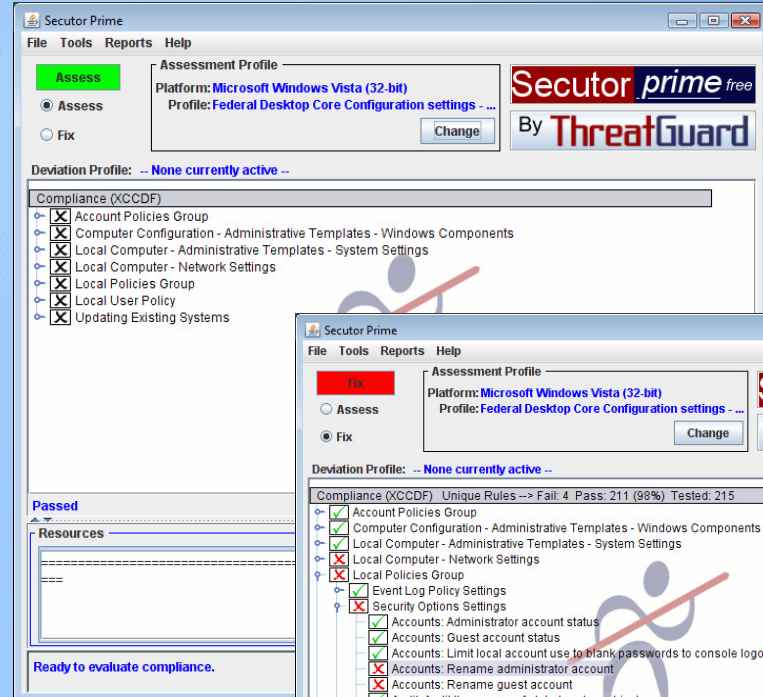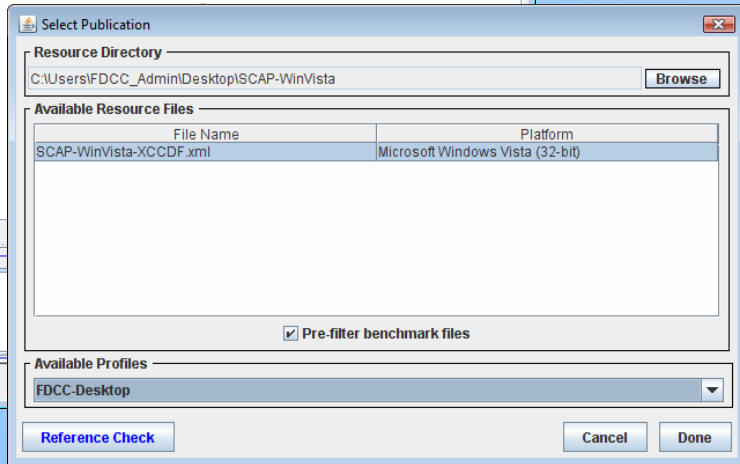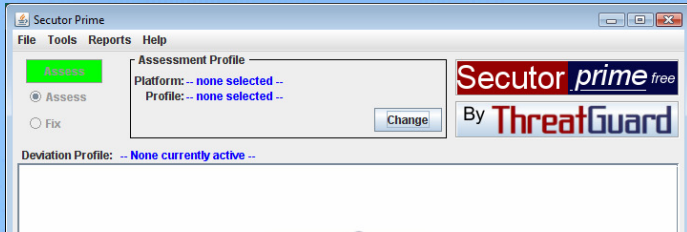
More Information

NIST FDCC Questions fdcc@nist.gov

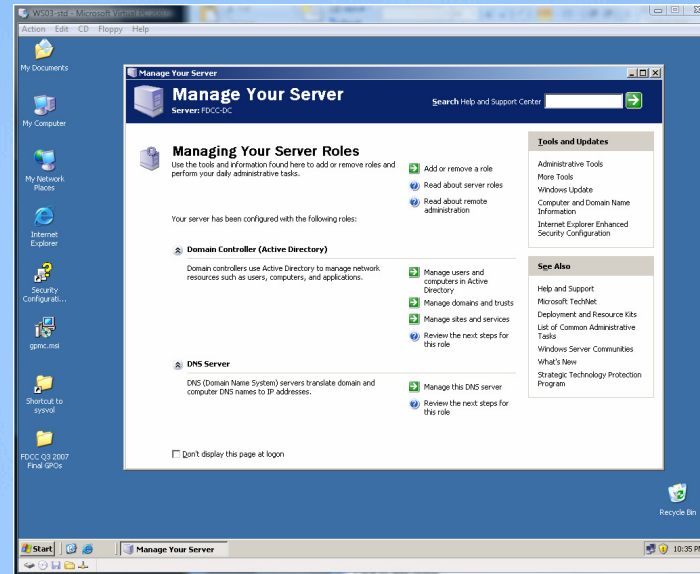NIST FDCC Web Site http://fdcc.nist.gov

- FDCC SCAP Checklists

- FDCC Settings

- Virtual Machine Images

- Group Policy Objects

National Checklist Program http://checklists.nist.gov

National Vulnerability Database http://nvd.nist.gov or http://scap.nist.gov

- SCAP Checklists

- SCAP Capable Products

- SCAP Events

NIST SCAP Mailing Lists Scap-update@nist.gov

Scap-dev@nist.gov

Scap-content@nist.gov

Contact Information

Policy Questions
Dan Costello – OMB
Daniel_J._Costello@omb.eop.gov

ISAP NIST Project Lead
Steve Quinn
(301) 975-6967
stephen.quinn@nist.gov

NVD Project Lead
Peter Mell
(301) 975-5572
mell@nist.gov

Senior Information Security Researchers and Technical Support

Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

Murugiah Souppaya
(301) 975-4758
murugiah.souppaya@nist.gov

Matt Barrett
(301) 975-3390
matthew.barrett@nist.gov

Information and Feedback
Web: http://nvd.nist.gov/scap
Comments: scap-update@nist.gov

NIST FDCC Team Members

High Impact Settings
What 800 Pound Gorilla?

- Operate the system as a standard user
- Accounts: Administrator account status -Disabled
- Wireless Service - Disabled
- Maximum password age – 60 days
- Minimum password length – 12 characters
- Microsoft network client: Digitally sign communications (always) – Enabled
- Network security: LAN Manager authentication level - Send NTLMv2 Response only. Refuse LM and NTLM
- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing – Enabled
- Windows Firewall – Enabled
- Signed Drivers – XP only

Common Mailing List Questions

- How does FDCC relate to FISMA compliance and SP800-53?

- How do I report compliance and exceptions? To whom do I report that information? Any special format?

- Where can I find a centralized list of FDCC compliant applications?

- Does 100% pass on SCAP-based scans mean I am 100% FDCC compliant?

- We have implemented wireless within our enterprise. Do I really need to disable wireless? What if I am using a third-party wireless client?

- Is FDCC applicable to:

  - Windows XP and Vista when used as a server?

  - logically or physical separated desktops and laptops?

  - developer or test desktops and laptops?

  - contractor computers?

  - special purpose (e.g., process control) computers?

- What about FDCC for UNIX, Macintosh, applications, etc?

Questions

National Institute of Standards & Technology
Information Technology Laboratory
Computer Security Division

Current State of Information Security

FISMA Compliance Model

30,000 FT

FISMA Legislation
High Level, Generalized, Information Security Requirements

15,000 FT

Federal Information Processing Standards
FIPS 199: Information System Security Categorization
FIPS 200: Minimum Information Security Requirements

5,000 FT

Management-level Security Controls

Technical-level Security Controls

Operational-level Security Controls

Hands On

Information System Security Configuration Settings
NIST, NSA, DISA, Vendors, Third Parties (e.g., CIS) Checklists and Implementation Guidance

Current State: Compliance and Configuration Management

Compliance Management

FISMA	HIPAA	SOX	DCID	COMSEC '97	DoD	ISO	Vendor	3rd Party
SP 800-53	Title III	???	DCID6/3	NSA Req	DoD IA Controls	17799/ 27001		
SP 800-68	Security		Agency Guides	NSA Guides	DISA STIGS & Checklists	???	Guide	Guide

Finite Set of Possible Known IT Risk Controls & Application Configuration Options

Agency Tailoring
Mgmt, Operational, Technical Risk Controls

Configuration Management

Windows → XP → SP1 → Enterprise / Mobile / Stand Alone / SSLF
SP1 → Mobile → High / Moderate / Low
XP → SP2

Millions of settings to manage

OS or Application	Version/ Role	Major Patch Level	Environment	Impact Rating or MAC/CONF

Current State Summary - Compliance

A Study in Cause and Effect

Governing Bodies

Recognize the need to improve security and mandate it in an increasing number of laws, directives, and policies

Standards Bodies

Try to keep pace with an increasing number of mandates by generating more frameworks and guidelines

Product Teams

Based on the increasing number of mandates, see the need for automation, many seek to enable it through proprietary methods

Service Providers

Based on the increasing number of mandates, see the need for automation and have responded by 1) learning a wide variety of both open and proprietary technologies and 2) implementing point solutions

Operations Teams

Lacking true automation, 1) have become overwhelmed by an increasing number of mandates, frameworks, and guidelines and 2) are spending a considerable amount of resources trying to keep pace

Current State: Vulnerability Trends

A 20-50% increase over previous years

Legend:
- CERT/CC
- NVD
- OSVDB
- Symantec
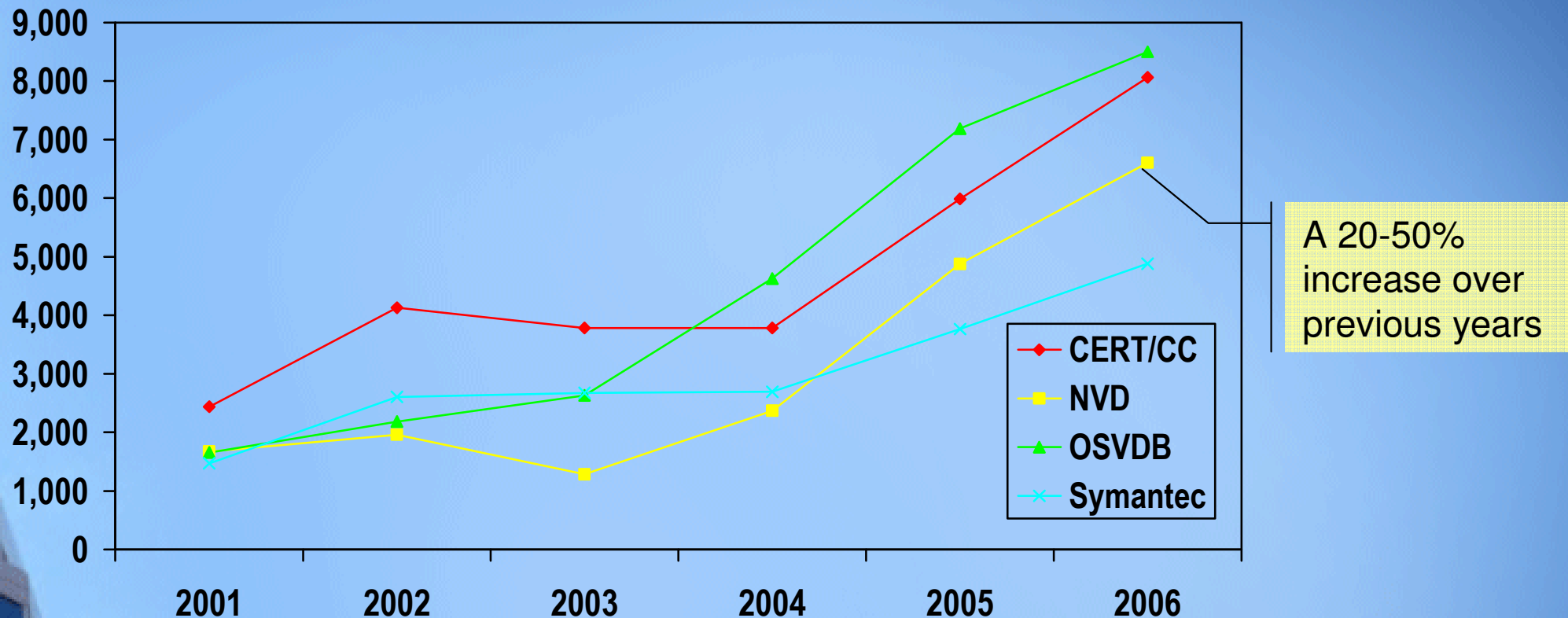
- Decreased timeline in exploit development coupled with a decreased patch development timeline (highly variable across vendors)
- Increased prevalence of zero day exploits
- Three of the SANS Top 20 Internet Security Attack Targets 2006 were categorized as "configuration weaknesses." Many of the remaining 17 can be partially mitigated via proper configuration.

Current State: Vulnerability Management Industry

- Product functionality is becoming more hearty as vendors acknowledge connections between security operations and a wide variety of IT systems (e.g., asset management, change/configuration management)

- Some vendors understand the value of bringing together vulnerability management data across multiple vendors

- Vendors driving differentiation through:

  - enumeration,   Hinders information sharing and automation

  - evaluation,   Reduces reproducibility across vendors

  - content,

  - measurement, and   Drives broad differences in prioritization and remediation

  - reporting

Enabling Network Centric Operations
A Wish List

*Goal 1. Assured DoD mission execution in the face of cyber attack, or
Goal 1. Dependability of the information and information infrastructure in
the face of cyber attack*   -Richard Hale, 2007 Security Automation Conference

Tactical

- Push button understanding of likely exposure to vulnerability/attack
- Push button understanding of actual vulnerability
- Ability to automatically aggregate vulnerability data from tools of varied manufacture
- Ability to implement security configurations and remediate vulnerability in a controlled yet automated way, including SSLF environments
- Ability to dynamically build trust relationships and join computer systems with mission partners
- Reduce effort and expense of documenting system vulnerability and compliance status (e.g., C&A)
- Reduce effort and expense of demonstrating compliance with various mandates

Strategic

Supplemental – SCAP Platform Evaluation Tutorial

Current and Near-Term Use Cases

Configuration

Organization Guidelines (e.g., STIG)

National Checklist Program

Misconfiguration Software Flaws

XCCDF, CPE, CVE, CCE, OVAL, CVSS

National Vulnerability Database

Information Feeds

Vulnerability Alerts (e.g., IAVA)

Organization Vulnerability Database

Monitor/Assess/Evaluate

Standardized Checklist
XCCDF

Standardized Test Procedures
OVAL

Standardized Measurement and Reporting
XCCDF CVSS

Decision and Change Control Process

Risk Decision Report
XCCDF CVSS

Compliance Report
XCCDF CVSS

Metrics Report
XCCDF CVSS

Risk Management and Compliance Process

Implement/Remediate

Standardized Change List
XCCDF

Standardized Change Procedures
OVRL

Standardized Measurement and Reporting
CVSS XCCDF

Legend

- Organization
- COTS / GOTS
- NIST

Current Problems
Conceptual Analogy (Continued)

Before
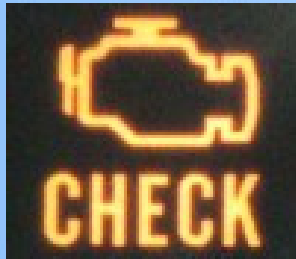
After

Error Report

Problem
 Air Pressure Loss

Impact
Car Will Not Start (9/10)

Diagnosis Accuracy:
All Sensors Reporting

Diagnosis:
Replace Gas Cap

Expected Cost:
 $25.00

XML Made Simple

XCCDF - eXtensible Car Care Description Format

```
<Car>
 <Description>
   <Year> 1997 </Year>
   <Make> Ford </Make>
   <Model> Contour </Model>
 <Maintenance>
   <Check1> Gas Cap = On <>
   <Check2>Oil Level = Full <>
 </Maintenance>
 </Description>
</Car>
```

OVAL – Open Vehicle Assessment Language

```
<Checks>
 <Check1>
   <Location> Side of Car <>
   <Procedure> Turn <>
 </Check1>
<Check2>
   <Location> Hood <>
   </Procedure> … <>
 </Check2>
</Checks>
```

Error Report

Problem:
Air Pressure Loss

Diagnosis Accuracy:
All Sensors Reporting

Diagnosis:
Replace Gas Cap

Expected Cost:
$25.00

SCAP Content Made Simple

XCCDF - eXtensible Checklist Configuration Description Format

OVAL – Open Vulnerability Assessment Language

```
<Document ID> NIST SP 800-68
  <Date> 04/22/06 </Date>
    <Version> 1 </Version>
    <Revision> 2 </Revision>
<Platform> Windows XP <>
    <Check1> Password >= 8 <>
    <Check2> Win XP Vuln <>
  </Maintenance>
 </Description>
</Car>
```

```
<Checks
 <Check1>
    <Registry Check> … <>
    <Value> 8 </Value>
 </Check1>
<Check2>
    <File Version> … <>
    <Value> 1.0.12.4 </Value>
 </Check2>
</Checks>
```

(red)	CPE
(yellow)	CCE
(green)	CVE

XCCDF security benchmark automation

CVSS

Application to Automated Compliance
The Connected Path

800-53 Security Control

800-68 Security Guidance

ISAP Produced Security Guidance in XML Format

Result

API Call

COTS Tool Ingest

Application to Automated Compliance

The Connected Path

**800-53 Security Control
DoD IA Control**

AC-7 Unsuccessful Login Attempts

**800-68 Security Guidance
DISA STIG/Checklist
NSA Guide**

AC-7: Account Lockout Duration

AC-7: Account Lockout Threshold

**ISAP Produced Security
Guidance in XML Format**

```
- <registry_test id="wrt-9999"
comment="Account Lockout Duration Set to
5" check="at least 5">
- <object>
  <hive>HKEY_LOCAL_MACHINE</hive>
  <key>Software\Microsoft\Windows</key>
  <name>AccountLockoutDuration</name>
  </object>
- <data operation="AND">
  <value operator="greater than">5*</value>
```

Result

```
RegQueryValue (lpHKey, path, value, sKey,
Value, Op);
If (Op == '>" )
if ((sKey < Value )
return (1); else
return (0);
```

API Call

```
lpHKey = "HKEY_LOCAL_MACHINE"
Path = "Software\Microsoft\Windows\"
Value = "5"
sKey = "AccountLockoutDuration"
Op = ">"
```

COTS Tool Ingest

Supplemental – SCAP Value Reference

SCAP Value

Feature	Benefit
Standardizes *how* computers communicate vulnerability information – the protocol	■Enables interoperability for products and services of various manufacture
Standardizes *what* vulnerability information computers communicate – the content	■Enables repeatability across products and services of various manufacture ■Reduces content-based variance in operational decisions and actions
Based on open standards	■Harnesses the collective brain power of the masses for creation and evolution ■Adapts to a wide array of use cases
Uses configuration and asset management standards	■Mobilizes asset inventory and configuration information for use in vulnerability and compliance management
Applicable to many different Risk Management Frameworks – Assess, Monitor, Implement	■Reduces time, effort, and expense of risk management process
Detailed traceability to multiple security mandates and guidelines	■Automates portions of compliance demonstration and reporting ■Reduces chance of misinterpretation between Inspector General/auditors and operations teams
Keyed on NIST SP 800-53 security controls	■Automates portions of FISMA compliance demonstration and reporting

Supplemental – FAQ for NIST FISMA Documents

Fundamental FISMA Questions

What are the NIST Technical Security Controls?

What are the _Specific_ NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST Recs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?

Fundamental FISMA Documents

FIPS 200 / SP 800-53

Security Control Selection

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

SP 800-18

Security Control Documentation

What are the NIST Technical Security Controls?

What are the _Specific_ NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST Recs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?

SP 800-37

Security Control Monitoring

SP 800-37

System Authorization

SP 800-53A / SP 800-26 / SP 800-37

Security Control Assessment

SP 800-70

Security Control Implementation