Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

Security Content Automation Program

automating compliance checking, vulnerability management, and security measurement

Automating Compliance Checking, Vulnerability Management, and Security Measurement

Peter Mell and Stephen Quinn

Computer Security Division

NIST

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

A DISA, NSA, and NIST Partnership Sponsored by DHS

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

Outline

- Security Content Automation Program
  - Objectives and Benefits
- FISMA and DOD Compliance Automation
  - How and why
- Enabling Automation Through Integration of Government and Industry Programs
- Technical Approach
- Status

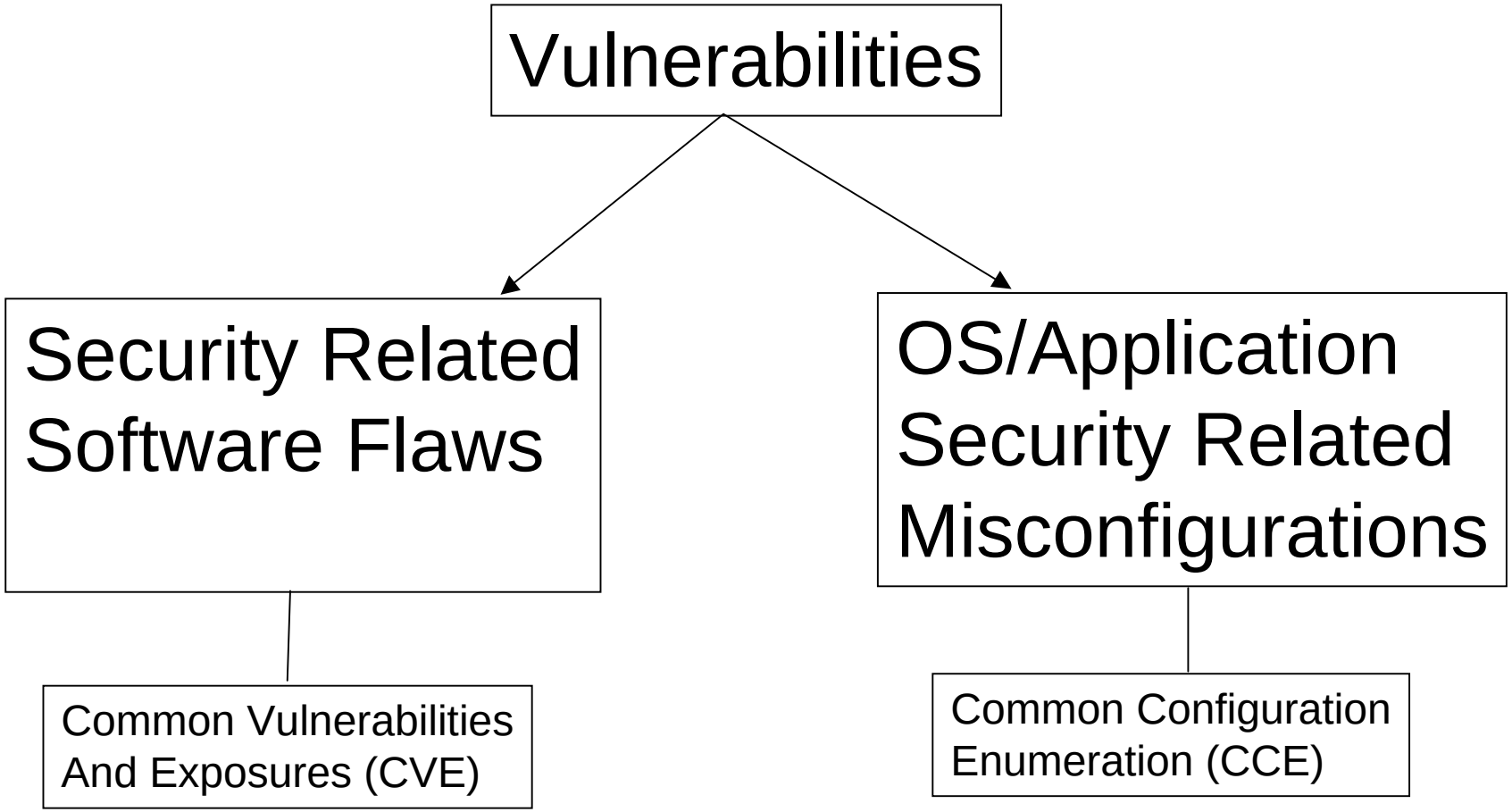
High Level Objectives

- Enable technical control compliance automation
  - Low level vulnerability checks to map to high level compliance requirements
- Enable standardized vulnerability management
  - Empower security product vendor community to perform on-demand, Government directed security and compliance audits
  - End user organization can specify requirements
  - COTS tools automatically perform checks
- Enable security measurement
  - FISMA scorecard have a quantitative component that map to actual low level vulnerabilities

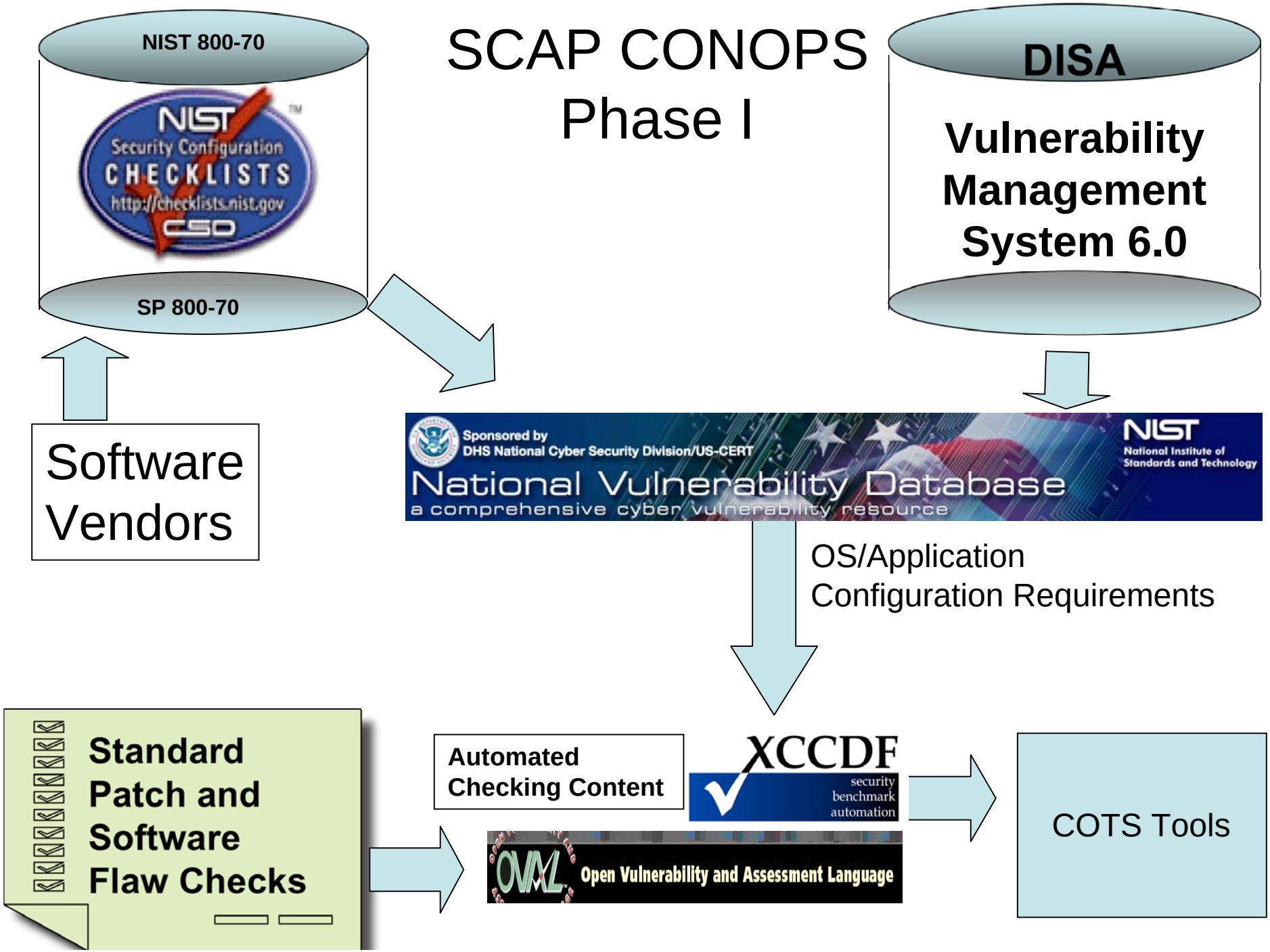
Additional Security Content Automation Program Objectives

- Replace Stove-pipe GOTS Approaches
- Establish vulnerability management standards
- Encourage product vendors (i.e. Microsoft, Sun, Oracle, Red Hat etc.) to provide direct support in the form of security guidance/content.

Covering the Vulnerability Landscape



SCAP CONOPS
Phase I



SCAP CONOPS- Phase I (continued…)

ThreatGuard
TENABLE Network Security
McAfee
symantec.
secure elements

Security Product Vendors
&
Point Solution Providers

ManTech International Corporation
G2
CSC EXPERIENCE. RESULTS.

Federal Agencies
DoD & Civil Security

Standardized Security Measurement

Agency Specified Vulnerability Management

Compliance

FISMA | HIPAA | SOX | GLB | INTEL | ISO | DoD 8500

Introductory Benefits

- Federal Agencies
  - Automation of technical control compliance (FISMA)
  - Ability of agencies to specify how systems are to be secured
  - Ability to measure security using standardized methods
- COTS Tool Vendors –
  - **Vendors compete on quality of tool, not the checking content**
  - Provision of an enhanced IT security data repository
    - No cost and license free
    - Standards based: CVE/OVAL/XCCDF/CVSS/CCE
    - Cover both software flaw and configuration issues
  - Elimination of duplication of effort/Cost reduction through standardization

Outline

- Security Content Automation Program
  - Objectives and Benefits
- FISMA and DOD Compliance Automation
  - How and why
- Enabling Automation Through Integration of Government and Industry Programs
- Technical Approach
- Status

Let’s Talk Compliance

Trying to be Accommodating

Guidance without Substance

The Right Path?

Rushing to Comply

Some Things are Obvious

Some Things are Confusing

Some Things Seem Misplaced

The Current Quagmire…

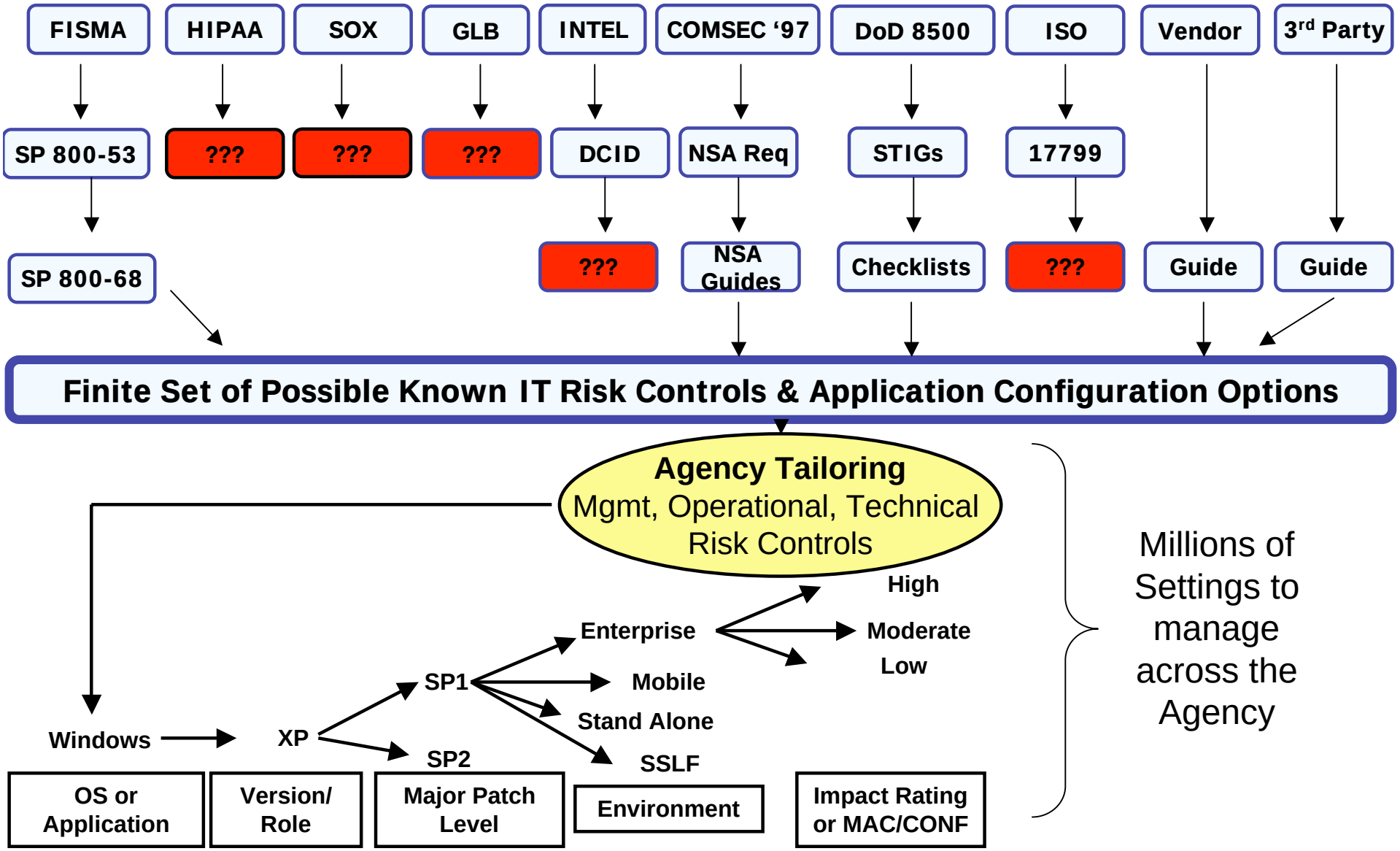
- Agency must secure system
  - Much of this is implementing and monitoring low level security settings
    - Ensure secure OS/Application installations (e.g., secure images)
    - Vulnerability mitigation/Patch application
    - Security monitoring
  - Insufficient funding available
- Agency much comply with regulations
  - Higher level security controls
  - Requires low level operational security to be performed but often implemented as a paperwork exercise
  - Consumes large amounts of resources

Compliance & Security

- Problem – Comply with policy.
- How – Follow recommended guidelines – So many to choose from.
- Customize to your environment – So many to address.
- Document your exceptions – I've mixed and matched, now what?
- Ensure someone reads your exceptions – Standardized reporting format.
- Should be basic:
  - One coin, different sides.
  - If I configure my system to compliance regulation does is mean its secure and vice versa?

The Compliance Game

Every high level policy should ultimately map to low level settings

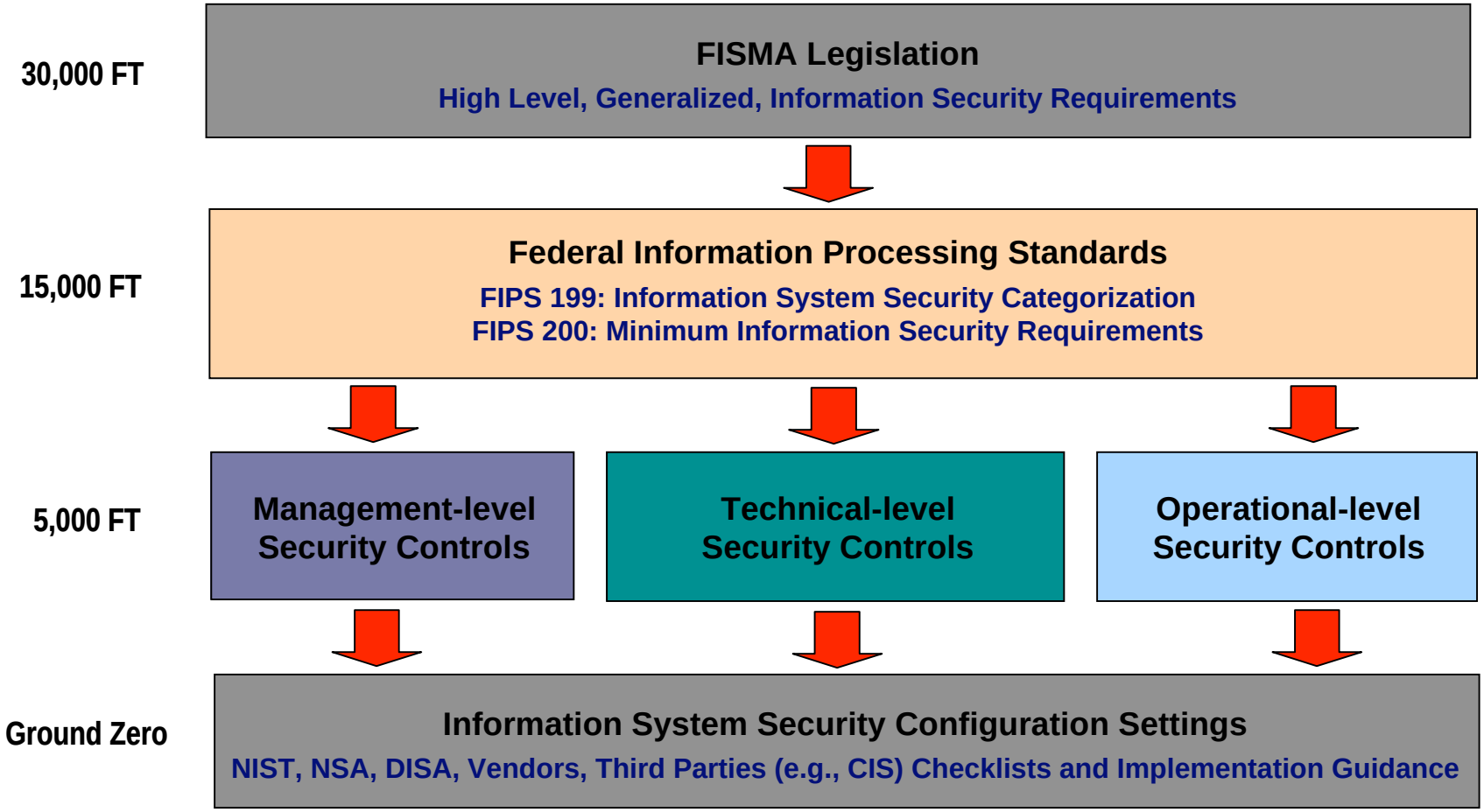


The Compliance Answer

- Reduce high level security requirements (e.g., 800-53 controls)?
- Congress provides more resources?

Standards Based Automation

FISMA Compliance Model



It is not possible to manually get from 30,000 ft to ground zero, automated security techniques must be employed

Common FISMA Statements

- While FISMA compliance is important, it can be complex and demanding.
- “Can parts of FISMA compliance be streamlined and automated”?
- “My organization spends more money on compliance than remediation”.

Fundamental FISMA Questions

What are the NIST Technical Security Controls?

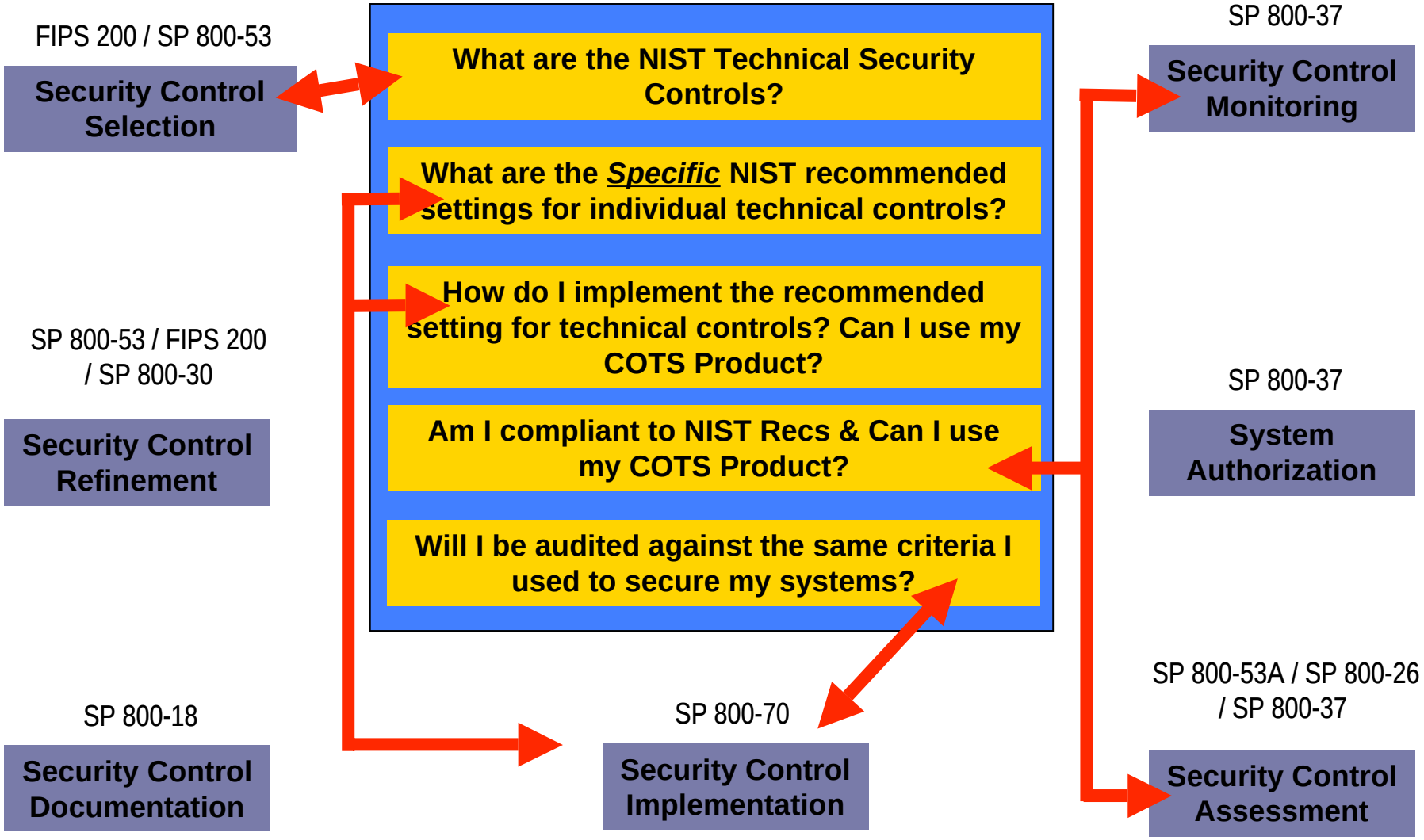
What are the *Specific* NIST recommended settings for individual technical controls?

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?

FISMA Documents



Automation of FISMA Technical Controls

COTS Tools

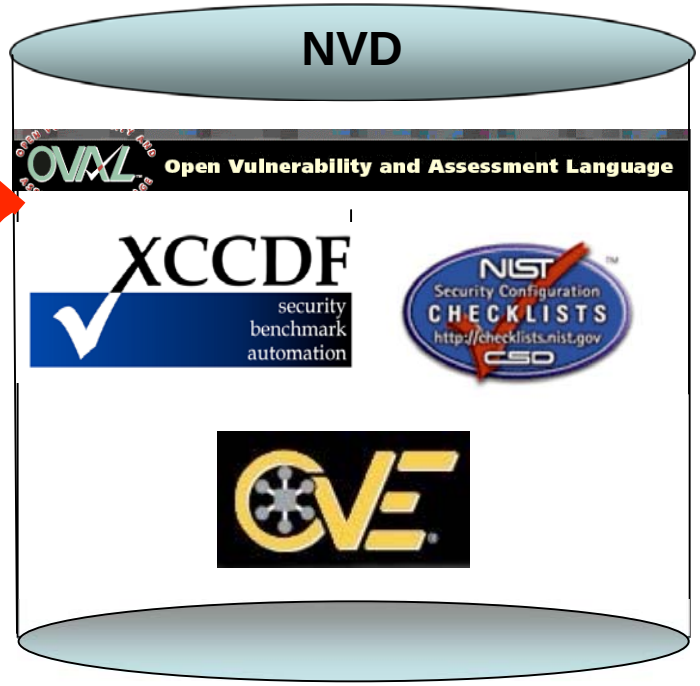
What are the NIST Technical Security Controls?

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

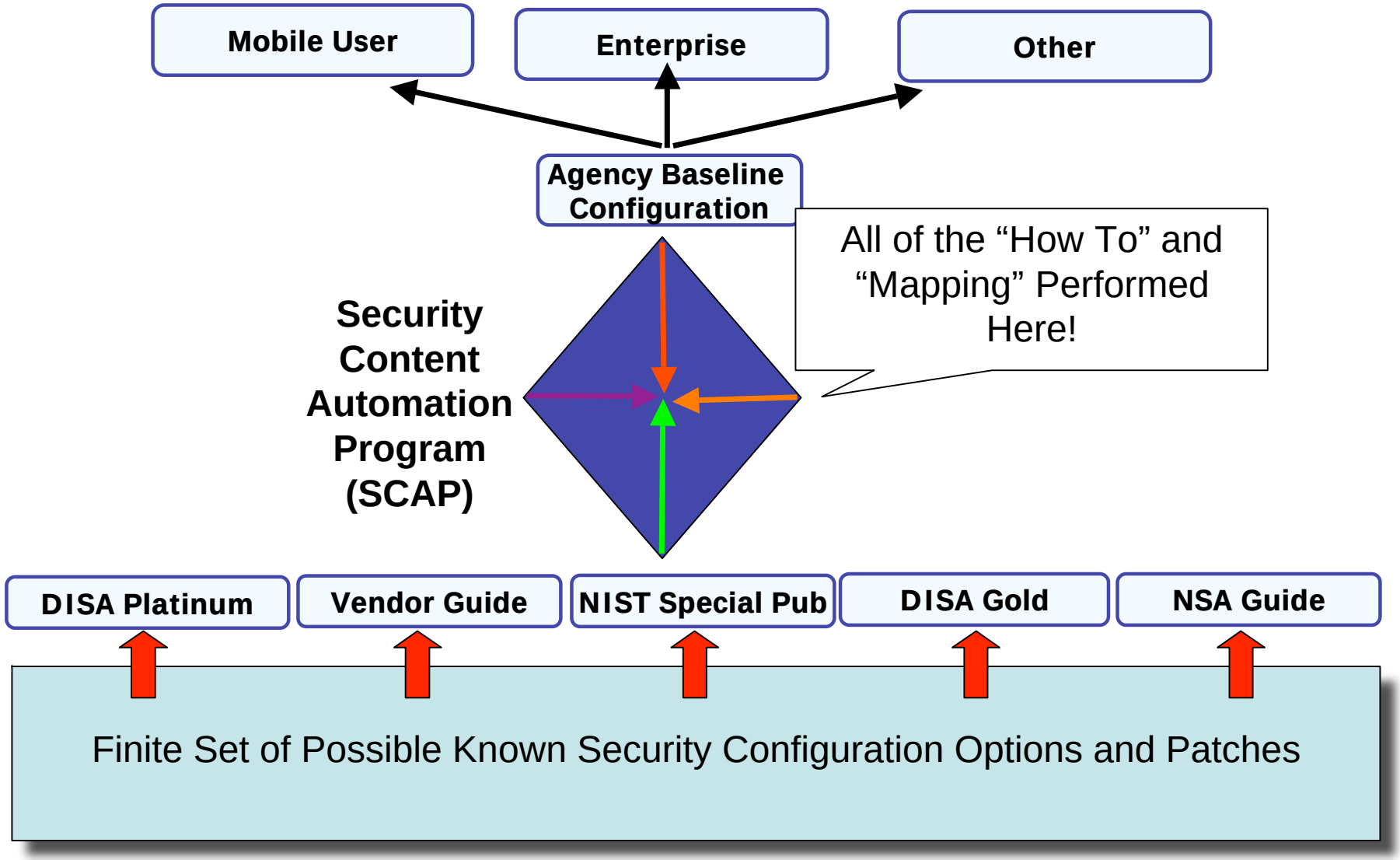
How do I implement the recommended setting for technical controls? Can I use my COTS Product?

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

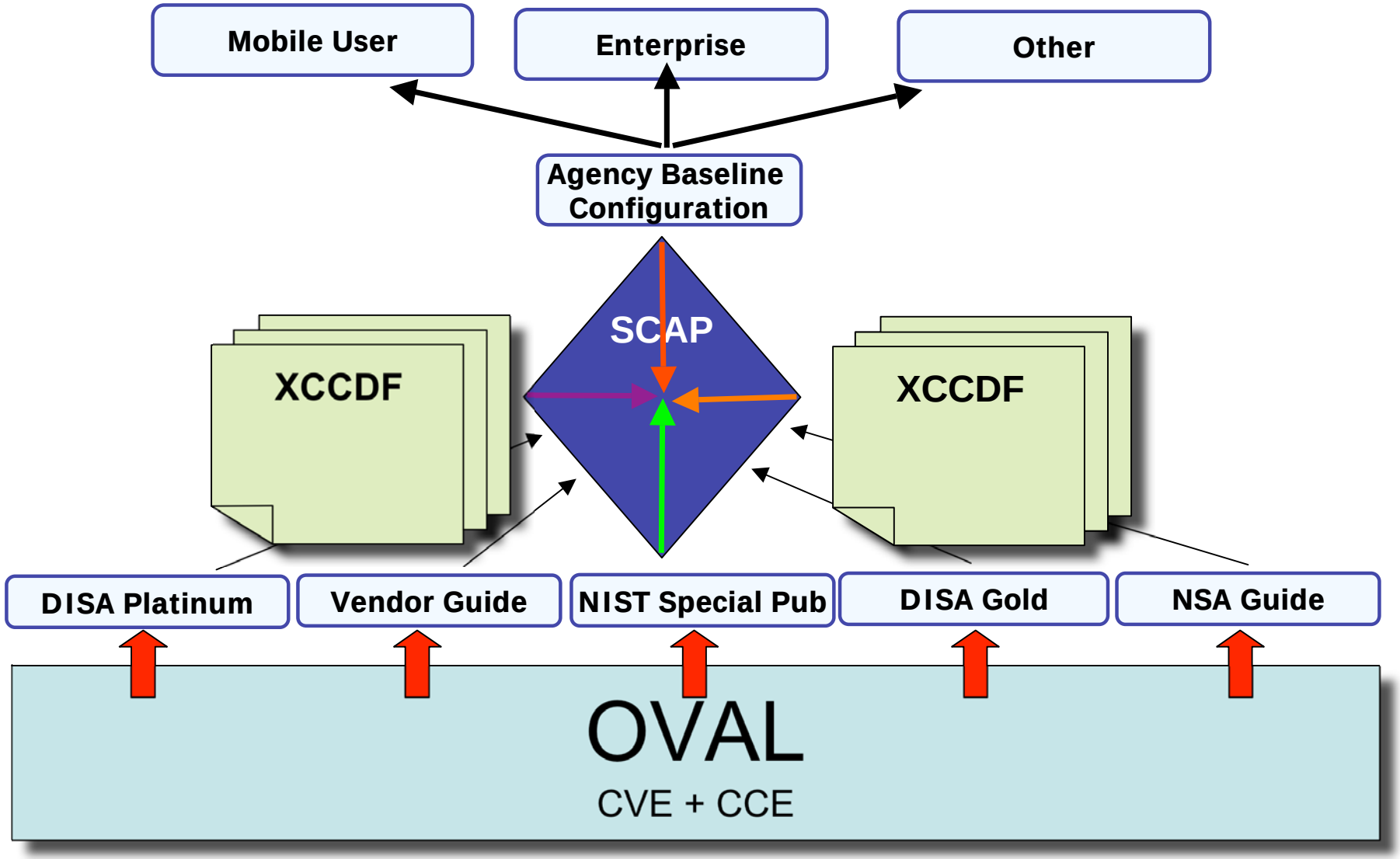
Will I be audited against the same criteria I used to secure my systems?



How Security Automation Helps



How Does This Work?



Number of Controls with Automated Validation Support

Cyber Security Assessment and Mgmt	Full Automation	21 (13%)
	Partial Automation	28 (17%)
Security Content Automation Program Machine-readable Security Report Formats	Full Automation:	31 (19%)
	Partial Automation:	39 (24%)
Future Automation Techniques or No Automation		44 (27%)
	Total Controls	163 (100%)

Inside The Numbers

- Importance/Priority
  - Securely configuring an IT system is of great importance.
- Complexity of Implementation
  - Provide Common Framework
  - Some controls require system-specific technical knowledge not always available in personnel.
- Labor
  - Some Controls (i.e. AC-3, CM-6, etc.) require thousands of specific checks to ensure compliance.

On the Schedule

- Windows Vista *
- Windows XP *
- Windows 2003 *
- Windows 2000
- Red Hat Enterprise Linux *
- Oracle
- Sun
- Windows desktop applications
- Web servers

* = Some beta content is available

Mappings To Policy & Identifiers

- FISMA Security Controls (All 17 Families and 163 controls for reporting reasons)
- DoD IA Controls
- CCE Identifiers (configuration issues)
- CVE Identifiers (software flaw issues)
- CVSS Scoring System (vulnerability impact)
- DISA Vulnerability Management System
  - Gold Disk
- NSA References
- Vendor References
- etc.

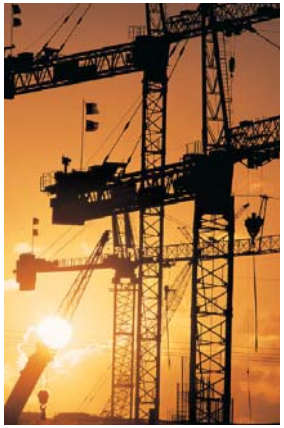
NIST Publications

- NIST Checklist Publication (Revised Special Publication 800-70)
- NIST IR – National Security Automation Program
- NIST IR 7275 – XCCDF version 1.1.2 (Draft Posted)

Outline

- Security Content Automation Program
  - Objectives and Benefits
- FISMA and DOD Compliance Automation
  - How and why
- Enabling Automation Through Integration of Government and Industry Programs
- Technical Approach
- Status

Combining Existing Initiatives



- **DISA**
  - STIG & Checklist Content
  - Gold Disk & VMS Research
- **FIRST**
  - Common Vulnerability Scoring System (CVSS)
- **MITRE**
  - Common Vulnerability Enumeration (CVE)
  - Common Configuration Enumeration (CCE)
  - Open Vulnerability & Assessment Language (OVAL)
- **NIST**
  - National Vulnerability Database
  - Checklist Program
  - Security Content Automation Program
- **NSA**
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Security Guidance & Content

Existing NIST Products

- National Vulnerability Database
  - 2.5 million hits per month
  - 16 new vulnerabilities per day
  - Integrated standards: 244 products, 22 vendors, 8 vendors 24 products
- Checklist Program
  - 115 separate guidance documents
  - Covers 140 IT products

National Vulnerability Database

- NVD is a comprehensive cyber security vulnerability database that:
  - Integrates all publicly available U.S. Government vulnerability resources
  - Provides references to industry resources.
  - It is based on and synchronized with the CVE vulnerability naming standard.
  - XML feed for all CVEs
  - http://nvd.nist.gov

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

Search CVE, Download CVE, Statistics, CVSS, Vendors, Contact, FAQ

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.

Resource Status

NVD contains:
20691 CVE Vulnerabilities
75 US-CERT Alerts
1698 US-CERT Vuln Notes
2966 Oval Queries
Last updated:
11/27/06
Publication rate:
16 vulnerabilities / day

Search CVE Vulnerability Database (Perform Advanced Search)

Keyword search: [ ] Search All

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search last 3 months | Search last 3 years

Show only vulnerabilities that have the following associated resources:

- [ ] US-CERT Technical Alerts
- [ ] US-CERT Vulnerability Notes
- [ ] OVAL Queries

Automated FISMA and Compliance Metrics (NSA/DISA/NIST Beta Site)!!

The Security Content Automation Program (SCAP) is a public free repository of security content to be used for automating technical control compliance activities (e.g. FISMA/800-53), vulnerability checking (both application misconfigurations and software flaws), and security measurement.

New CVE Community Service!!

NVD announces a new service to allow software development organizations to make official statements regarding the set of CVE vulnerabilities that apply to their products. They can now provide the CVE community (300+ products and services) deeper insight into the vulnerabilities within their products. For example, they can dispute third party vulnerability information, clarify vulnerability applicability, provide configuration and remediation

National Vulnerability Database - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://nvd.nist.gov/nvd.cfm?startrow=1 Go Links

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

Search CVE, Download CVE, Statistics, CVSS, Contact, FAQ

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.

Resource Status

NVD contains:
16418 CVE Vulnerabilities
54 US-CERT Alerts
1245 US-CERT Vuln Notes
1162 Oval Queries
Last updated:
04/14/06
Publication rate:
17 vulnerabilities / day

Workload Index

Vulnerability Workload Index: 6.89

Email List

Enter your e-mail address and press "Add" to receive NVD announcements.

Add

About Us

NVD is a product of the

There are **28** matching records. Displaying matches **1** through **20**.

Next 20 Matches

CVE-2006-0012 TA06-101A VU#641460

Summary: Unspecified vulnerability in Windows Explorer in Microsoft Windows 2000 SP4, XP SP1 and SP2, and Server 2003 SP1 allows remote attackers to execute arbitrary code via attack vectors involving COM objects and "crafted files and directories," aka the "Windows Shell Vulnerability."
Published: 4/11/2006
CVSS Severity: 5.6 (Medium)

CVE-2006-0003 TA06-101A VU#234812

Summary: Unspecified vulnerability in the RDS.Dataspace ActiveX control, which is contained in ActiveX Data Objects (ADO) and distributed in Microsoft Data Access Components (MDAC) 2.7 and 2.8, allows remote attackers to execute arbitrary code via unknown attack vectors.
Published: 4/11/2006
CVSS Severity: 5.6 (Medium)

CVE-2006-1189 TA06-101A VU#341028

Summary: Unspecified vulnerability in Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via a crafted URL with double-byte characters, aka the "Double Byte Character Parsing Memory Corruption Vulnerability."
Published: 4/11/2006
CVSS Severity: 10.0 (High)

CVE-2006-1188 TA06-101A VU#824324

Summary: Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via HTML elements with a certain crafted tag, which leads to memory corruption.
Published: 4/11/2006
CVSS Severity: 7.0 (High)

CVE-2006-1186 TA06-101A

Summary: Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via by instantiating the (1) Mdt2gddr.dll, (2) Mdt2dd.dll, and (3) Mdt2gddo.dll COM objects as ActiveX controls, which leads to memory corruption.
Published: 4/11/2006
CVSS Severity: 10.0 (High)

CVE-2006-1185 TA06-101A VU#503124

Summary: Unspecified vulnerability in Microsoft Internet Explorer 5.01 through 6 allows

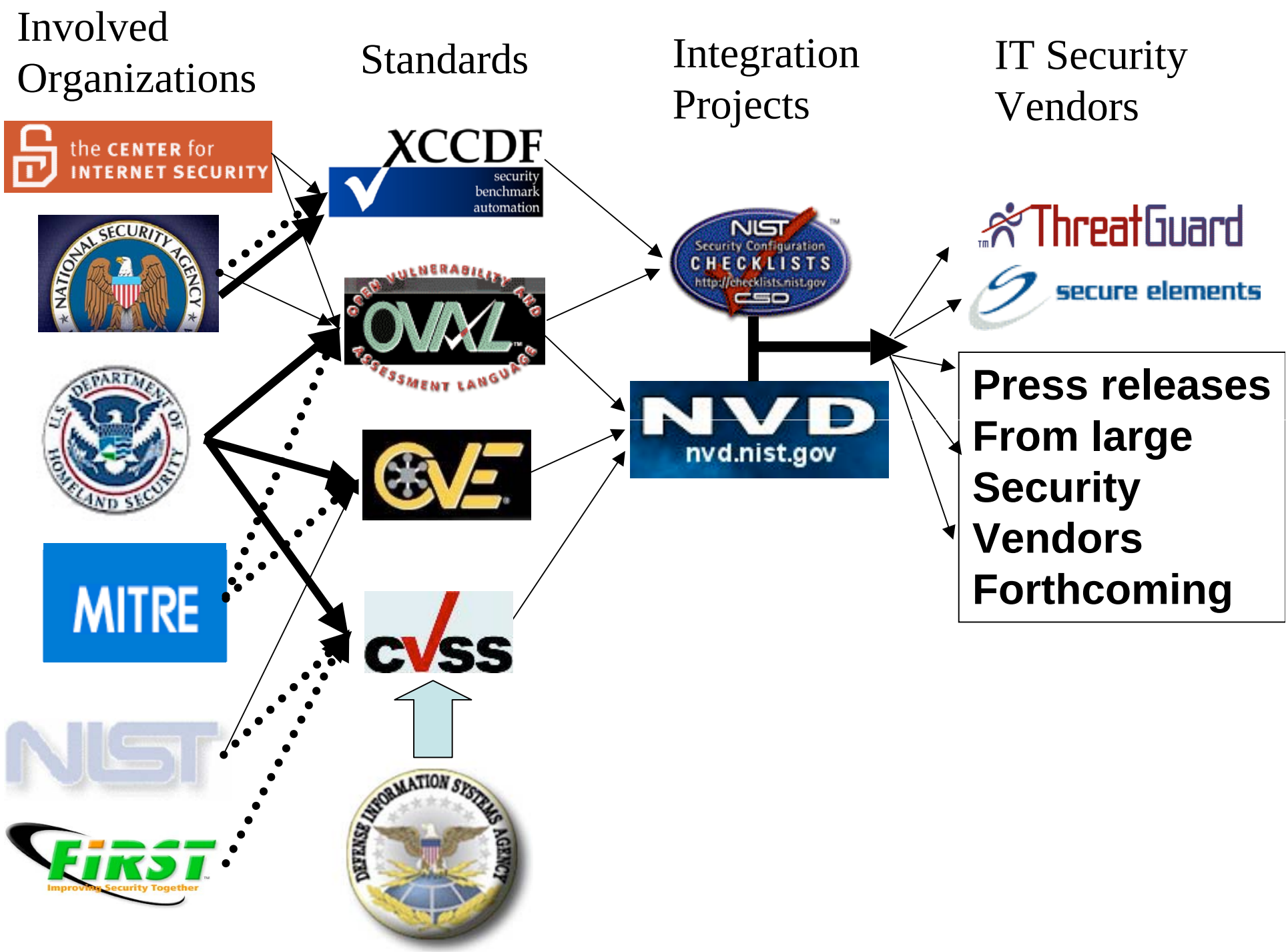
Internet

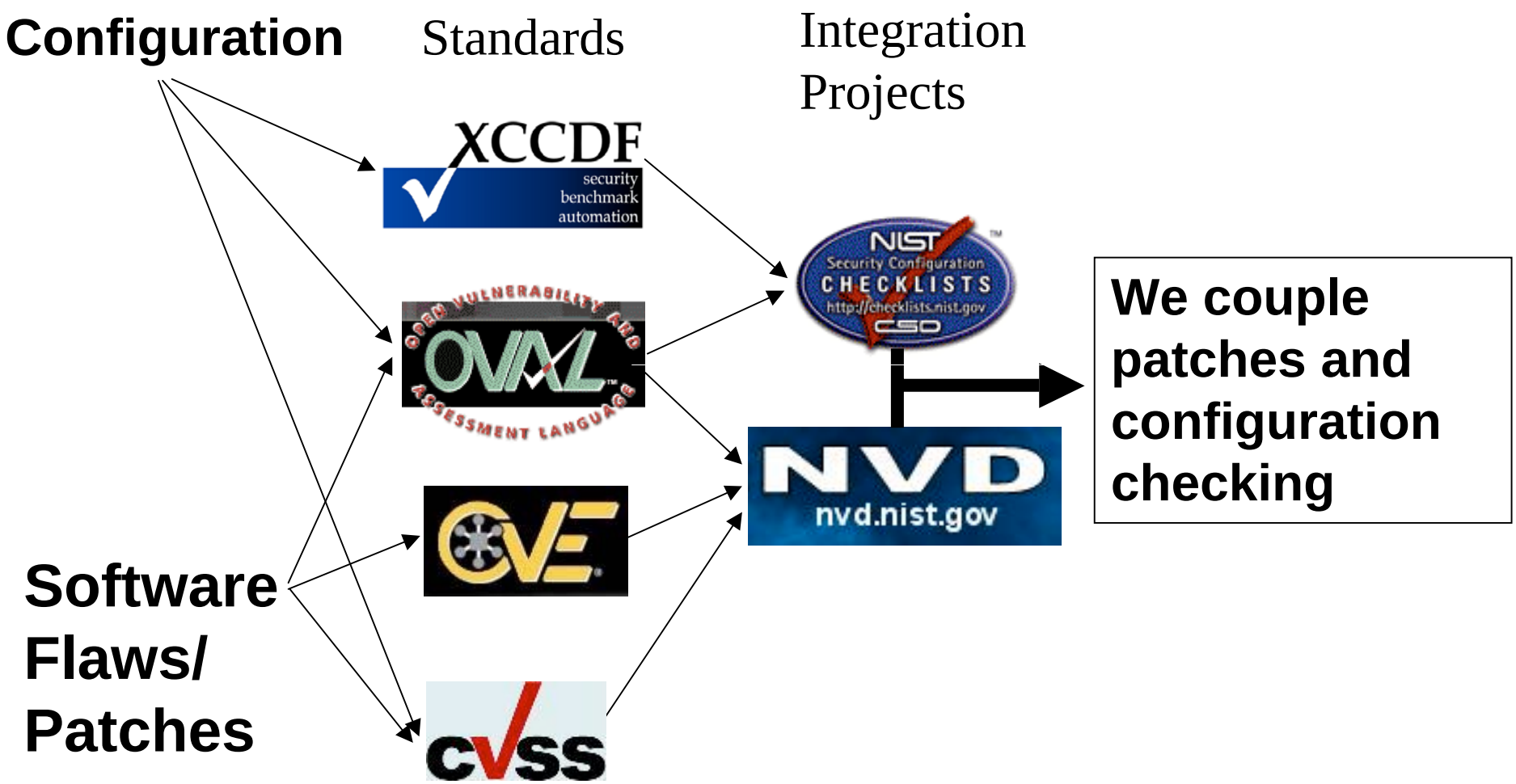
NIST Checklist Program

- In response to NIST being named in the Cyber Security R&D Act of 2002.
- Encourage Vendor Development and Maintenance of Security Guidance.
- Currently Hosts 115 separate guidance documents for over 140 IT products.
  - In English Prose and automation-enabling formats (i.e. .inf files, scripts, etc.)
- Need to provide configuration data in standard, consumable format.
- http://checklists.nist.gov

eXtensible Configuration Checklist Description Format

- Developed by the NSA
- Designed to support:
  - Information Interchange
  - Document Generation
  - Organizational and Situational Tailoring
  - Automated Compliance Testing and Scoring
- Published as NIST IR 7275
- Foster more widespread application of good security practices
- http://nvd.nist.gov/scap/xccdf/xccdf.cfm


Involved Organizations
Standards
Integration Projects
IT Security Vendors
the CENTER for INTERNET SECURITY
NATIONAL SECURITY AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY
MITRE
NIST
FIRST
Improving Security Together
XCCDF
security benchmark automation
OVAL
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
CVE
CVSS
DEFENSE INFORMATION SYSTEMS AGENCY
NIST Security Configuration CHECKLISTS
http://checklists.nist.gov
CSO
NVD
nvd.nist.gov
ThreatGuard
secure elements
Press releases From large Security Vendors Forthcoming


Configuration
Standards
Integration Projects
XCCDF
security benchmark automation
OVAL
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
CVE
CVSS
NIST Security Configuration CHECKLISTS
http://checklists.nist.gov
CSD
NVD
nvd.nist.gov
We couple patches and configuration checking
Software Flaws/ Patches

Outline

- Security Content Automation Program
  - Objectives and Benefits
- FISMA and DOD Compliance Automation
  - How and why
- Enabling Automation Through Integration of Government and Industry Programs
- Technical Approach
- Status

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>
```

XCCDF & OVAL Made Simple

XCCDF - eXtensible Checklist Configuration Description Format

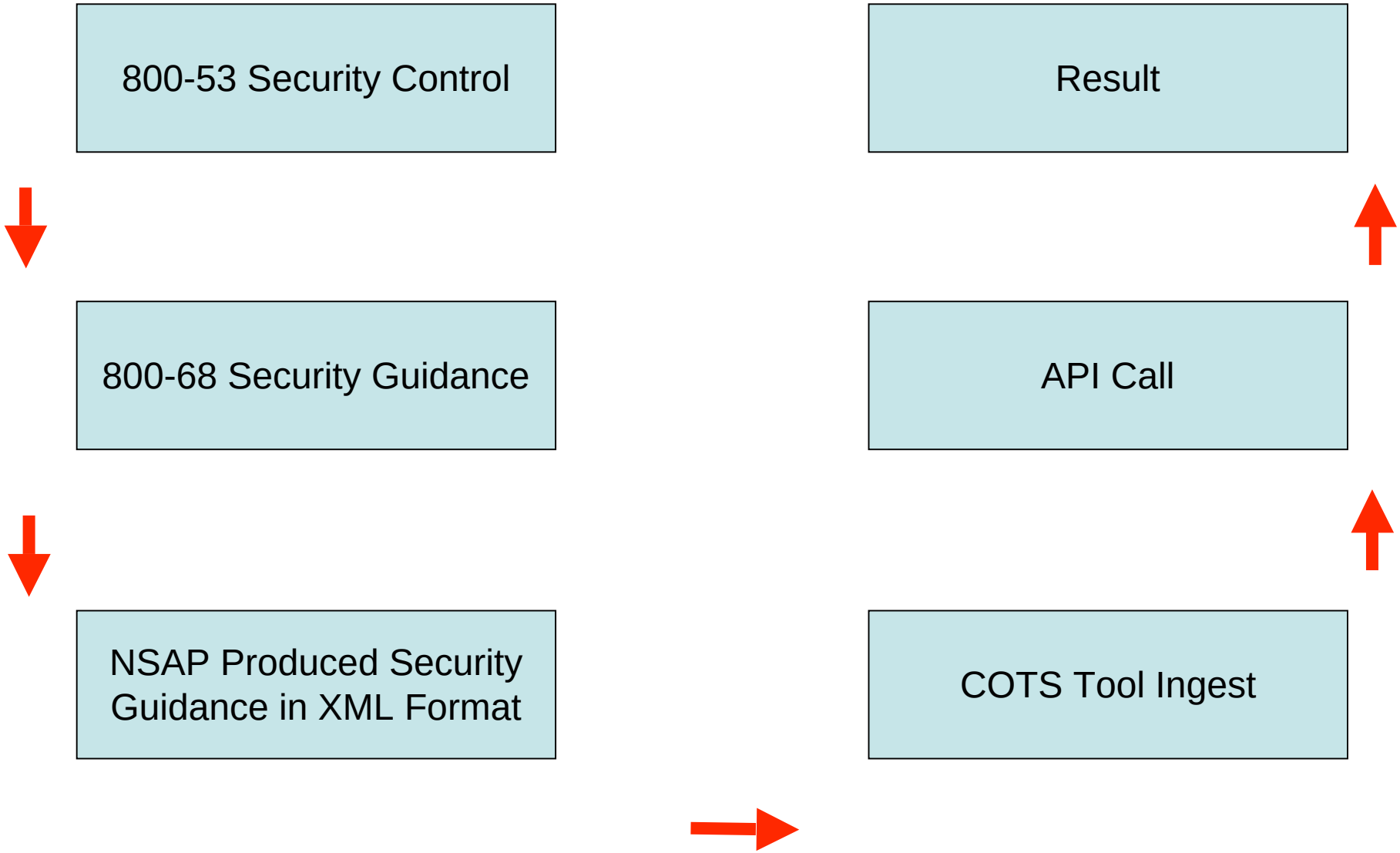
```
<Document ID> NIST SP 800-68
  <Date> 04/22/06 </Date>
    <Version> 1 </Version>
    <Revision> 2 </Revision>
 <Platform> Windows XP
    <Check1> Password >= 8 <>
    <Check2> FIPS Compliant <>
  </Maintenance>
 </Description>
</Car>
```

OVAL – Open Vulnerability Assessment Language

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

Application to Automated Compliance

The Connected Path



Application to Automated Compliance

800-53 Security Control
DISA STIG

AC-7 Unsuccessful Login

800-68 Security Guidance
DISA Checklist
NSA Guide

AC-7: Account Lockout Duration

AC-7: Account Lockout Threshold

NSAP 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);
```

Security Measurement

- How secure is my computer?
  - Measure security of the configuration
    - Measure conformance to recommended application and OS security settings
    - Measure the presence of security software (firewalls, antivirus…)
  - Measure presence of vulnerabilities (needed patches)
- How well have I implemented the FISMA requirements (NIST SP800-53 technical controls)?
  - Measure deviation from requirements
  - Measure risk to the agency

Setting Ground Truth/Defining Security

FISMA/FIPS 200
800-53

Required technical security controls

For each OS/application

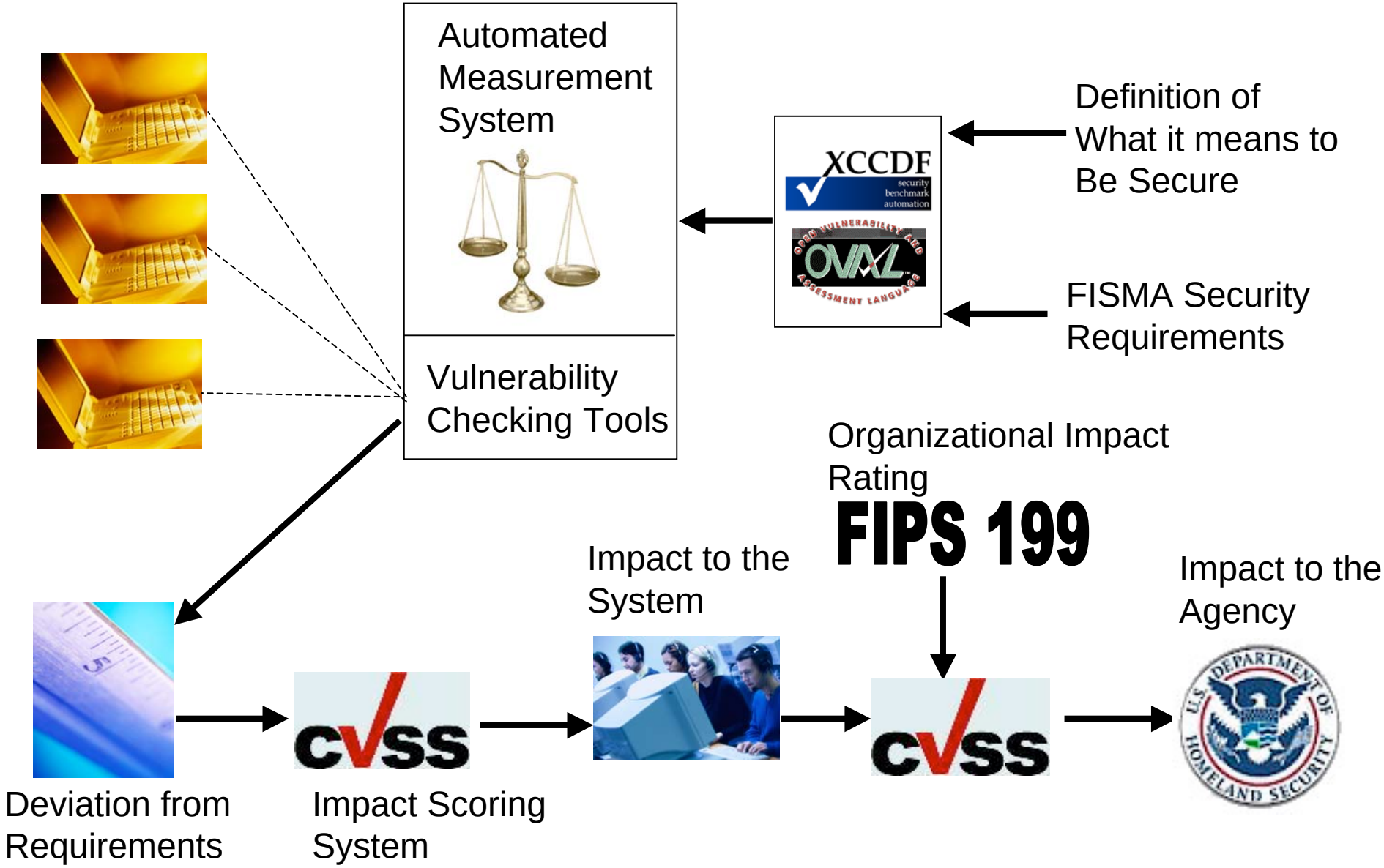
List of all known vulnerabilities

Secure Configuration Guidance

Low Level Checking Specification

Security Specifications for Platforms And Application
- Vulnerabilities
- Required Configurations
- Necessary Security Tools

Automated Security Measurement System



Configuration Guidance in the Context of 800-53/FIPS 199

- 800-53, Appendix D specifies security control applicability according to High, Moderate, and Low impact rating of an IT System.
- 800-68 provides specific configuration information according to environment (Standalone, Enterprise, SSLF, and Legacy)
- The NIST XML specifies the applicable 800-68 security settings according to the 800-53 guidelines.

EXAMPLE:

- AC-12 (session termination) is applicable for IT systems with either moderate or high impact rating, but not for system rated at a low.
- The XCCDF profile for High and Moderate systems enables the group for AC-12 rule execution, but disables the group for low system.
- The XCCDF rules ‘refer’ to the appropriate OVAL definitions in the companion OVAL file (named: WindowsXP-SP800-68.xml)

Outline

- Security Content Automation Program
  - Objectives and Benefits
- FISMA and DOD Compliance Automation
  - How and why
- Enabling Automation Through Integration of Government and Industry Programs
- Technical Approach
- Status

Security Content Automation Program (SCAP) Status

NIST,DISA,NSA Security Automation Conference

- September 2006
- 250+ attendees
- Keynote addresses by DISA CIAO Richard Hale, DOJ CISO Dennis Heretick, and NSA's Vulnerability Analysis and Operations Group Chief Tony Sager)

- SCAP Beta Web Site / Repository
  - Deployed on October 20th.
  - http://nvd.nist.gov/scap/scap.cfm

SCAP Tool Vendor Adoption

Tool Vendor Adoption of SCAP

ThreatGuard (fr

Secure Elemer

Tenable Nessus (under development)

Asserted Statements of Compliance to SCAP

Symantec (not received)

McAfee (not received)

ASG (received)

ManTech (evaluating)

CSC (evaluating)

Beta Security Automation Files Available

- Windows Vista
  - Misconfigurations
  - DISA/NSA/NIST, Microsoft, Air Force policies
- Windows XP
  - Misconfigurations/Software flaws
  - NIST FISMA and DISA policies (SP 800-68 / Gold Disk)
- Windows Server 2003
  - Misconfigurations/Software flaws
  - Microsoft and NIST FISMA policies
- Red Hat Enterprise Linux
  - Software flaws

Many more under development!!

Questions?

Peter Mell (NVD / SCAP)
Stephen Quinn (SCAP / NIST Checklist Program)
Computer Security Division
NIST, Information Technology Laboratory
mell@nist.gov, stquinn@nist.gov