Federal CIO Council

Federal Desktop Core Configuration

Security Content Automation Protocol

1 August 2007 Update

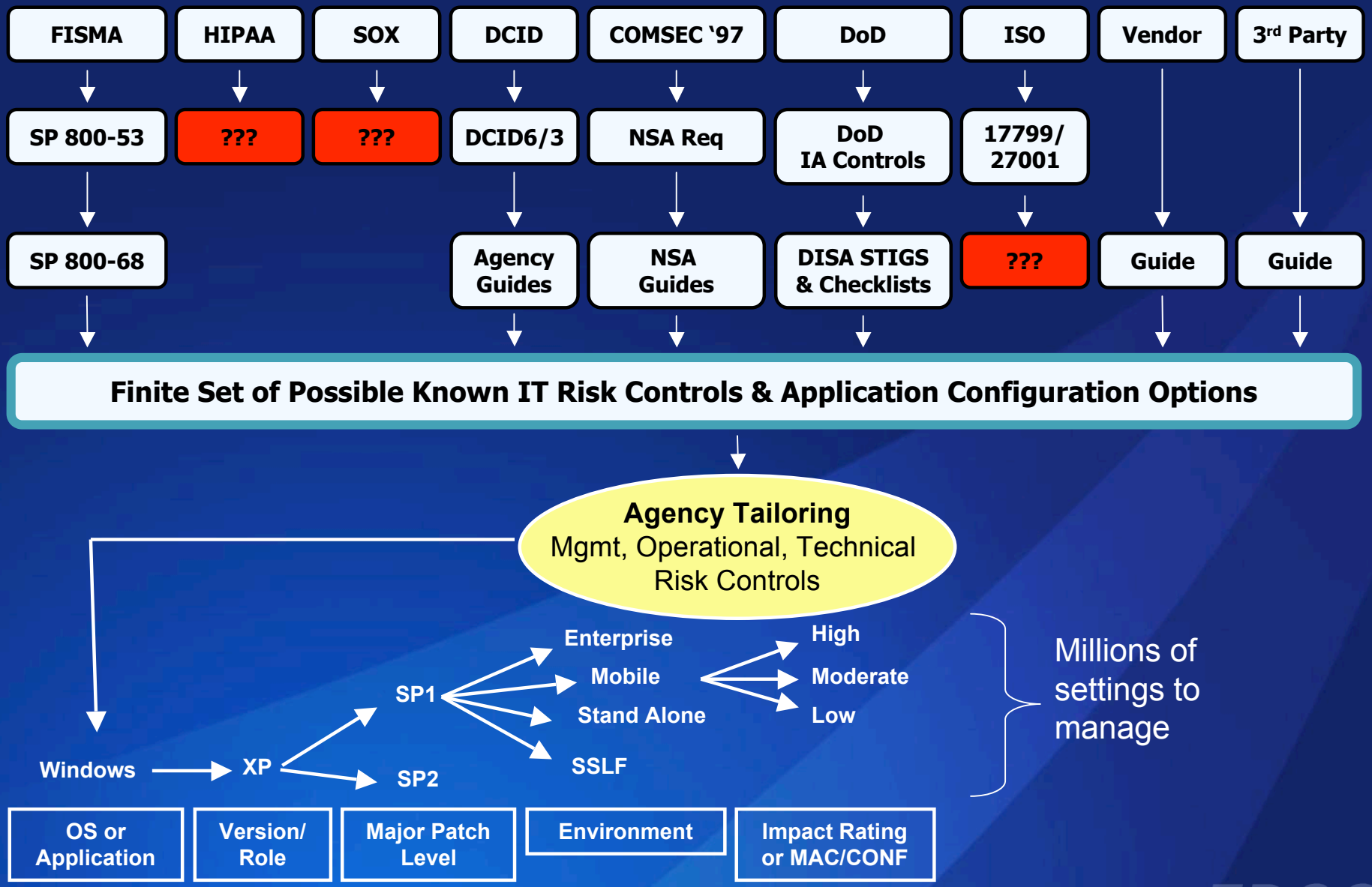
Matt Barrett
National Institute of Standards and Technology

FDCC

Agenda

- Current State of Compliance and Configuration Management
- Basis for SCAP
- SCAP Primer
- Use of SCAP during FDCC Testing
- Accomplishing FDCC with SCAP
- Relationship Between FDCC and SCAP Product Compliance
- Applicability for SCAP Beyond FDCC
- Conclusion

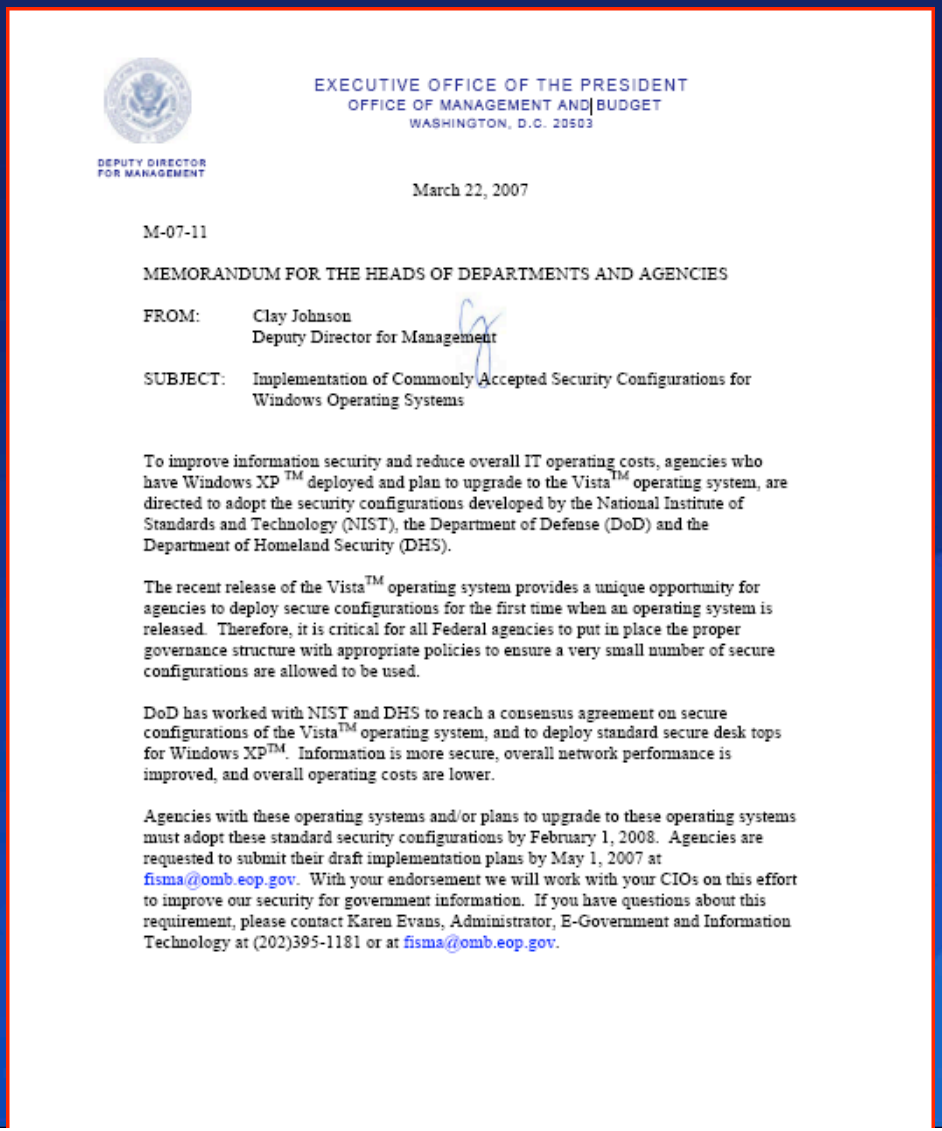
Current Compliance and Configuration Management



FDCC

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."

Security Content Automation Protocol

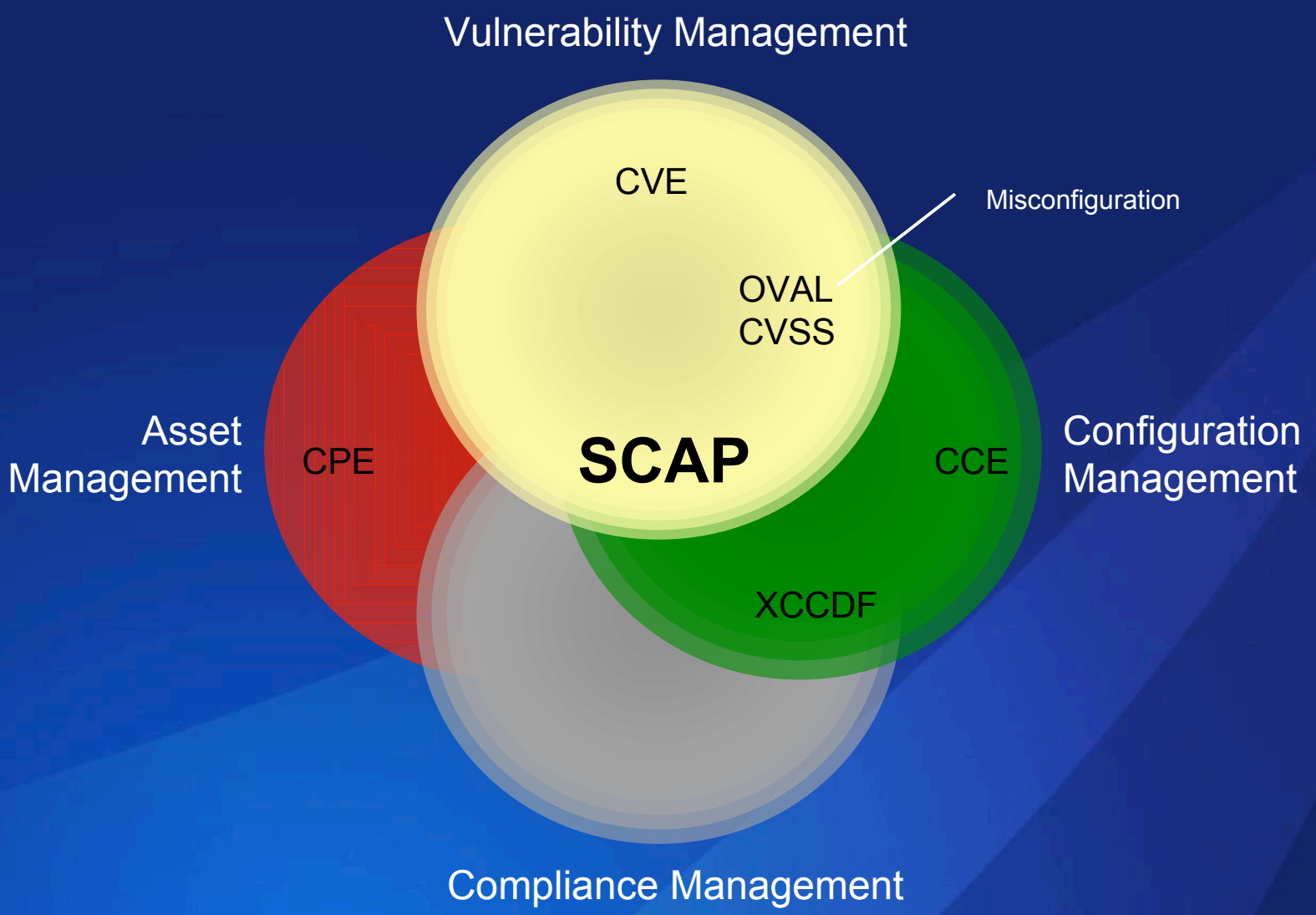
Standardizing How We Communicate

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
NSA	XCCDF	eXtensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
MITRE	OVAL	Open Vulnerability 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

FDCC

Integrating IT and IT Security Through SCAP



FDCC

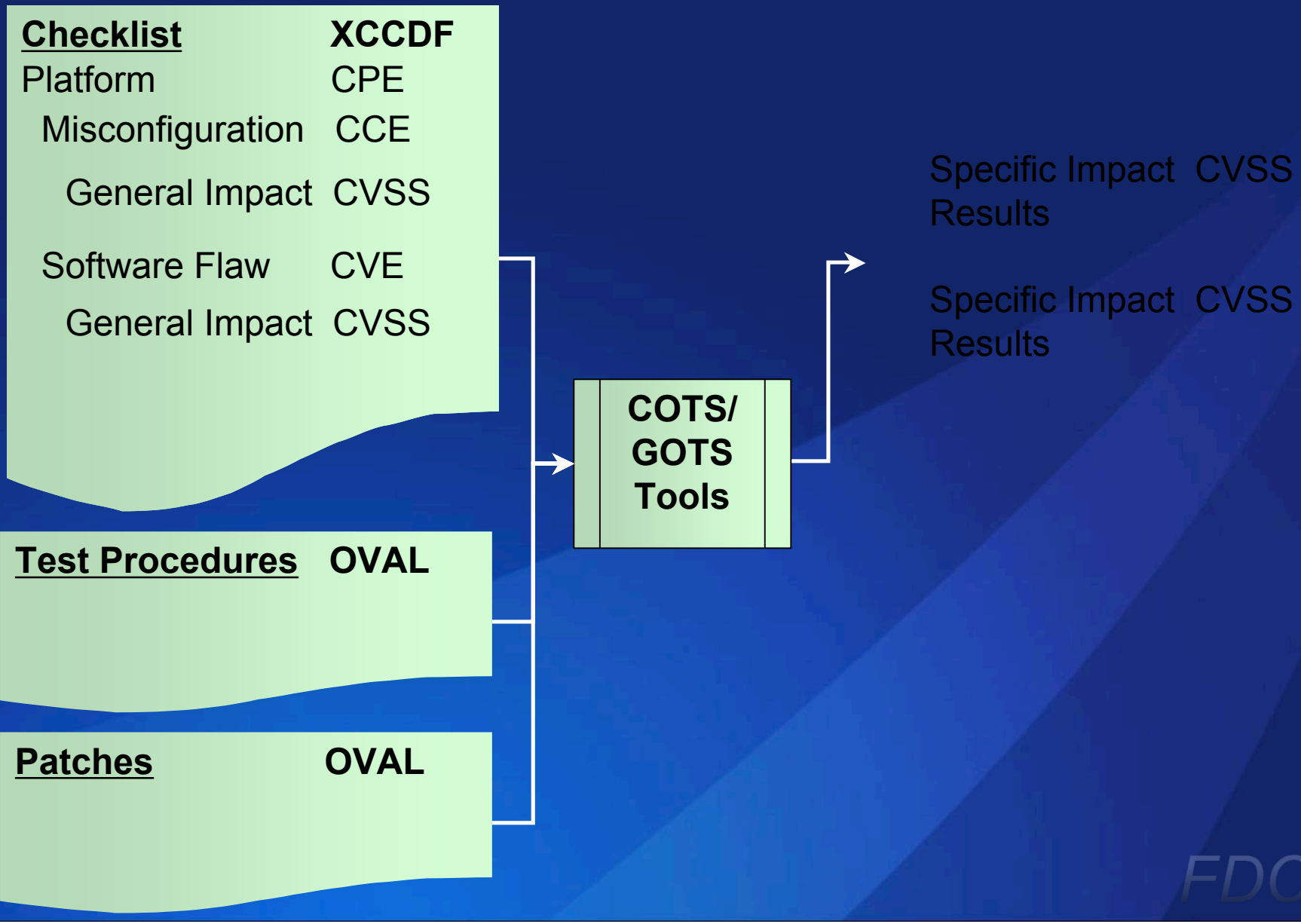
Existing Federal Services

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
- 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.
- Translating this backlog of checklists into the Security Content Automating Protocol (SCAP)

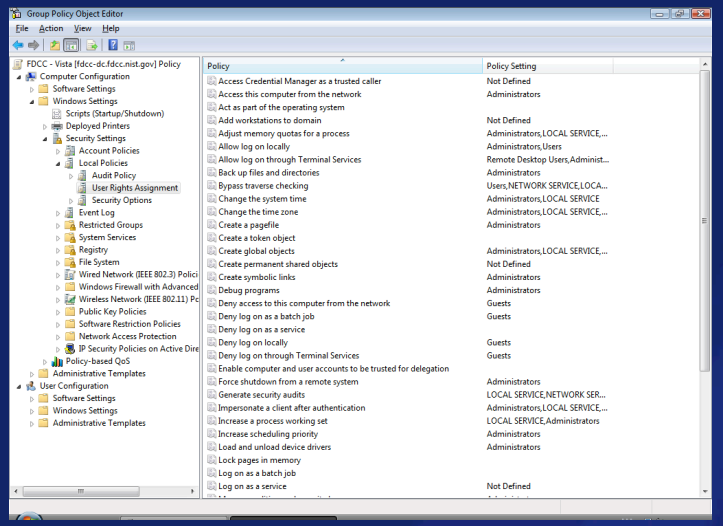
- 50 million hits per year
- 20 new vulnerabilities per day
- Mis-configuration cross references to:
  - NIST SP 800-53 Security Controls (All 17 Families and 163 controls)
  - DoD IA Controls
  - DISA VMS Vulnerability IDs
  - Gold Disk VIDs
  - DISA VMS PDI IDs
  - NSA References
  - DCID
  - ISO 17799
- 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



FDCC Testing

1. Implement FDCC settings on virtual machine images



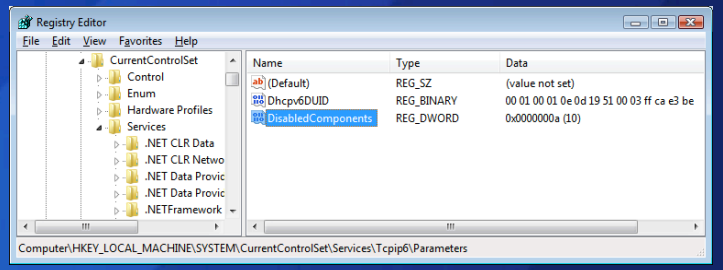
2. Use SCAP to verify FDCC settings were implemented correctly
   - Windows XP
   - Windows Vista
   - Windows XP Firewall
   - Windows Vista Firewall
   - Internet Explorer 7.0

ThreatGuard Secutor prime free

secure elements audit. evaluate. comply.

CS Compliance Platform

3. Reconcile any “failed” SCAP tests



4. Record any exceptions

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

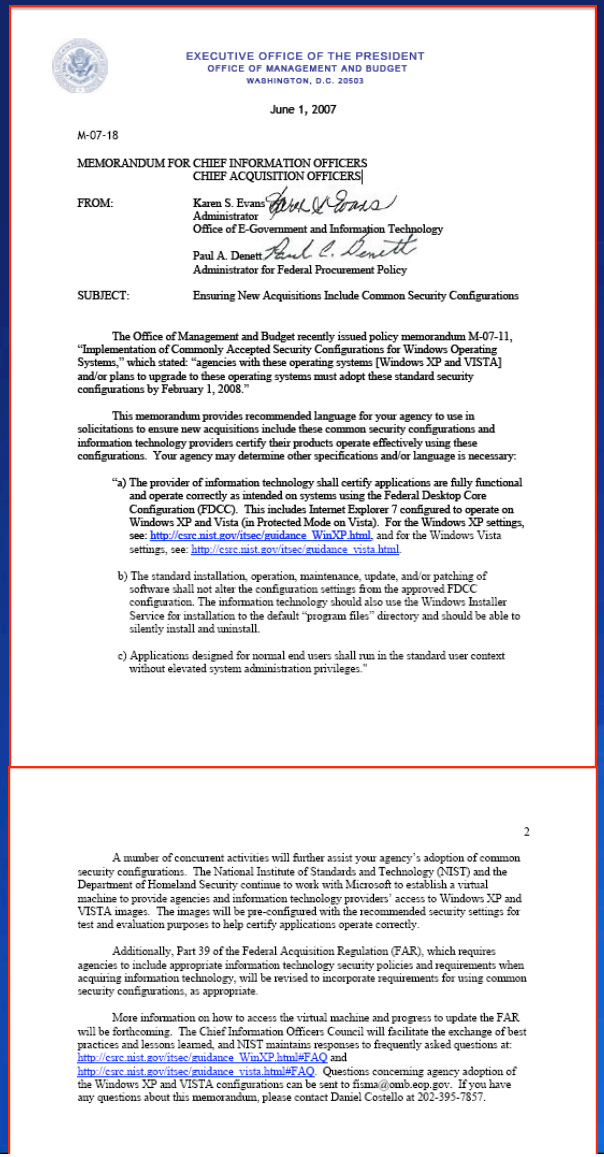
Quote from OMB Memo *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*

"**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. "

FDCC

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.** "

FDCC

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."**

FDCC

The Relationship Between FDCC and SCAP Product Compliance

SCAP Product

Self Asserts

SCAP Compliance

NIST

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?

FDCC

Stakeholders Value

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

Compliance Traceability within SCAP

```
<Group id="IA-5" hidden="true">
  <title>Authenticator Management</title>
    <reference>ISO/IEC 17799: 11.5.2, 11.5.3</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

Rational for security configuration

FDCC

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 Created and evolved with the broadest perspective
Utilizes configuration and asset management standards	Mobilizes asset inventory and configuration information for use in vulnerability and compliance management
Applicable to Federal Risk Management Framework – Assess, Monitor, Implement	Reduces time, effort, and expense of risk management process
Traceable to security mandates and guidelines	Automates portions of compliance demonstration and reporting
Keyed on NIST SP 800-53 security controls	Automates portions of FISMA compliance demonstration and reporting

Stakeholders and Contributors

DHS	Providing funding NVD partner, Supplying threat and patch info
NSA	Providing resources Applying the technology
DISA	Providing resources, Integrating into Host Based System Security (HBSS) and Enterprise Security Solutions
OSD	Incorporating into Computer Network Defense (CND) Data Strategy
DOJ	Incorporating into FISMA Cyber Security Assessment and Management (CSAM) tool
Army	Integrating Asset & Vulnerability Tracking Resource (AVTR) with DoD and SCAP content, Contributing patch dictionary
DOS	Incorporating into security posture by mapping SCAP to certification and accreditation process

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)
- Expo
  - Technology Demonstrations
  - Beta Testing and Use Case Presentation

More Information

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

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

- SCAP Checklists
- SCAP Capable Products

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

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

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

FDCC

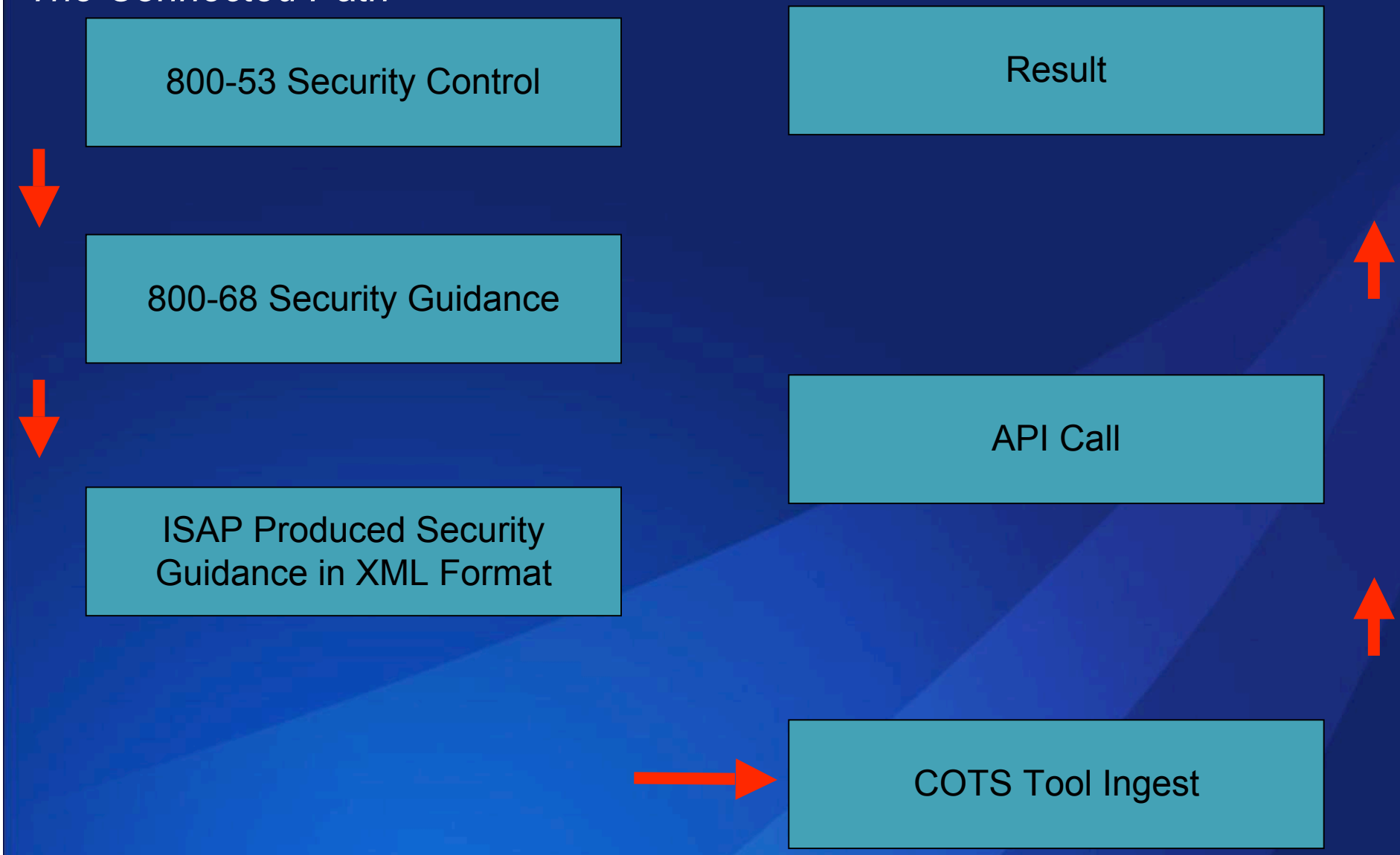
Questions

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

Supplemental – Connecting Compliance with Platform Assessment

Application to Automated Compliance

The Connected Path



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>
```

COTS Tool Ingest

API Call

lpHKey = "HKEY_LOCAL_MACHINE"

Path = "Software\Microsoft\Windows\"

Value = "5"

sKey = "AccountLockoutDuration"

Op = ">"

Result

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

FDCC

Supplemental – SCAP Platform Assessment Tutorial

FDCC

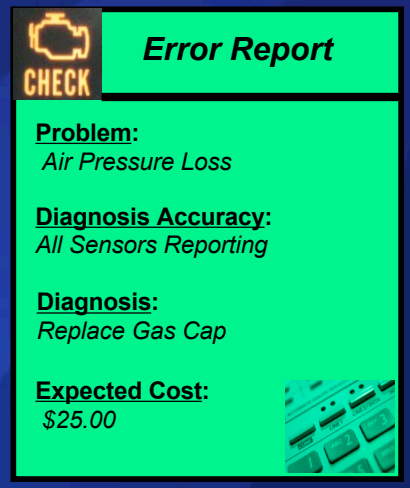
XML Made Simple

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>
```



FDCC

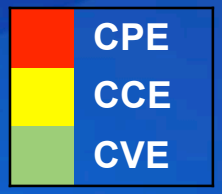
XML Made Simple

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

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



Supplemental – FAQ for NIST FISMA Documents

Fundamental FISMA Questions

What are the NIST Technical Security Controls?

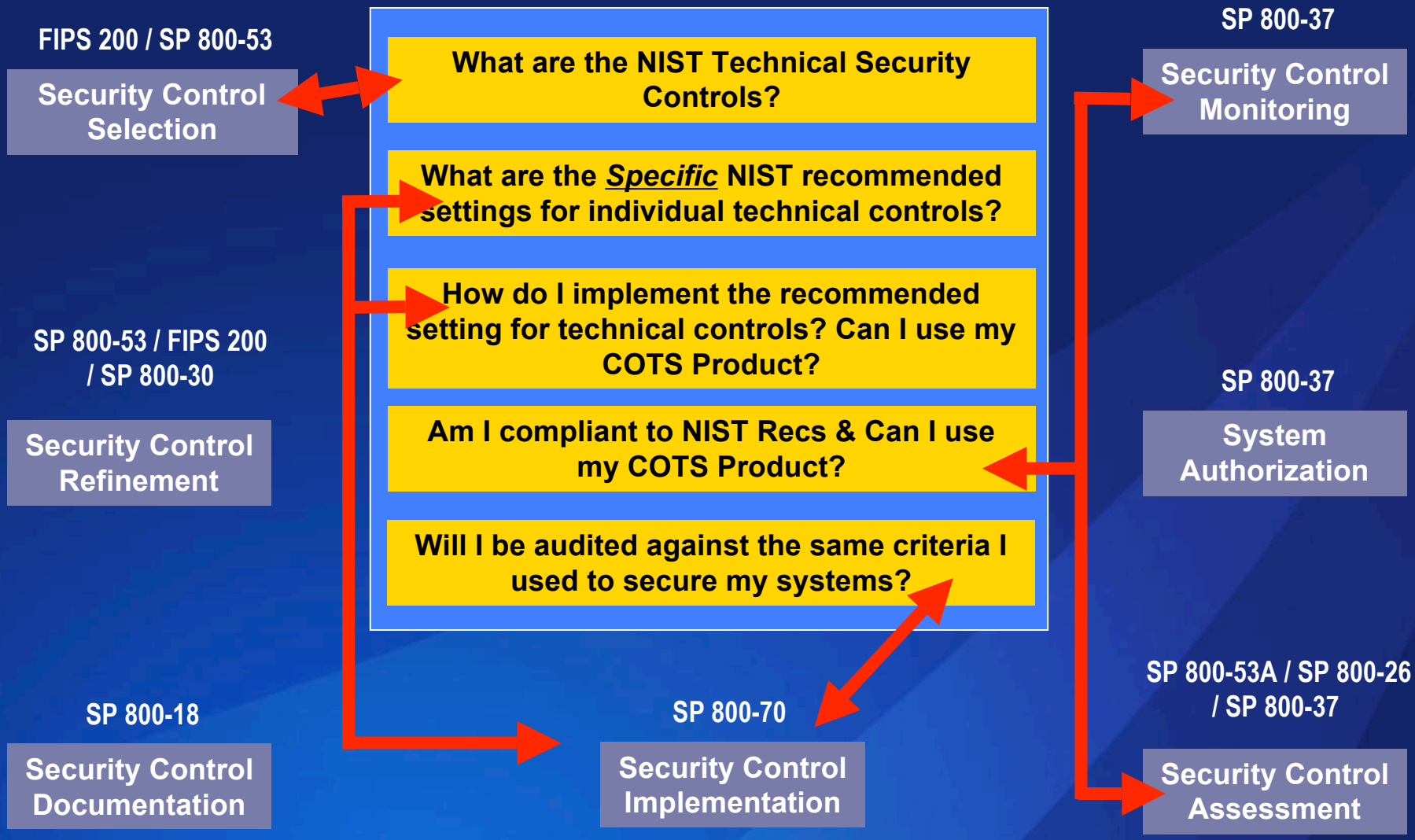
What are the *Specific* NIST recommended settings for individual technical controls?

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



FDCC