SCAP Nuts-n-Bolts

presented by:

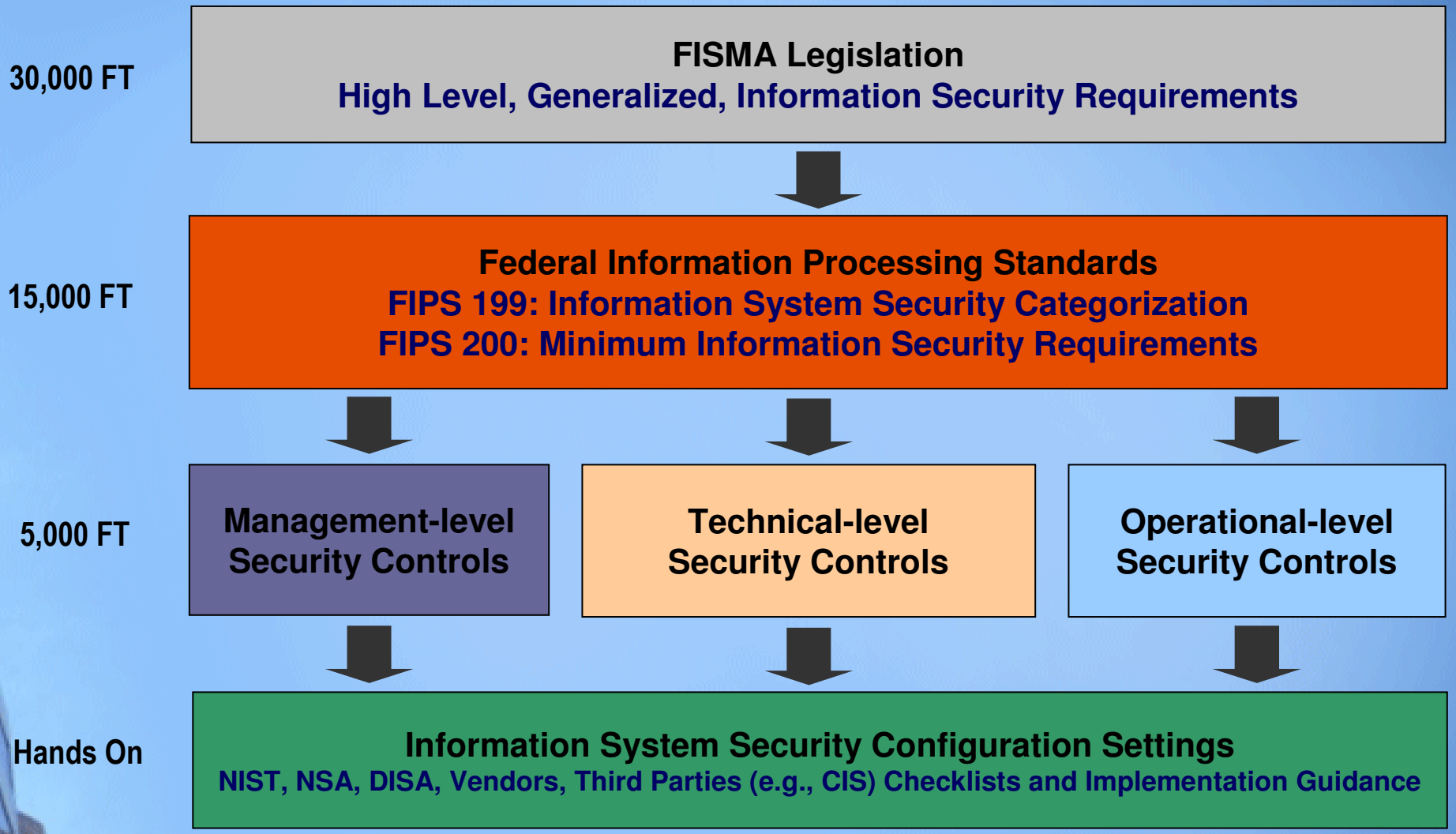
Matt Barrett

National Institute of Standards and Technology

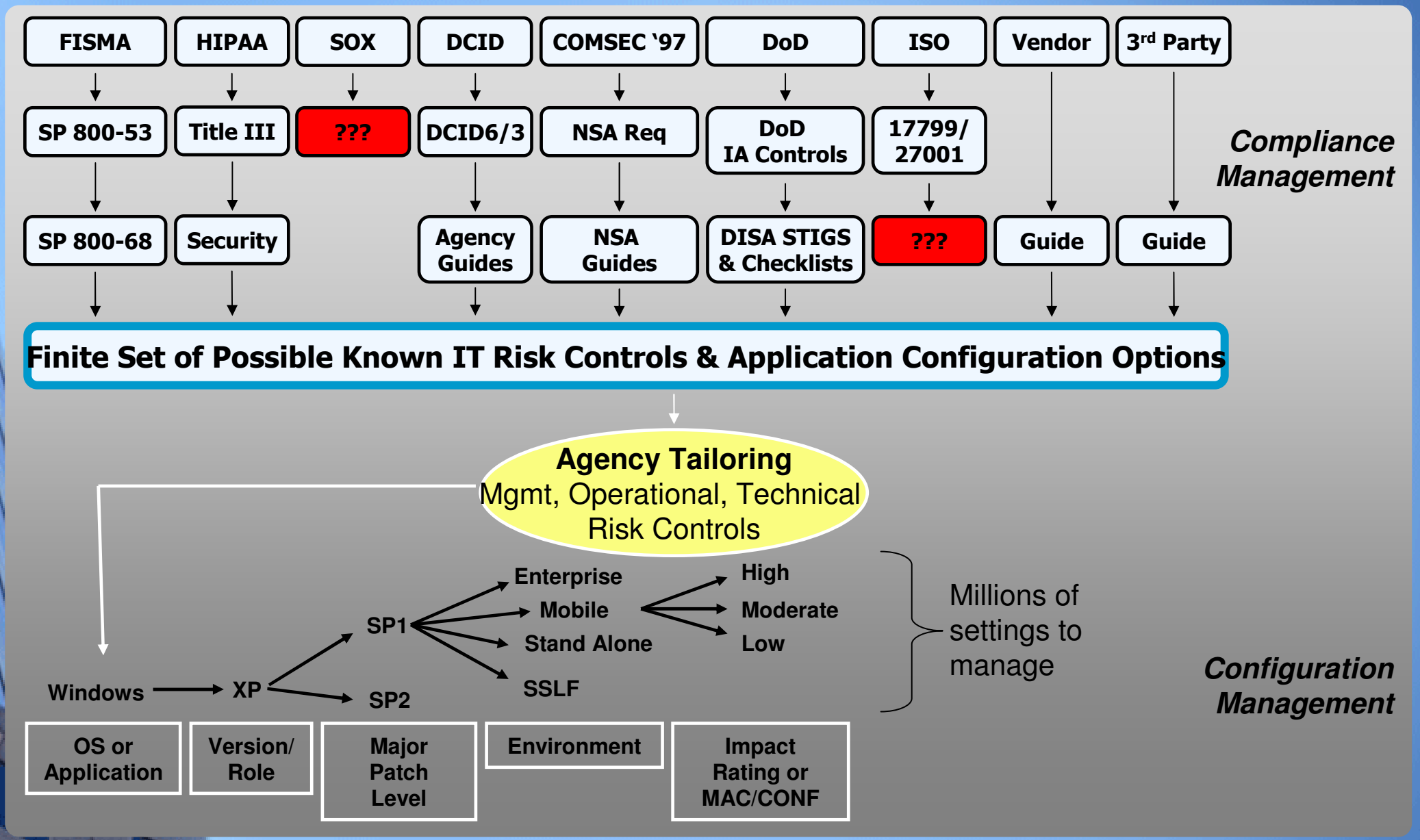
Agenda

- State of Security Operations
- Security Content Automation Protocol
- How SCAP Works
- Future of Security Operations
- SCAP and Federal Desktop Core Configuration

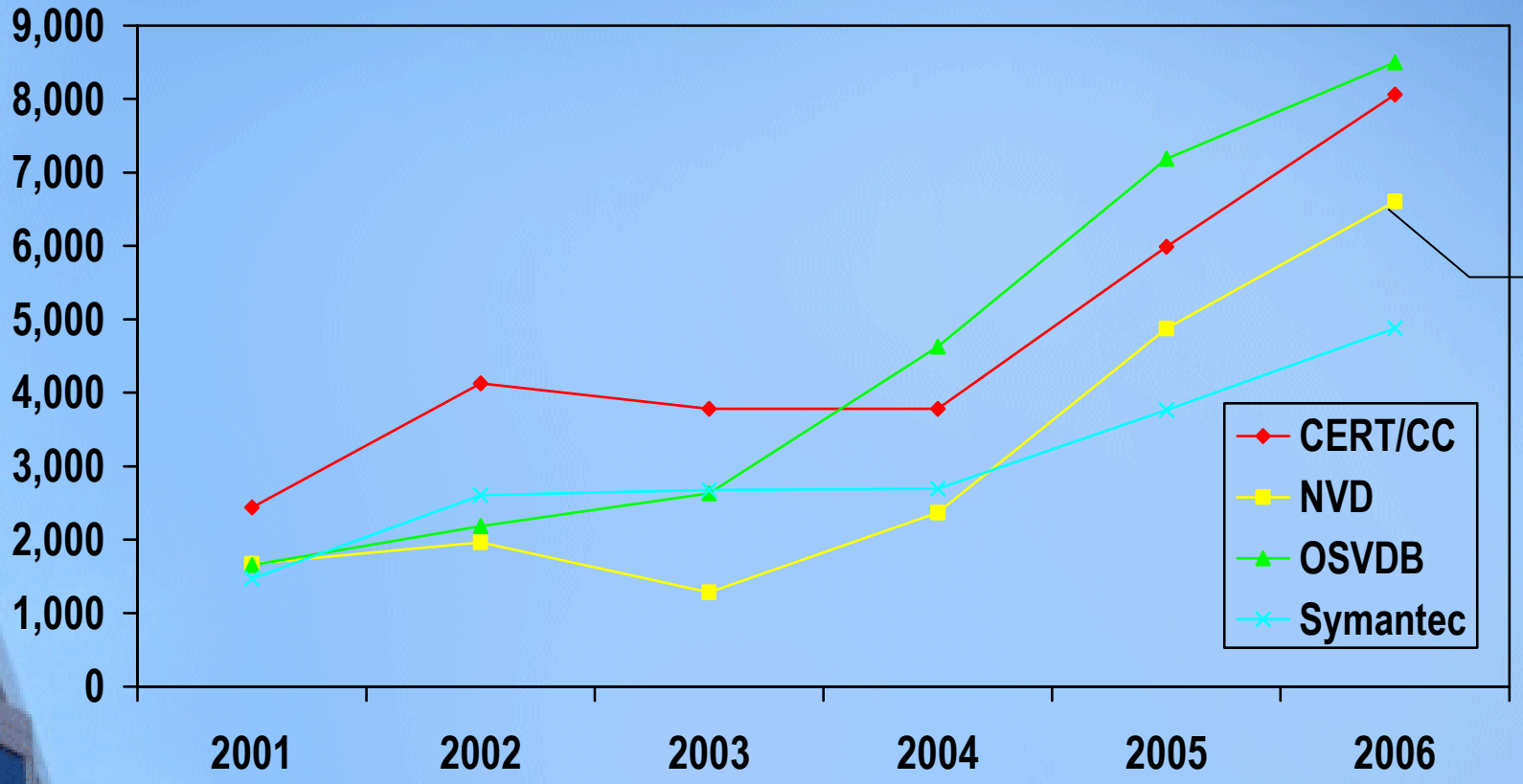
FISMA Compliance Model



Current State: Compliance and Configuration Management



Current State: Vulnerability Trends



A 20-50% increase over previous years

- 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
  - reporting

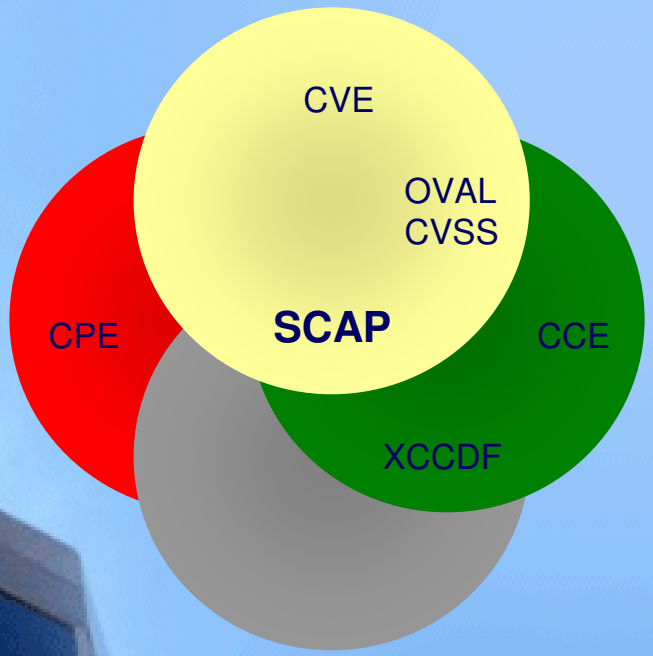
  } Drives broad differences in prioritization and remediation

What is SCAP?

How

Standardizing the format by which we communicate

Protocol



What

Standardizing the information we communicate

Content

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

CVE	Common Vulnerability Enumeration	Standard nomenclature and dictionary of security related software flaws
CCE	Common Configuration Enumeration	Standard nomenclature and dictionary of software misconfigurations
CPE	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
XCCDF	eXtensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
OVAL	Open Vulnerability and Assessment Language	Standard XML for test procedures
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

Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource
NIST National Institute of Standards and Technology

How SCAP Works

Checklist **XCCDF**
Platform CPE
Misconfiguration CCE
General Impact CVSS
Software Flaw CVE
General Impact CVSS

Test Procedures **OVAL**

Patches **OVAL**

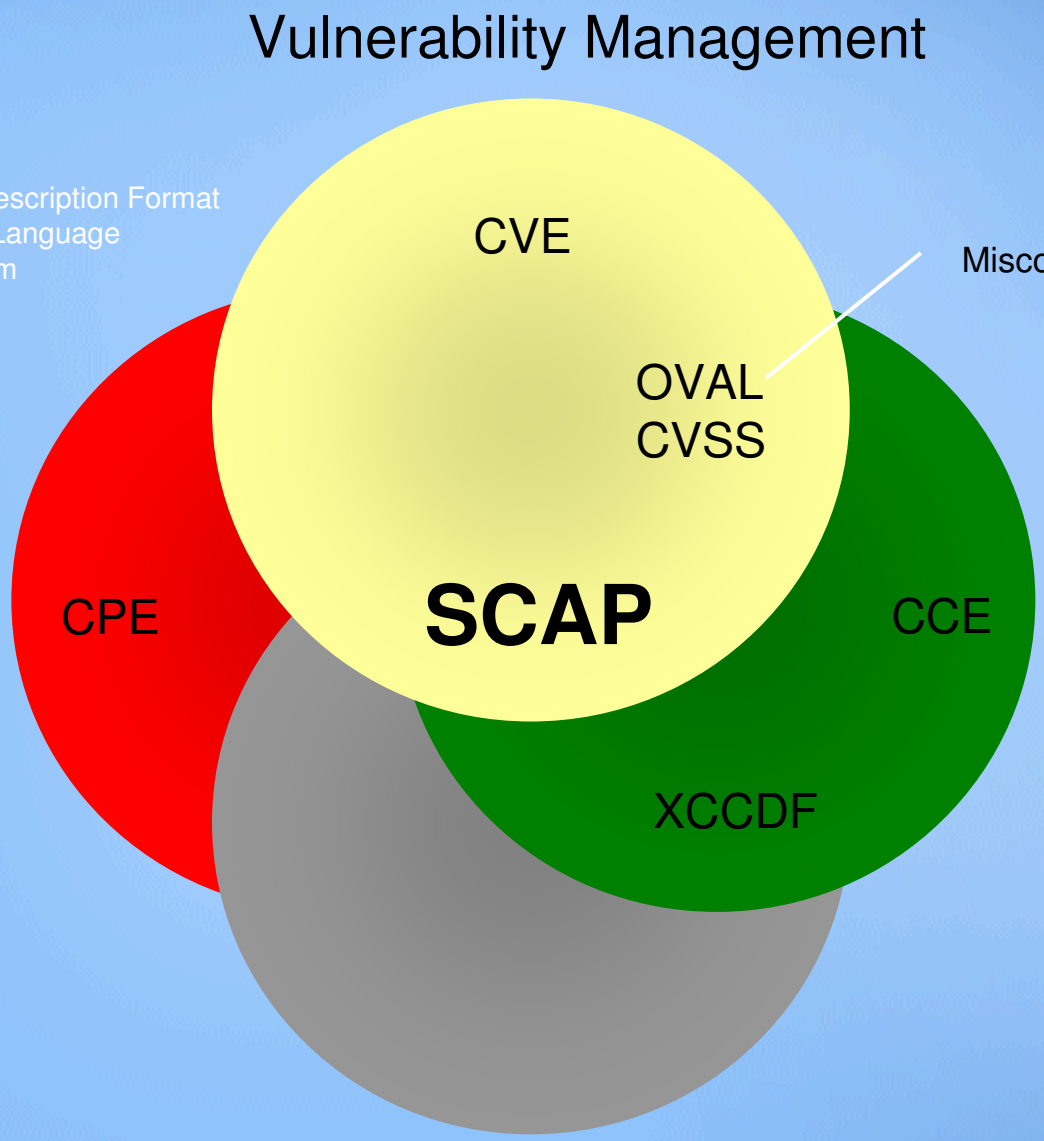
COTS/ GOTS Tools

Specific Impact CVSS Results

Specific Impact CVSS Results

Integrating IT and IT Security Through SCAP

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



Federal Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

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 800-53 / 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 800-18

Document
Security Controls

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

SP 800-70

Implement
Security Controls

Implement security controls; apply security configuration settings

SP 800-53A

Assess
Security Controls

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

SP 800-37

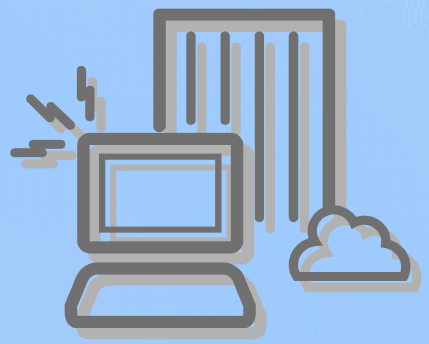
Authorize
Information System

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

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



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%	

Traceability within SCAP XCCDF

Keyed on SP800-53 Security Controls

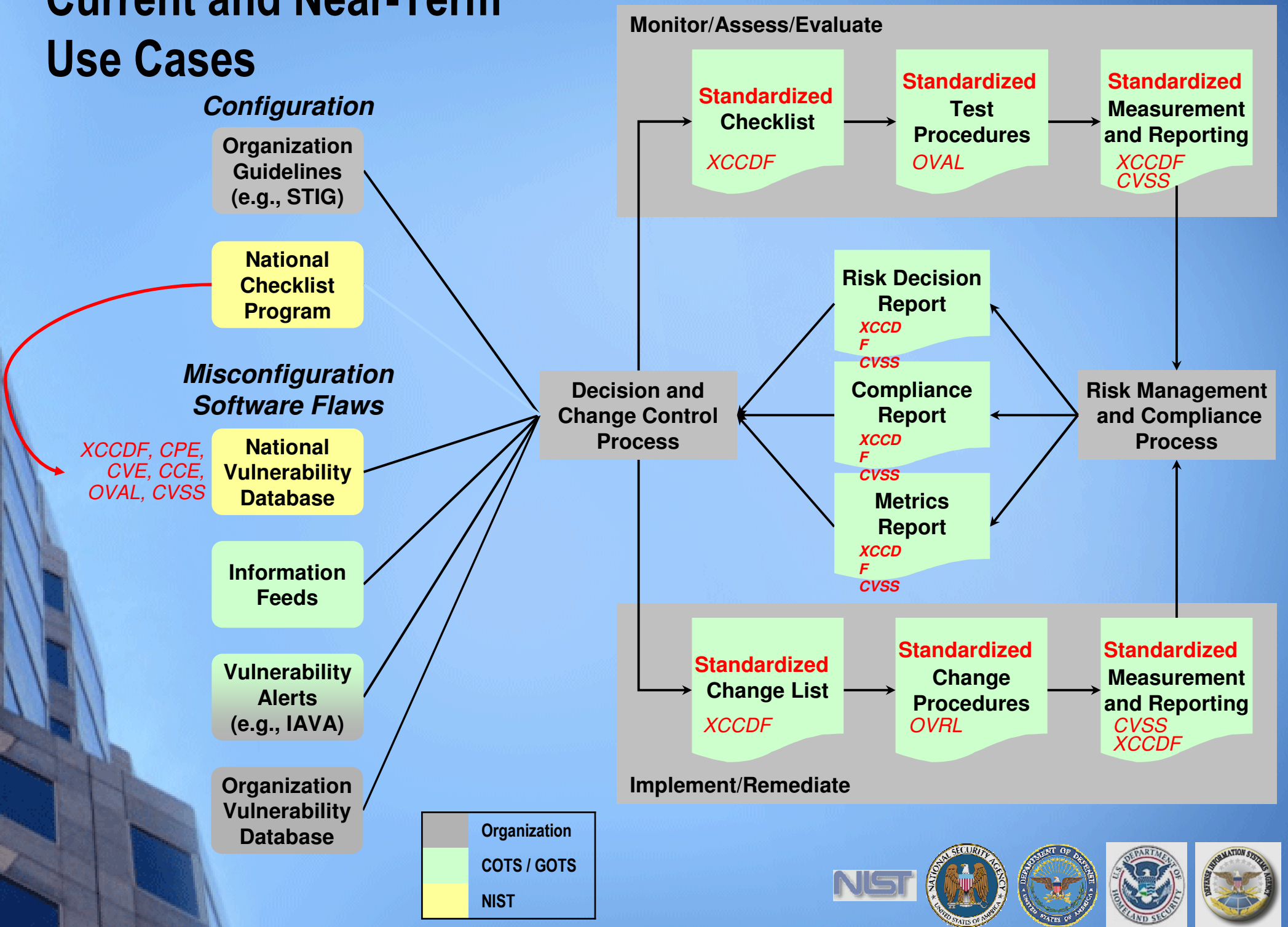
```
<Group id="IA-5" hidden="true">
 <title>Authenticator Management</title>
  <reference>ISO/IEC 17799: 11.5.2, 11.5.3</reference>
  <reference>NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10,
    15.1.11, 15.1.12, 15.1.13, 16.1.3, 16.2.3</reference>
  <reference>GAO FISCAM: AC-3.2</reference>
  <reference>DOD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

<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 Mandates

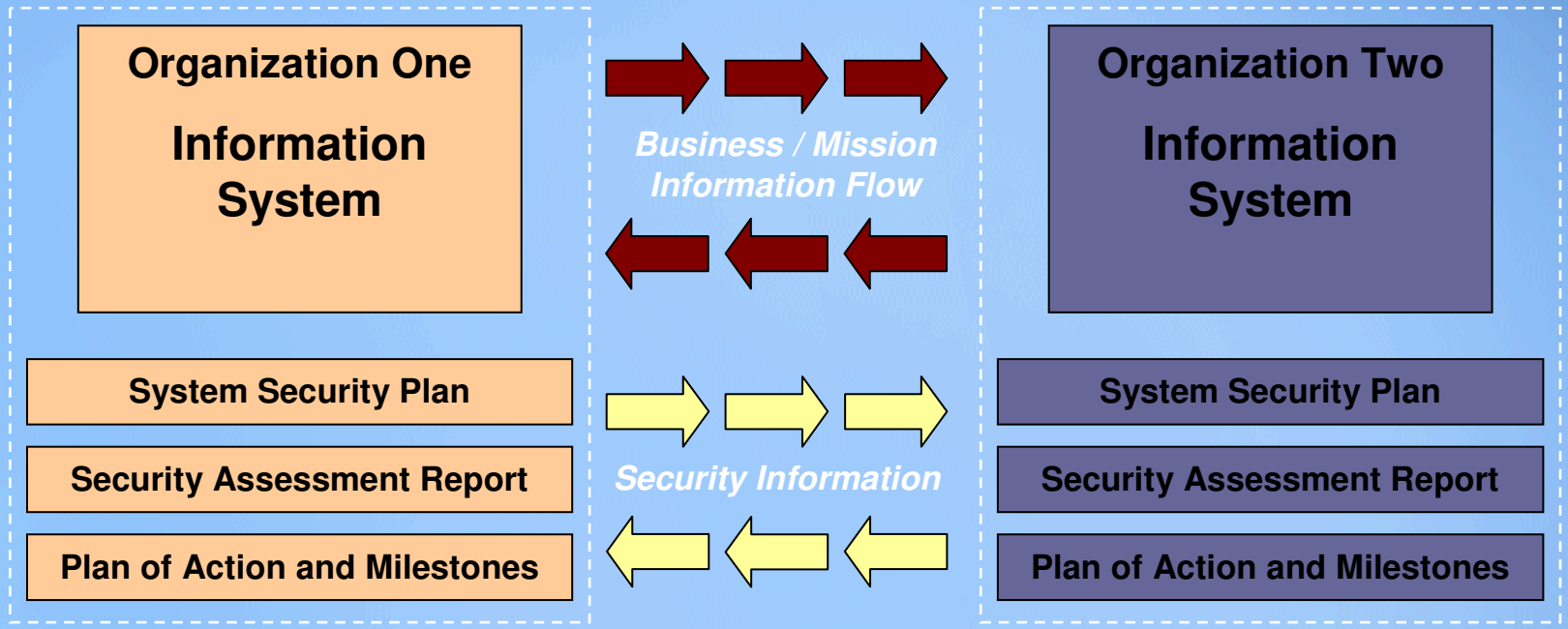
Traceability to Guidelines

Rationale for security configuration

Current and Near-Term Use Cases



Security Visibility Among Business/Mission Partners



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

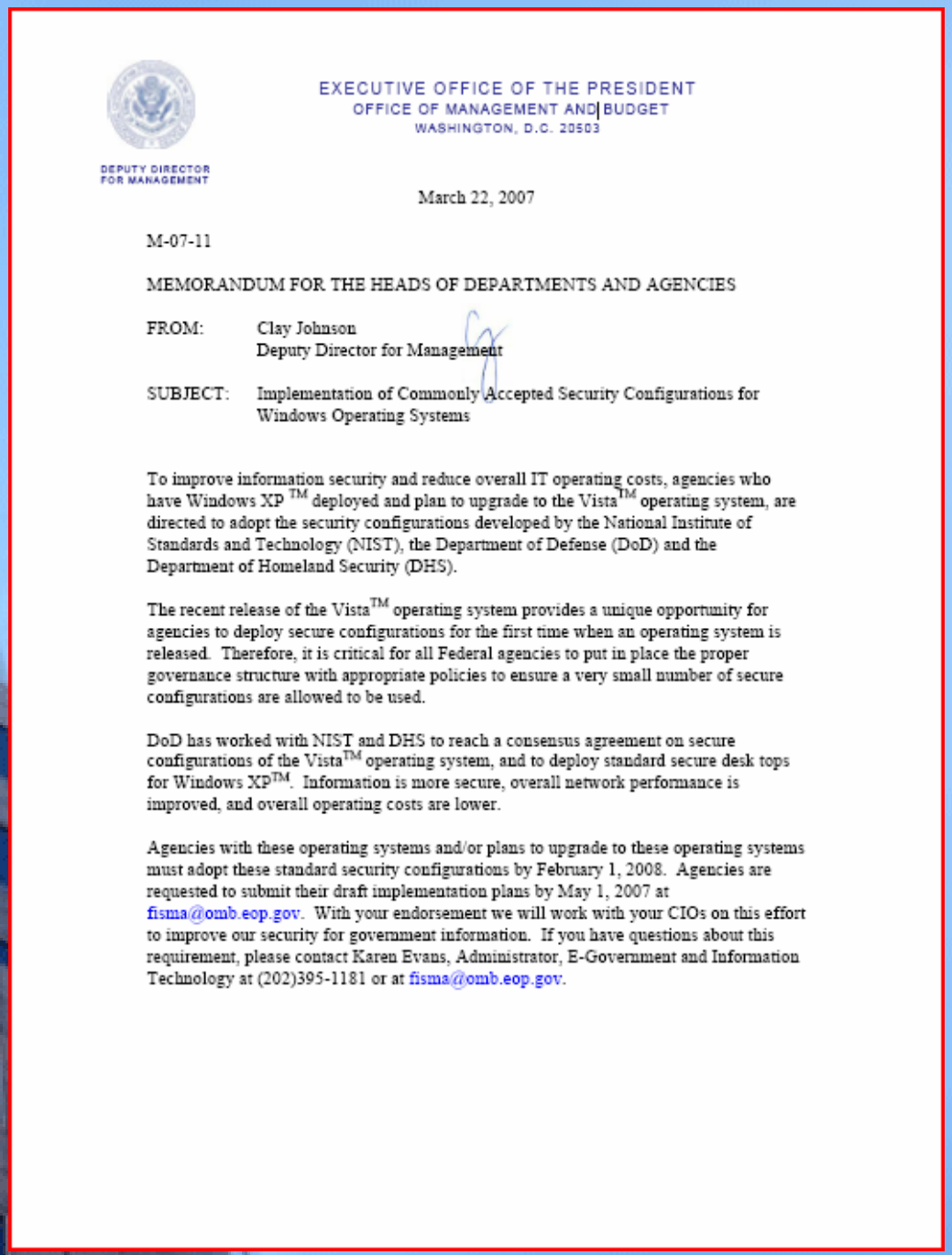
Stakeholder and Contributor Landscape: Federal Agencies

SCAP Infrastructure, Beta Tests, Use Cases, and Early Adopters

DHS		OMB	
NSA		IC	
OSD		DISA	
DOJ		EPA	
Army		NIST	
DOS			

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.

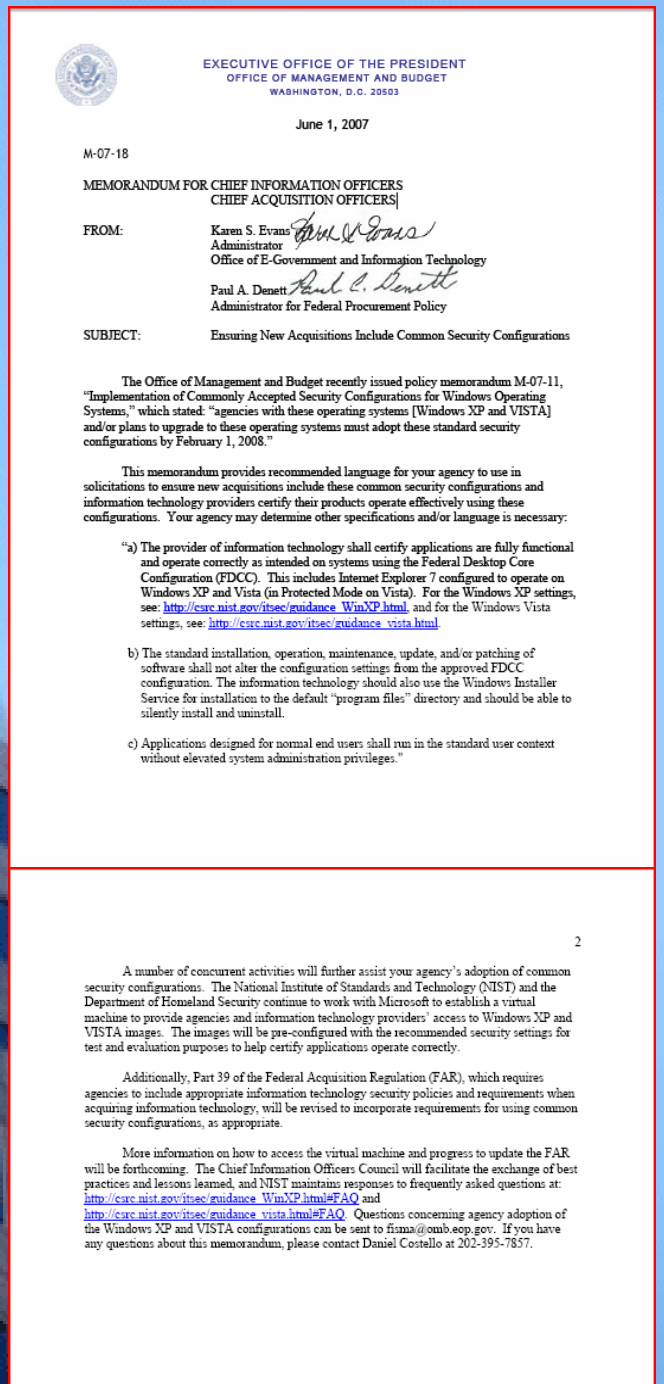
Corresponding OMB Memo to CIOs:

- 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



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

June 1, 2007

M-07-18

MEMORANDUM FOR CHIEF INFORMATION OFFICERS
CHIEF ACQUISITION OFFICERS

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

Paul A. Denett
Administrator for Federal Procurement Policy

SUBJECT: Ensuring New Acquisitions Include Common Security 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."

This memorandum provides recommended language for your agency to use in solicitations to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations. Your agency may determine other specifications and/or language is necessary:

"a) 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). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html, and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.

b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

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

2

A number of concurrent activities will further assist your agency's adoption of common security configurations. 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.

Additionally, Part 39 of the Federal Acquisition Regulation (FAR), which requires agencies to include appropriate information technology security policies and requirements when acquiring information technology, will be revised to incorporate requirements for using common security configurations, as appropriate.

More information on how to access the virtual machine and progress to update the FAR will be forthcoming. The Chief Information Officers Council will facilitate the exchange of best practices and lessons learned, and NIST maintains responses to frequently asked questions at: http://csrc.nist.gov/itsec/guidance_WinXP.html#FAQ and http://csrc.nist.gov/itsec/guidance_vista.html#FAQ. Questions concerning agency adoption of the Windows XP and VISTA configurations can be sent to fisma@omb.eop.gov. If you have any questions about this memorandum, please contact Daniel Costello at 202-395-7857.

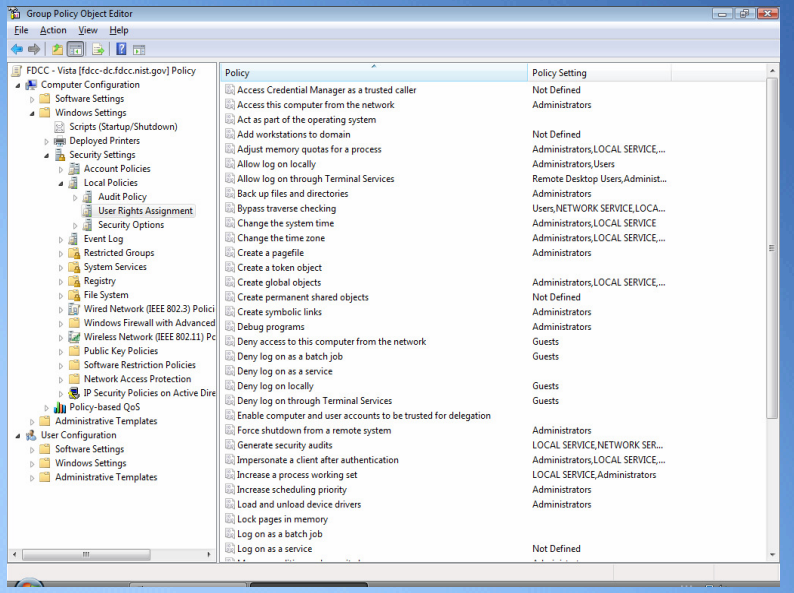
"The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista)."

"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

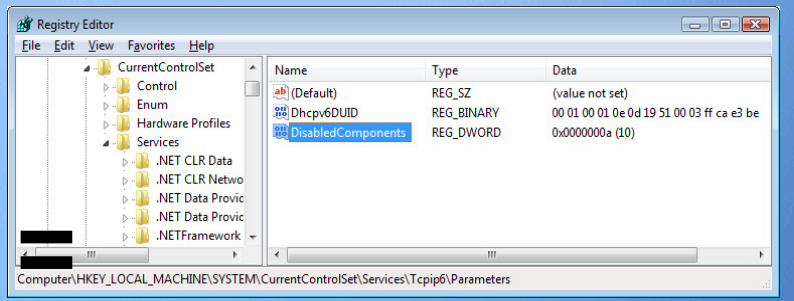
ThreatGuard Secutor prime free

secure elements® audit. evaluate. comply.

C5 Compliance Platform

Reconcile any “failed” SCAP tests

FDCC Virtual Machine Image



Record any exceptions

NIST · National Security Agency · Department of Defense · U.S. Department of Homeland Security · Defense Information Systems Agency

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

SCAP Product

Self Asserts

SCAP Compliance

NVLAP

Test Effort

SCAP Compliant Products

Product Vendor

Self Asserts

FDCC Compliance

Federal Agency

+

FDCC Virtual Machine Image

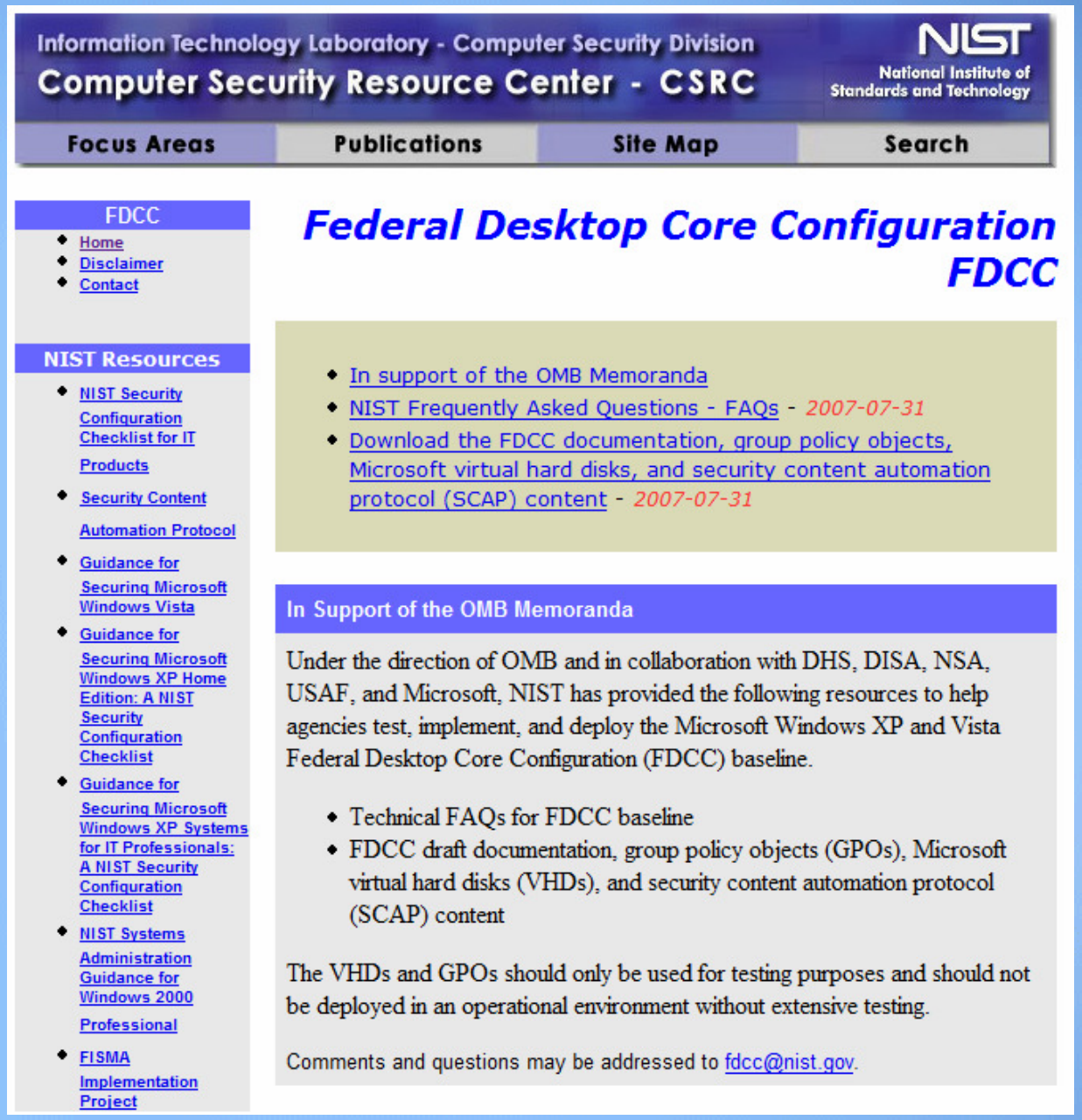
+

SCAP Compliant Product

=

Compliant with M-07-18? Implement Product?

http://csrc.nist.gov/fdcc



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 Configu
   2007 memorandum fr
   a corresponding mem
   Chief Information Off

2. **What operating sy**
   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 S
   guide that could be us
   do not exist, Federal a
   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 Func
   DoD customization of
   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 ac
   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 FDCC the Microsoft Windows F**
   No. The FDCC baseline reco
   the Microsoft Windows Firew
   system installation. However,
   firewall software instead of t

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

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 c
   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://csrc.nist.gov/fdcc/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

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

Federal Desktop Core Configuration FDCC

- DOWNLOAD PAGE -

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 Windows XP Professional SP2 and Vista systems and will not work on Windov 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The security pol 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, Win 2000 or Windows Server 2003.

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

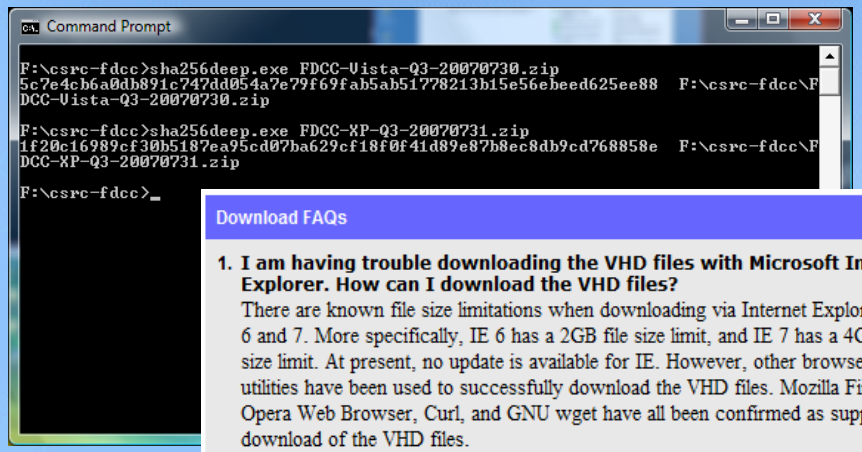
These recommendations were developed at the National Institute of Standards a Technology, which collaborated with DHS, DISA, NSA, USAF, and Microsoft to pro the Windows XP and Vista FDCC baseline. Pursuant to title 17 Section 105 of the States Code, these recommendations are not subject to copyright protection and the public domain. NIST assumes no responsibility whatsoever for their use by o parties, and makes no guarantees, expressed or implied, about their quality, relia 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
2007.07.31 FDCC Documentation Release 1.0 - Draft [xls, 100K] **SHA-1 Digest:** 2CB88444394B73E69EF41175897809A1232588A0 **SHA-256 Digest:** D6ECF963F4D2FA4AB92BA79D1527768DDF5ACCC875872496DE4C4C23E283CD17	2007.07.31 FDCC GPO Release 1.0 -Draft [zip, ~3 MB] **SHA-1 Digest:** B46C514BFABD312FA9C1AC149AFA04D2D15215FC **SHA-256 Digest:** 682B097721E068170AD7CE883BC70045803FE6A00A8C97A60A194C13CEFCDA5C	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	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.

Download FDCC VHD Files

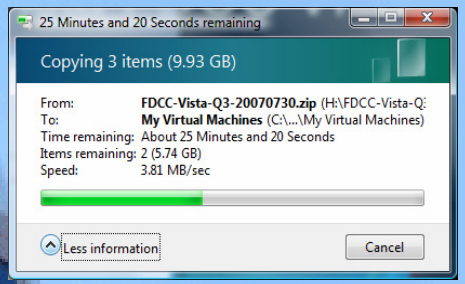


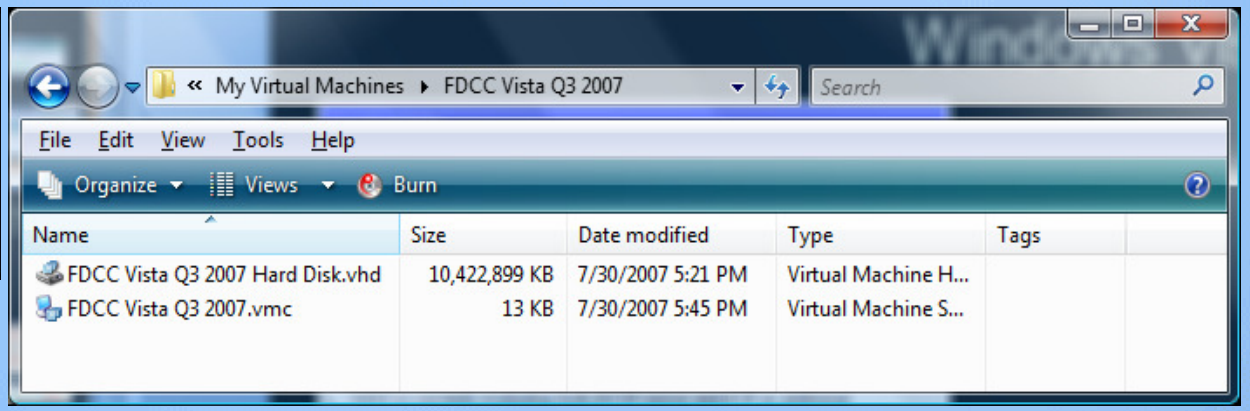
Download FAQs

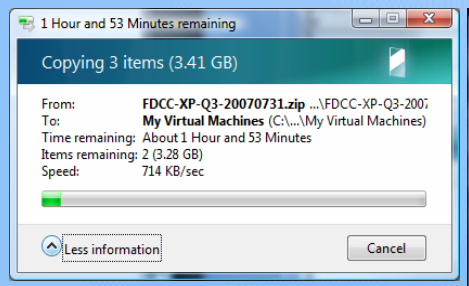
1. **I am having trouble downloading the VHD files with Microsoft Internet Explorer. How can I download the VHD files?**
   There are known file size limitations when downloading via Internet Explorer (IE) 6 and 7. More specifically, IE 6 has a 2GB file size limit, and IE 7 has a 4GB file size limit. At present, no update is available for IE. However, other browsers and utilities have been used to successfully download the VHD files. Mozilla Firefox, Opera Web Browser, Curl, and GNU wget have all been confirmed as supporting download of the VHD files.

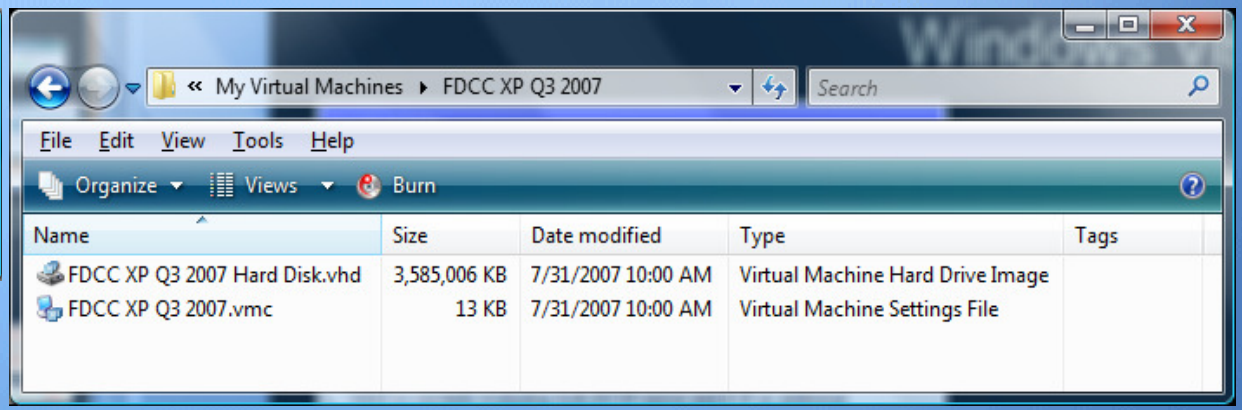
2. **Does NIST intend to have HTTP mirror or FTP alternate download sites available?**
   NIST is currently evaluating both HTTP mirror and FTP as additional mechanisms to download the VHD files. Additional and alternate sites will be linked to the download site as they become available.

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









More Information

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 FDCC Web Site — http://fdcc.nist.gov

- FDCC SCAP Checklists
- FDCC Settings
- Virtual Machine Images
- Group Policy Objects

NIST SCAP Mailing Lists — Scap-update@nist.gov

Scap-dev@nist.gov

Scap-content@nist.gov

Upcoming Events

3rd Annual Security Automation Conference and Expo

- 19-20 September
- Speakers
  - The Honorable Karen S. Evans (OMB)
  - Robert F. Lentz DAS DIIA (OSD)
  - Cita Furlani, Director ITL (NIST)
  - Tim Grance, Program Manager (NIST)
  - Dennis Heretick, CISO (DoJ)
  - Richard Hale, CIAO (DISA)
  - Sherrill Nicely, Deputy Associate Director (DNI)
  - Alan Paller, Director of Research (SANS)
  - Tony Sager, Chief (NSA)
  - Ron Ross, Program Manager (NIST)
  - Ron Knode, Adjunct Faculty, Towson State
- Expo
  - Technology Demonstrations
  - Beta Testing and Use Case Presentation

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

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

Questions

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

Supplemental – SCAP Platform Evaluation Tutorial

Current Problems

Conceptual Analogy (Continued)

Before

After

CHECK ***Error Report***

Problem

Air Pressure Loss

Impact

Car Will Not Start (9/10)

Diagnosis Accuracy:

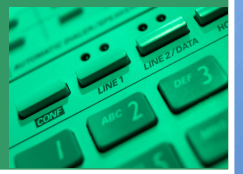
All Sensors Reporting

Diagnosis:

Replace Gas Cap

Expected Cost:

$25.00



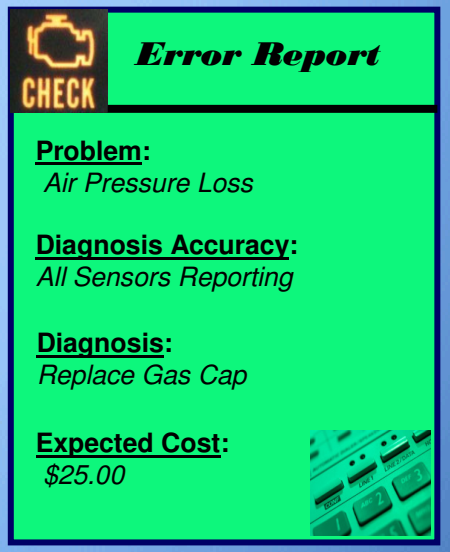
XML Made Simple

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>
```

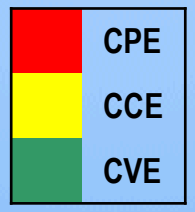


XML Made Simple

Standardized Checklist

XCCDF - eXtensible Checklist Configuration Description Format

```
<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>
```



OVAL – Open Vulnerability Assessment Language

Standardized Test Procedures

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

Standardized Measurement and Reporting

XCCDF security benchmark automation

CVSS

NIST

Application to Automated Compliance

The Connected Path

800-53 Security Control

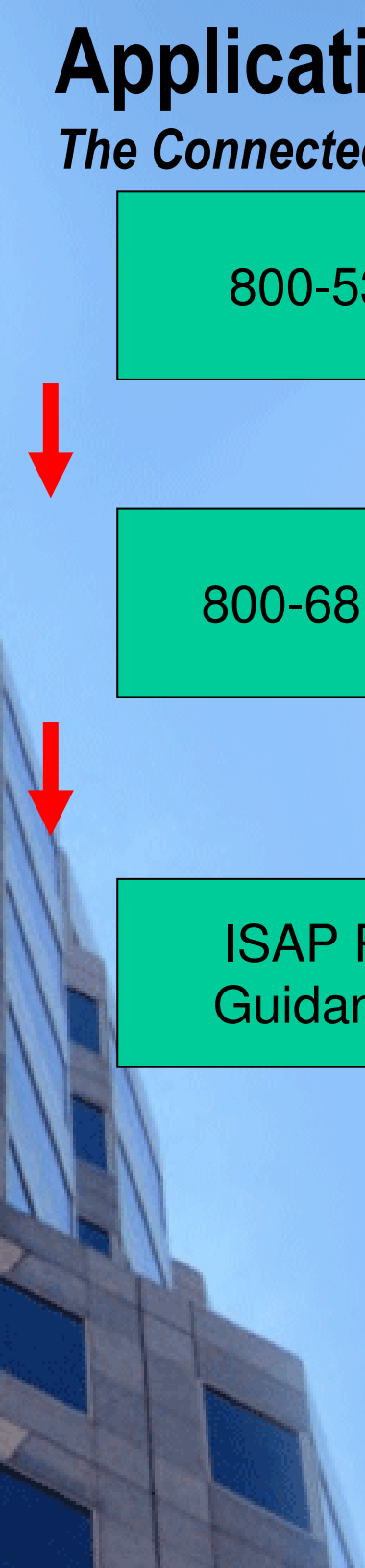
800-68 Security Guidance

ISAP Produced Security Guidance in XML Format

COTS Tool Ingest

API Call

Result



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 – 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