Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database
a comprehensive cyber vulnerability resource

Automated Security Compliance and Measurement

Stephen Quinn & Peter Mell

Computer Security Division

NIST

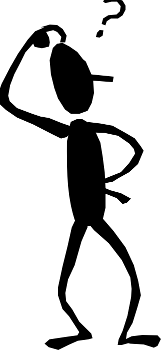
NIST™
Security Configuration
CHECKLISTS
http://checklists.nist.gov
CSD

I’m from the Federal Government…

and I’m here to help you!!

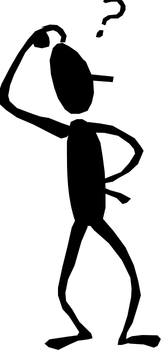
Introductory Benefits

- COTS Tool Vendors –
  - Provision of an enhanced IT security data repository
    - No cost and license free
    - CVE/OVAL/XCCDF/CVSS/CCE
    - Cover both patches and configuration issues
  - Elimination of duplication of effort
  - Cost reduction through standardization
- Federal Agencies
  - Automation of technical control compliance (FISMA)
  - Ability of agencies to specify how systems are to be secured



Current Problems

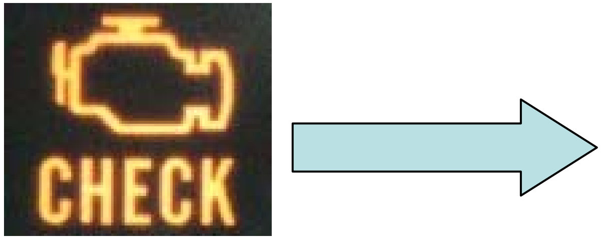
Conceptual Analogy



Current Problems

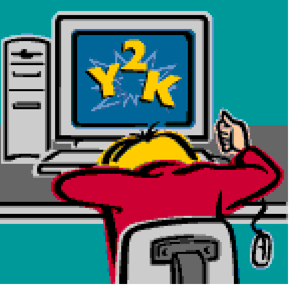
Conceptual Analogy Continued (2)

Outsource



National Institute for
AUTOMOTIVE
SERVICE
EXCELLENCE

In-House



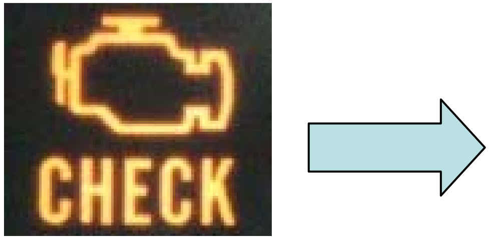
Current Problems

Conceptual Analogy Continued (3)

Outsource

Ford

PORSCHE



ASE National Institute for AUTOMOTIVE SERVICE EXCELLENCE

In-House

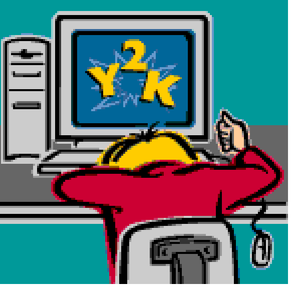
a.) Troubleshoot/Analyze

- Conduct Testing
- Is there a problem?
- Cause of error condition?
- Is this check reporting correctly?

b.) Document/Report Findings

c.) Recommendations

d.) Remediate



Current Problems

Conceptual Analogy Continued (5)

Standardize & Automate

a.) Troubleshoot/Analyze

- Is there a problem?
- Cause of error condition?
- Is this check reporting correctly?

More DATA

Outsource

In-House

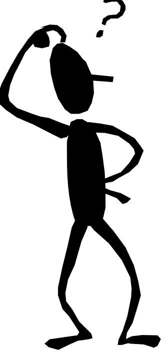
a.) Troubleshoot/Analyze

- Conduct Testing
- Is there a problem?
- Cause of error condition?
- Is this check reporting correctly?

b.) Document/Report Findings

c.) Recommendations

d.) Remediate

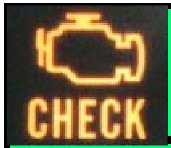


Current Problems

Conceptual Analogy Continued (6)

Before

After



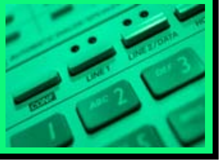
Error Report

Problem:
Air Pressure Loss

Diagnosis Accuracy:
All Sensors Reporting

Diagnosis:
Replace Gas Cap

Expected Cost:
$25.00



Let’s Talk Compliance

STOP WHEN FLASHING
BI

ORF 649

ONE WAY
NOT
TER
ONG
AY
ONE WA Y

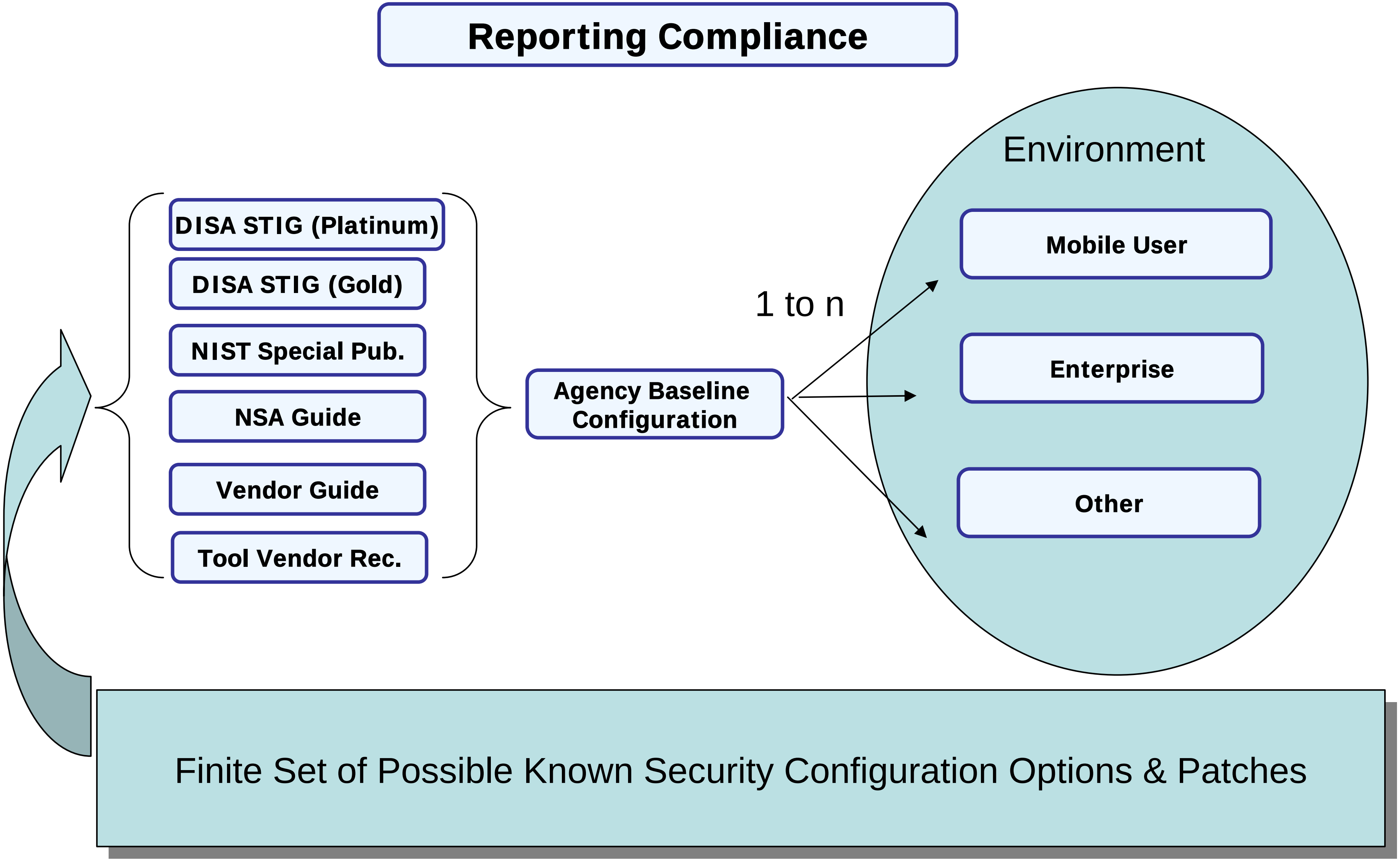
Compliance & Security

- 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 Current Quagmire…

- Agency must secure system.
- Agency much comply with regulations.
- Agency must use certain guidelines.
- Agency must ensure IT system functionality.
- Agency must report compliance after customization and ensuring functionality.
- Agency must report.
- Agency must be heard and understood.

…Looks Like This…



Reporting Compliance

DISA STIG (Platinum)

DISA STIG (Gold)

NIST Special Pub.

NSA Guide

Vendor Guide

Tool Vendor Rec.

Agency Baseline Configuration

1 to n

Environment

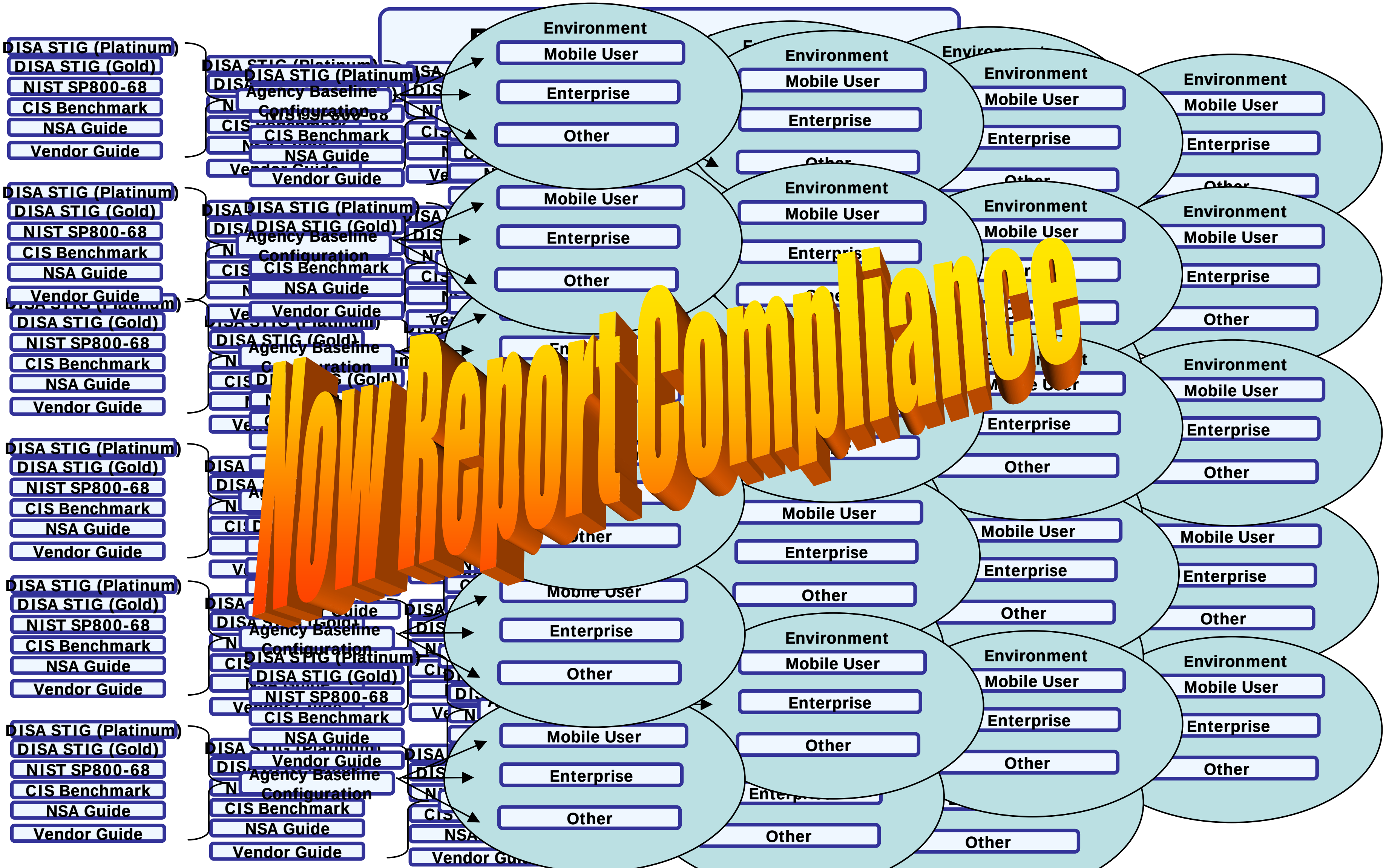
Mobile User

Enterprise

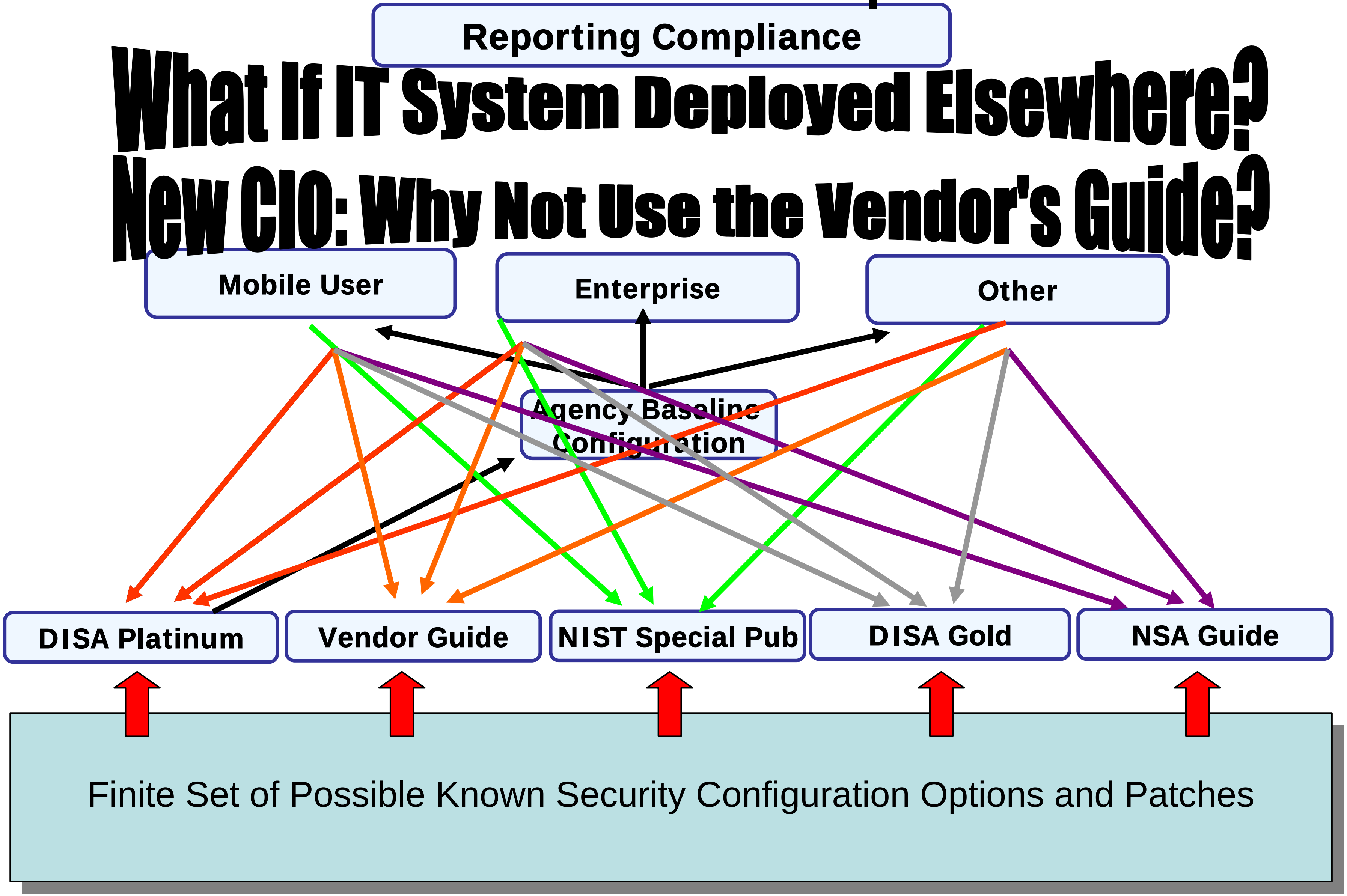
Other

Finite Set of Possible Known Security Configuration Options & Patches

…Looks Like This.



A Closer Look At Operations



Reporting Compliance

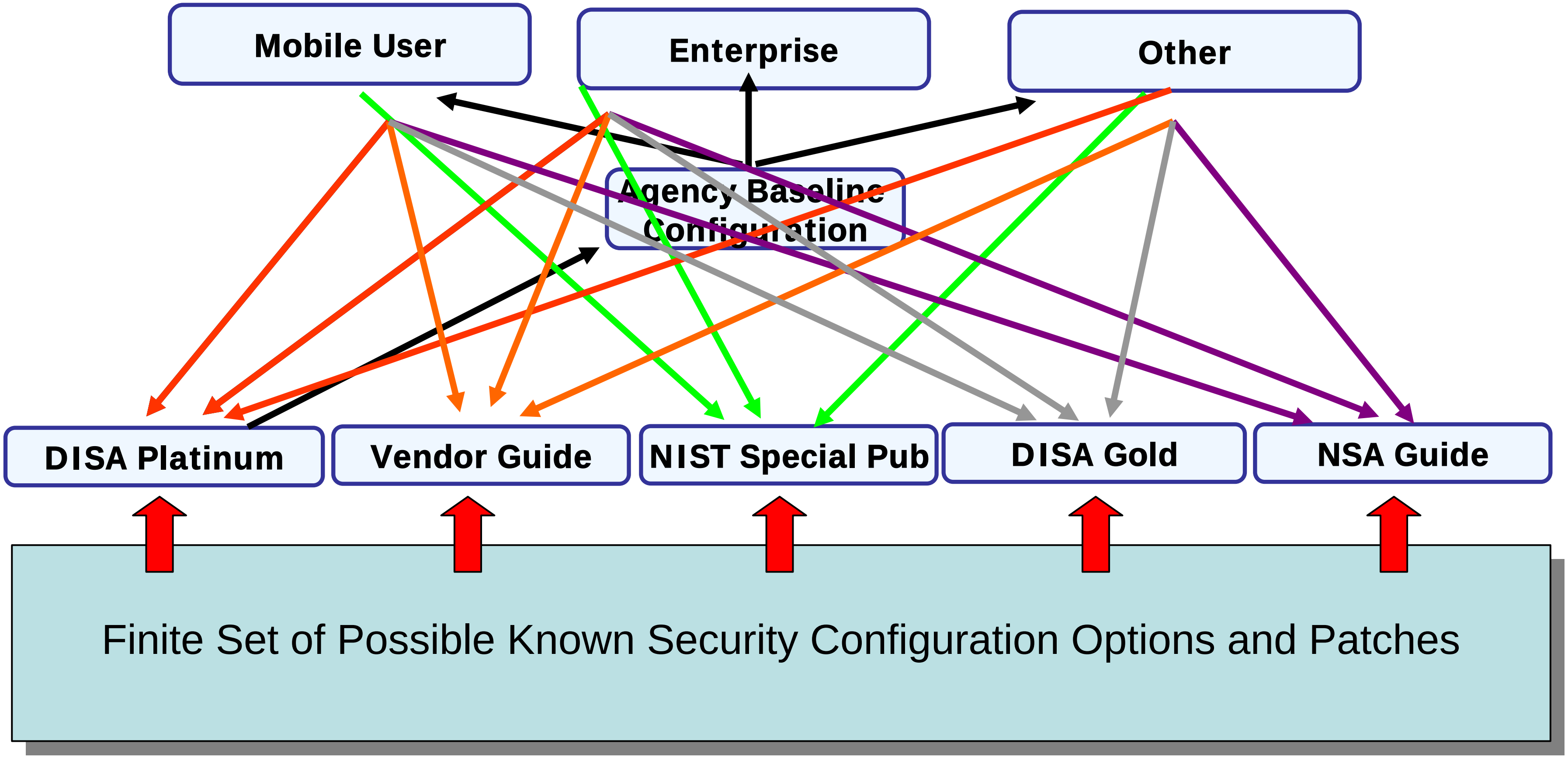
What If IT System Deployed Elsewhere?

New CIO: Why Not Use the Vendor's Guide?

Mobile User
Enterprise
Other
Agency Baseline Configuration
DISA Platinum
Vendor Guide
NIST Special Pub
DISA Gold
NSA Guide
Finite Set of Possible Known Security Configuration Options and Patches

A Closer Look At Operations

What Happens When Changes Occur to the Vendor Guide?



Mobile User

Enterprise

Other

Agency Baseline Configuration

DISA Platinum

Vendor Guide

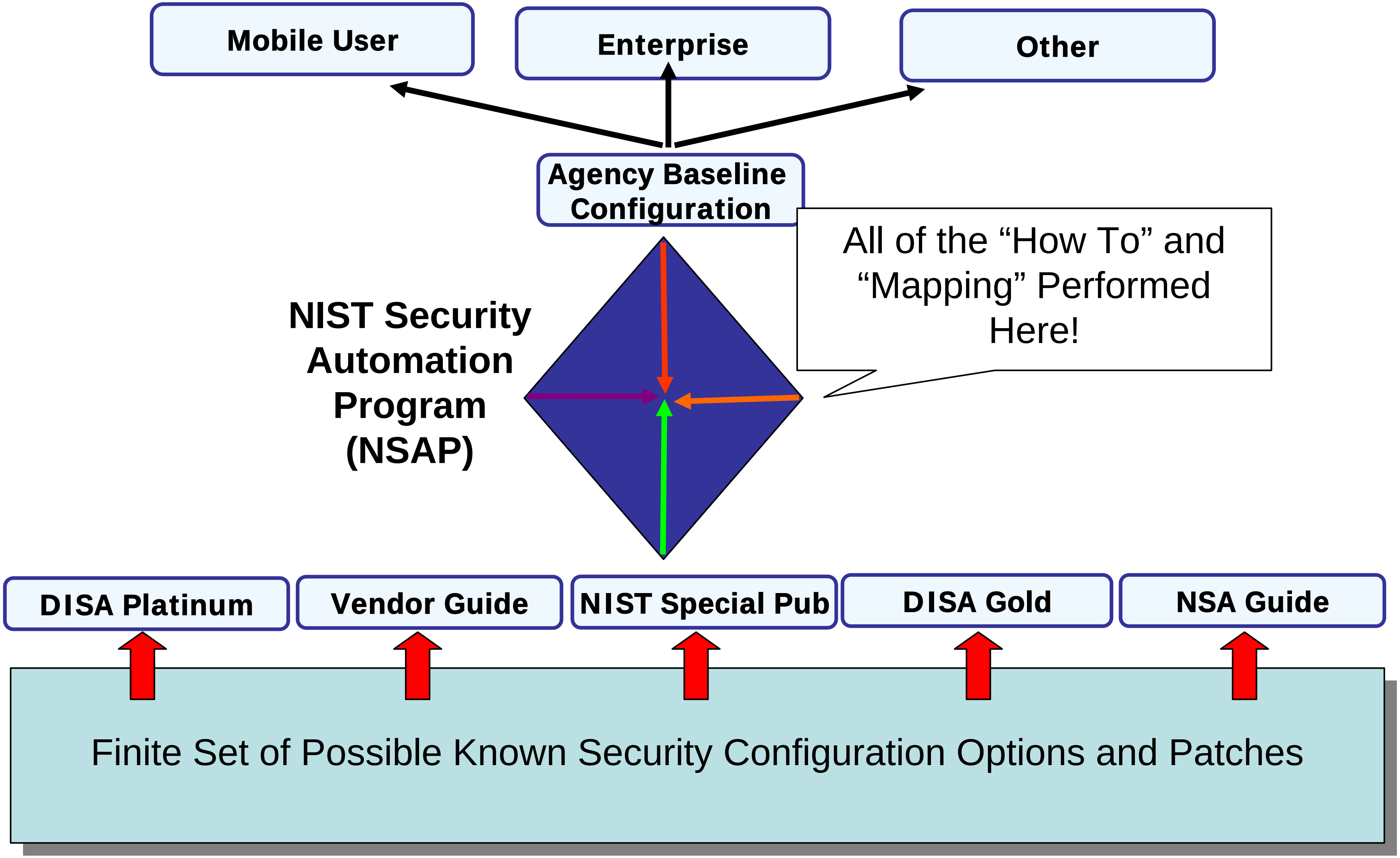
NIST Special Pub

DISA Gold

NSA Guide

Finite Set of Possible Known Security Configuration Options and Patches

How Security Automation Helps



Mobile User

Enterprise

Other

Agency Baseline Configuration

NIST Security Automation Program (NSAP)

All of the “How To” and “Mapping” Performed Here!

DISA Platinum

Vendor Guide

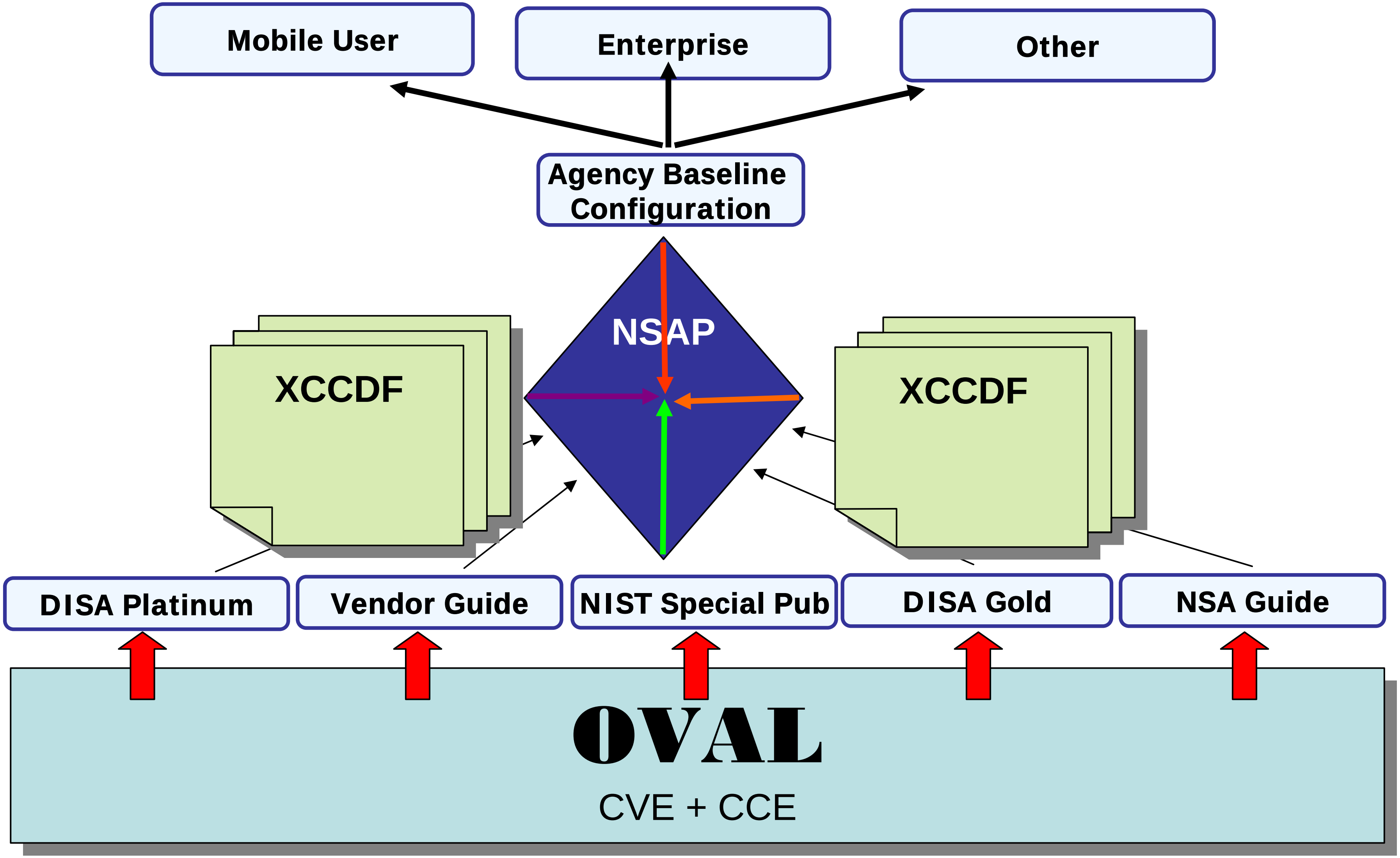
NIST Special Pub

DISA Gold

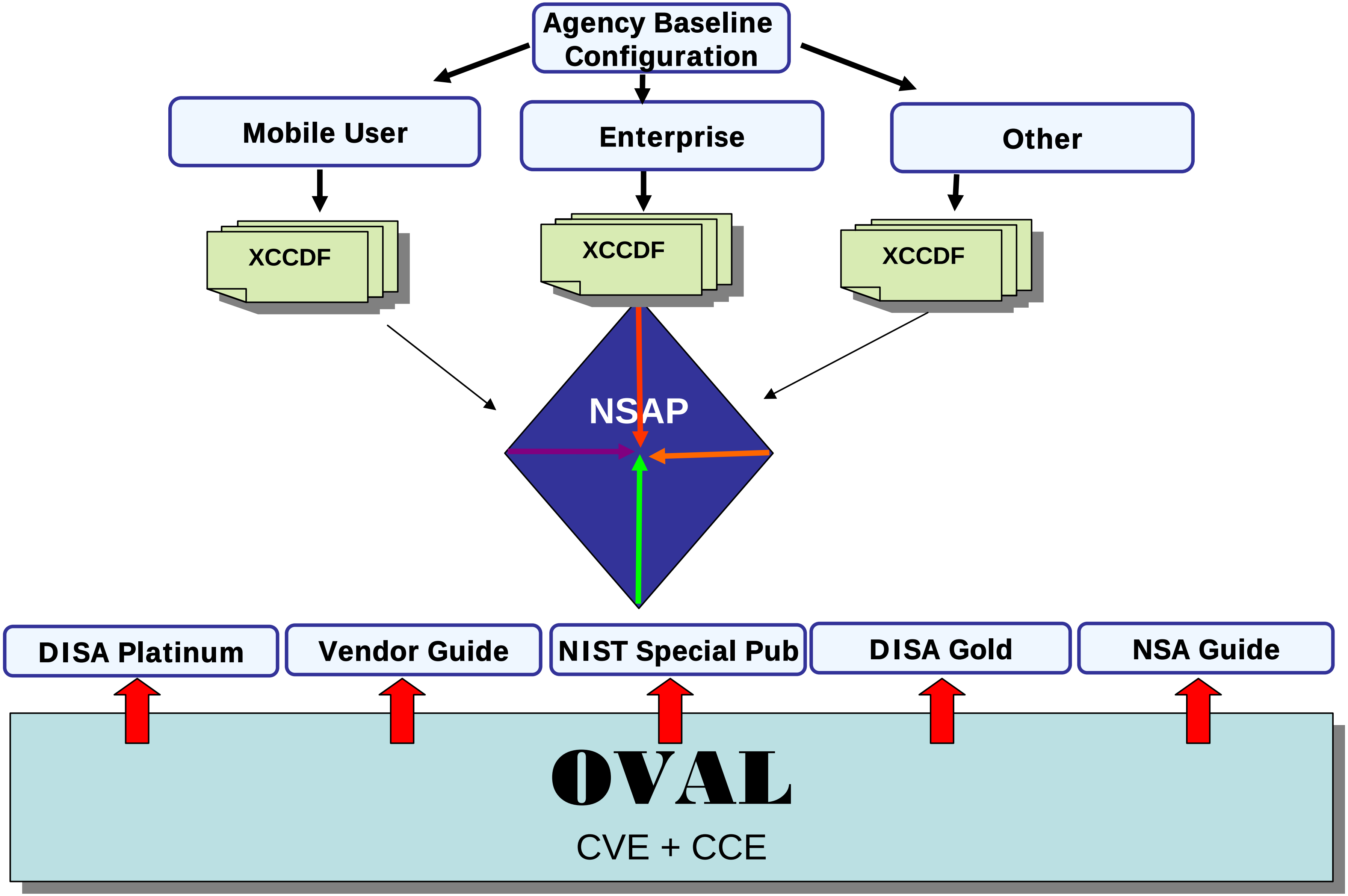
NSA Guide

Finite Set of Possible Known Security Configuration Options and Patches

How Does This Work?



Legacy Baselines?



Agency Baseline Configuration

Mobile User

Enterprise

Other

XCCDF

XCCDF

XCCDF

NSAP

DISA Platinum

Vendor Guide

NIST Special Pub

DISA Gold

NSA Guide

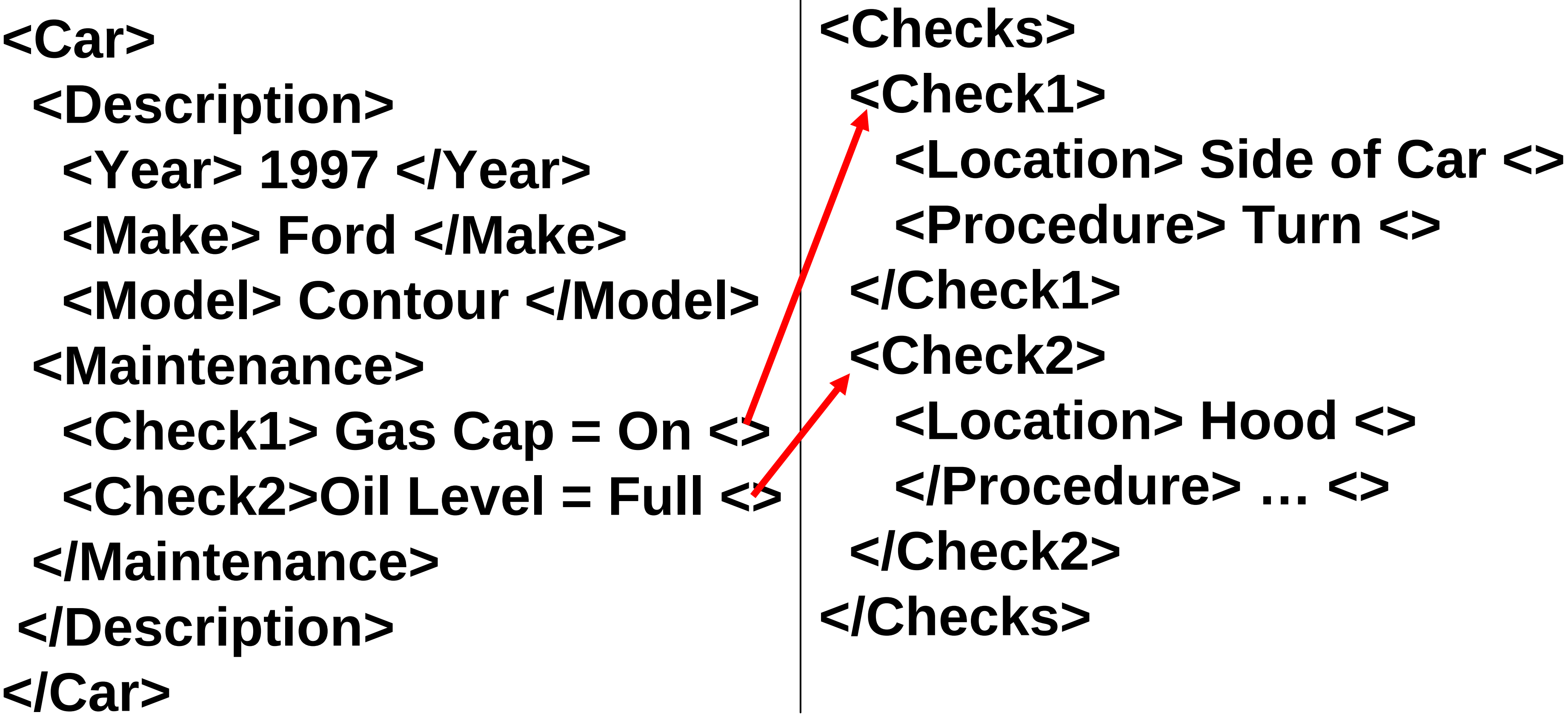
OVAL

CVE + CCE

XML Made Simple

XCCDF - eXtensible Car Care Description Format

OVAL – Open Vehicle Assessment Language



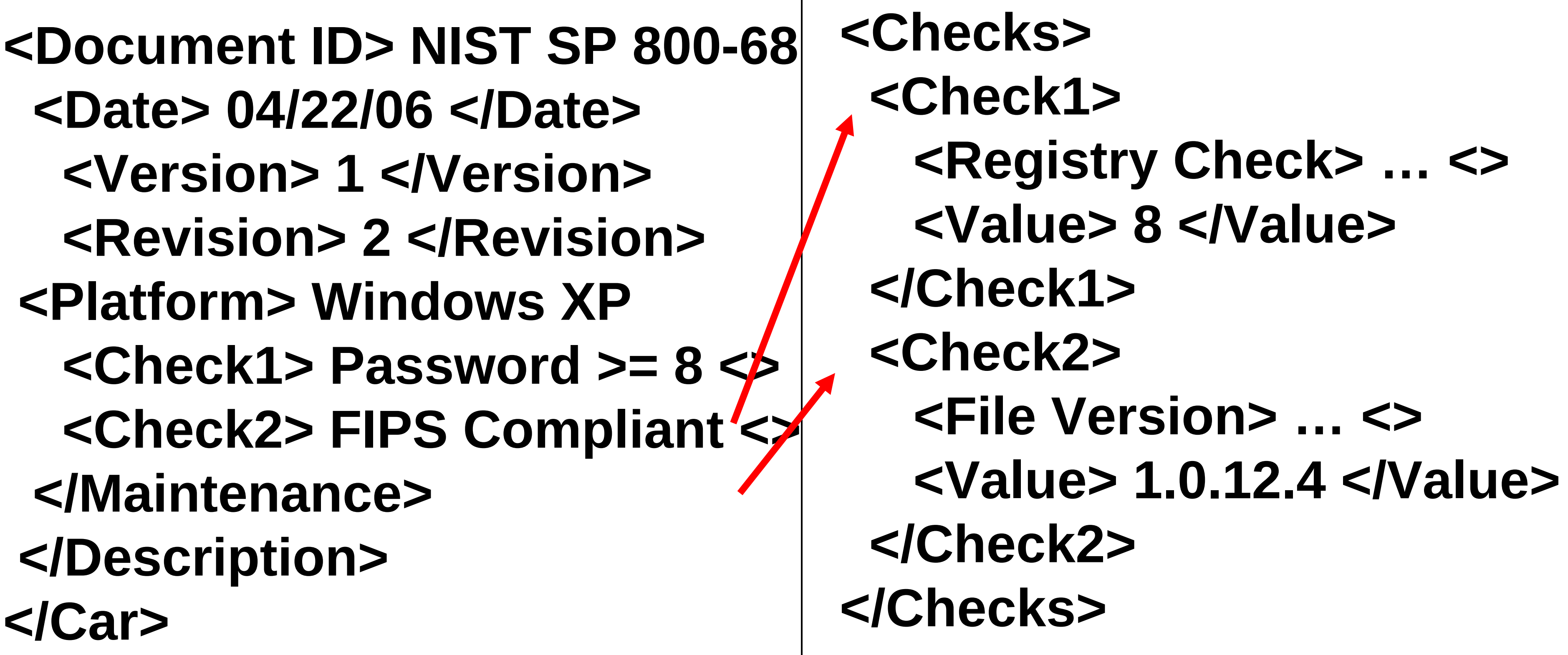
```
<Car>
  <Description>
    <Year> 1997 </Year>
    <Make> Ford </Make>
    <Model> Contour </Model>
  <Maintenance>
    <Check1> Gas Cap = On <>
    <Check2>Oil Level = Full <>
  </Maintenance>
 </Description>
</Car>
```

```
<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

OVAL – Open Vulnerability Assessment Language

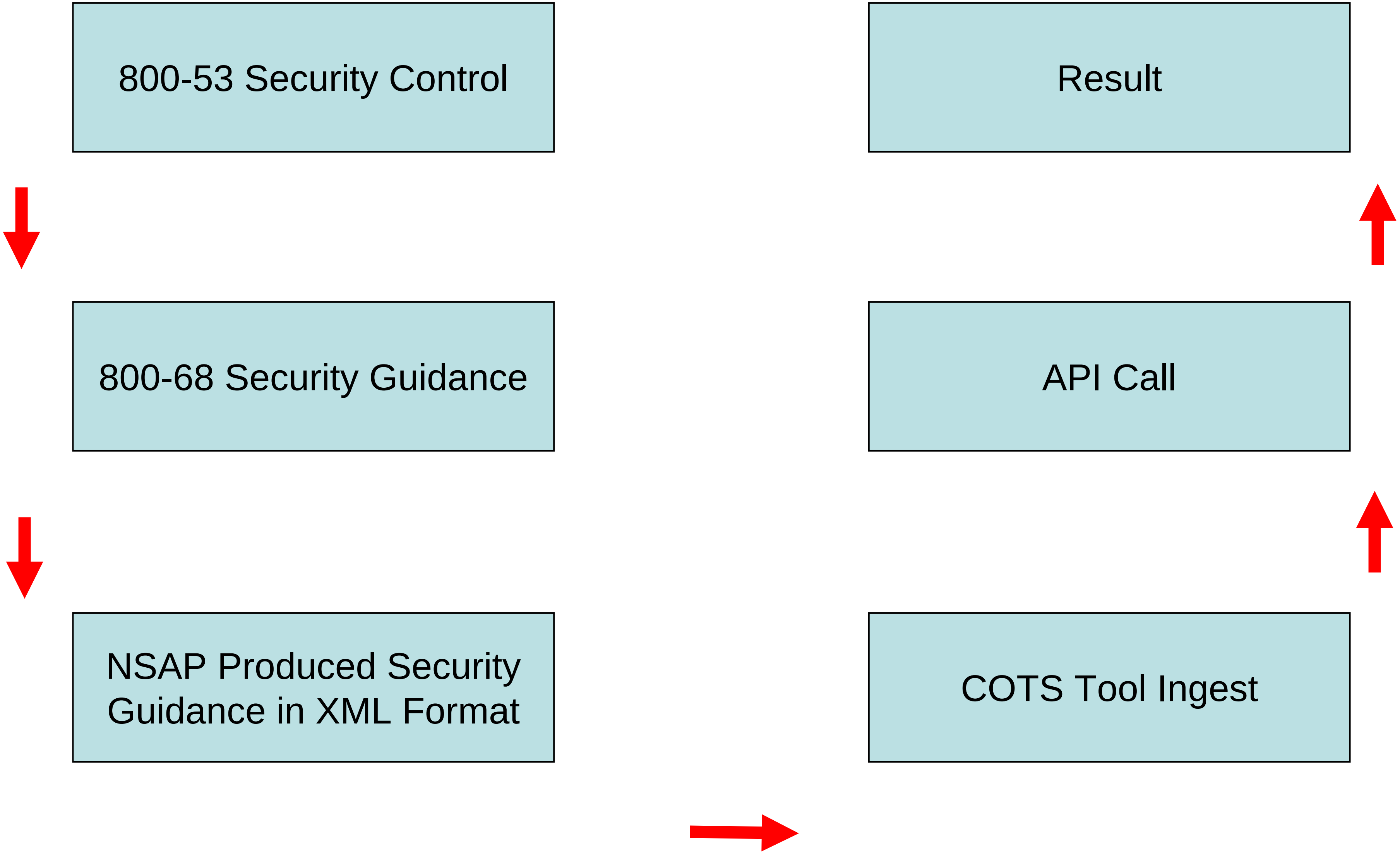


```
<Document ID> NIST SP 800-68
 <Date> 04/22/06 </Date>
  <Version> 1 </Version>
  <Revision> 2 </Revision>
 <Platform> Windows XP
  <Check1> Password >= 8 <>
  <Check2> FIPS Compliant <>
 </Maintenance>
</Description>
</Car>
```

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

Automated Compliance

The Connected Path



800-53 Security Control

800-68 Security Guidance

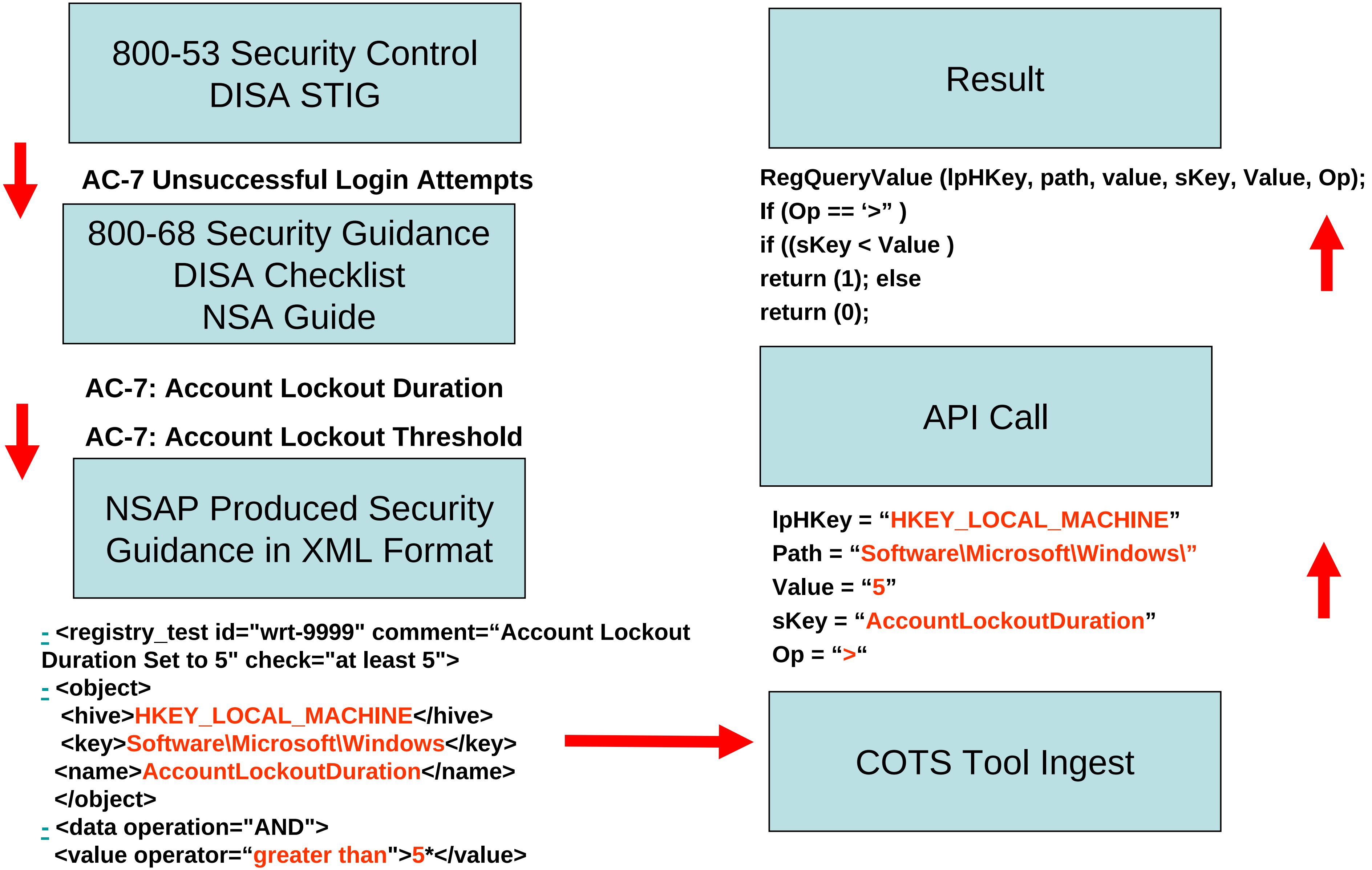
NSAP Produced Security Guidance in XML Format

COTS Tool Ingest

API Call

Result

Automated Compliance



800-53 Security Control
DISA STIG

AC-7 Unsuccessful Login Attempts

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>
```

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

On the Schedule

- Provide popular Windows XP Professional content (in Beta)
  - DISA Gold
  - DISA Platinum
  - NIST 800-68
  - NSA Guides
  - Vendor
  - Others as appropriate.
- Provide Microsoft Windows Vista
  - As per the Microsoft Guide
  - Tailored to Agency policy (if necessary)
- Provide Sun Solaris 10
  - As per the jointly produced Sun Microsystems Security Guide
- Address Backlog beginning with
  - Popular Desktop Applications
  - Windows 2000
  - Windows 2003
  - Windows XP Home

Mappings To Policy & Identifiers

- FISMA Security Controls (All 17 Families and 163 controls for reporting reasons)
- DoD IA Controls
- CCE Identifiers
- CVE Identifiers
- CVSS Scoring System
- DISA VMS Vulnerability IDs
- Gold Disk VIDs
- DISA VMS PDI IDs
- NSA References
- Vendor References
- IAVAs (TBD)
- etc.

NIST Publications

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

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?

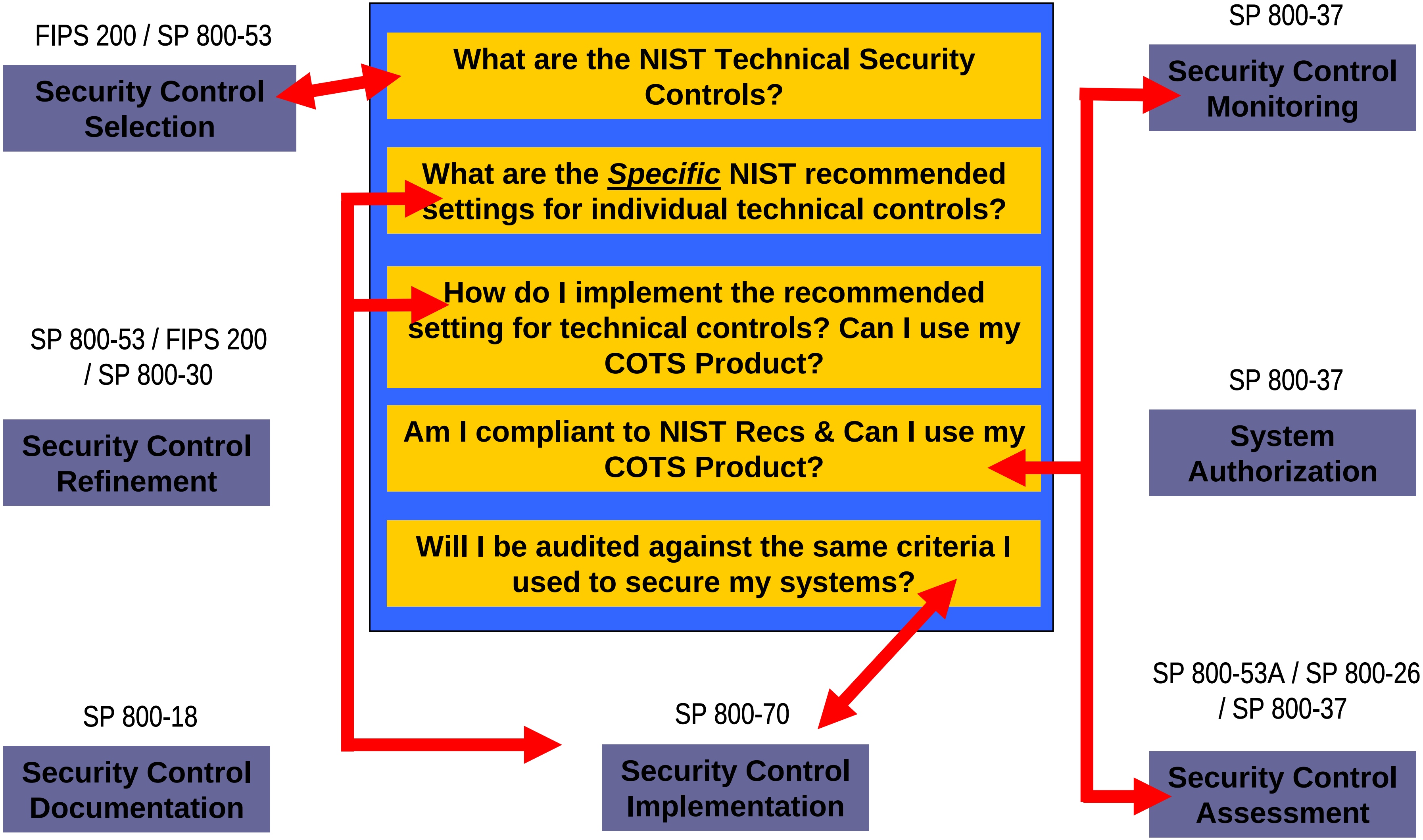
What are the *Specific* NIST recommended settings for individual technical controls?

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



FIPS 200 / SP 800-53

Security Control Selection

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 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

SP 800-37

System Authorization

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

Security Control Assessment

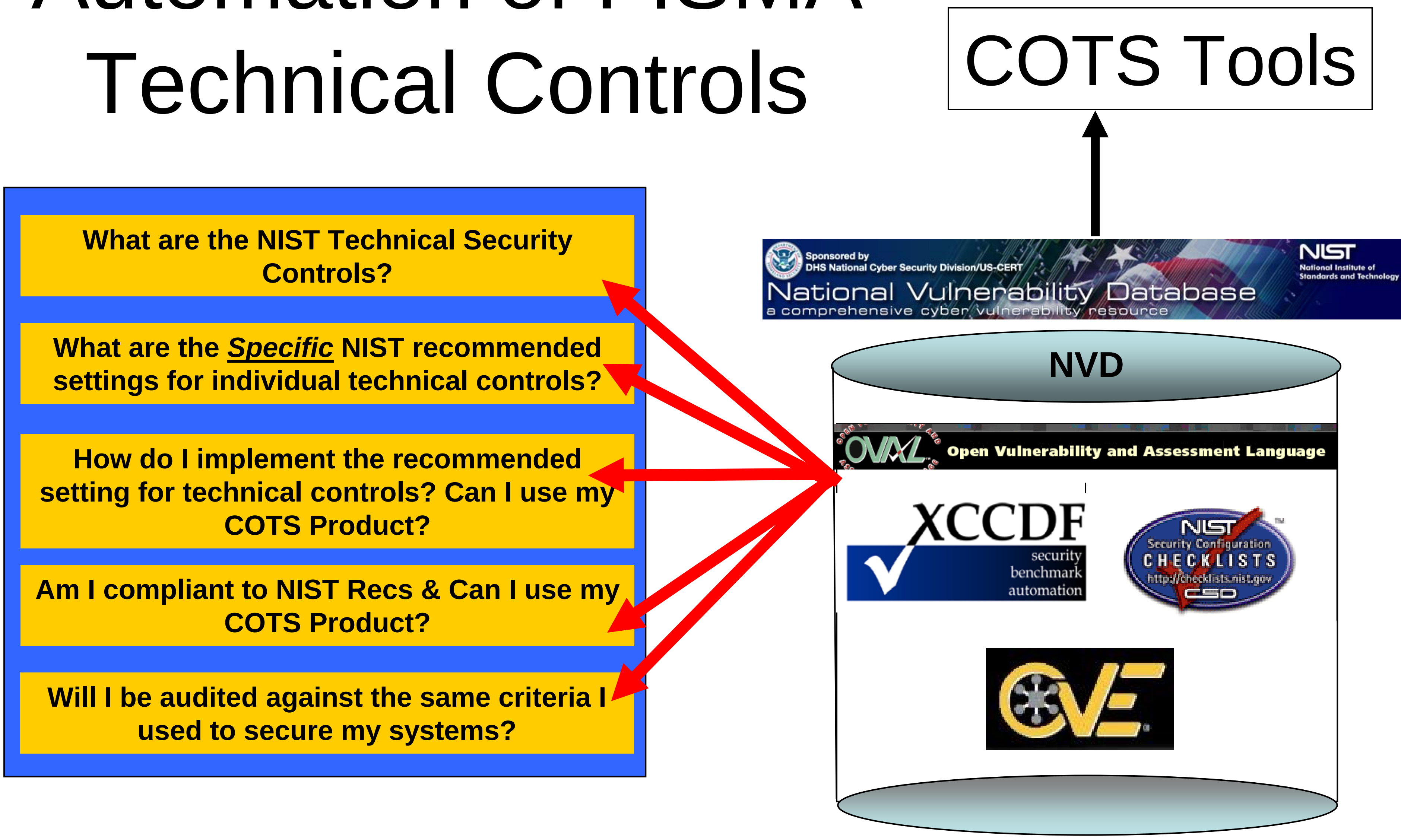
SP 800-18

Security Control Documentation

SP 800-70

Security Control Implementation

Automation of FISMA Technical Controls



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?

COTS Tools
Sponsored by
DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource
NIST
National Institute of Standards and Technology
NVD
OVAL
Open Vulnerability and Assessment Language
XCCDF
security benchmark automation
NIST Security Configuration CHECKLISTS
http://checklists.nist.gov
CSD
CVE

How Many SP800-53 Controls Can Be Automated?

Full Automation:	31 (19%)
Partial Automation:	39 (24%)
No Automation:	93 (57%)
Total Controls	163(100%)

Note: These statistics apply to our proposed methodology.
Other techniques may provide automation in different areas.

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.

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
  - Content Automation Program
- **NSA**
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Security Guidance & Content

Existing NIST Products

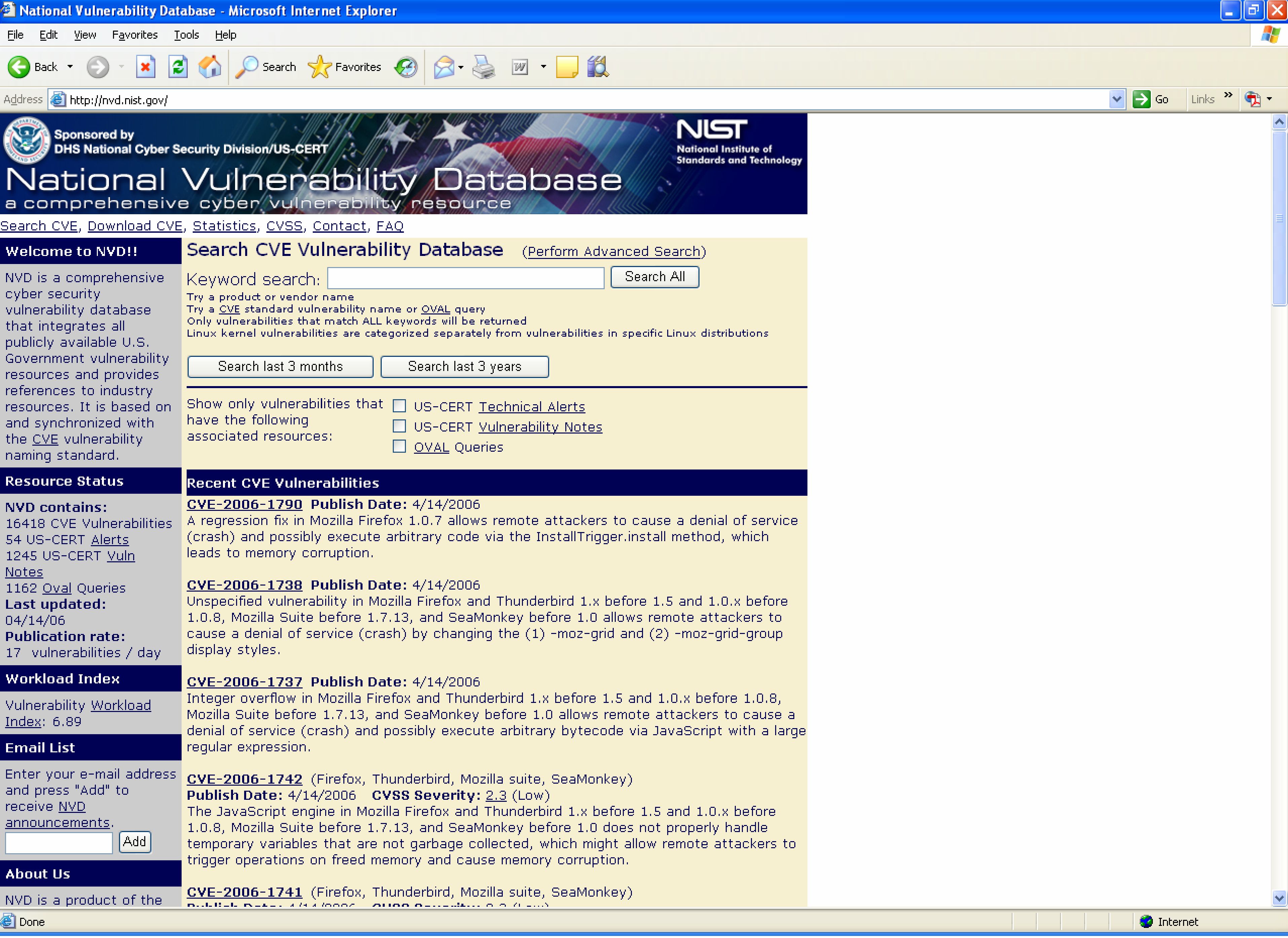
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

- National Vulnerability Database
  - 2.2 million hits per month
  - 20 new vulnerabilities per day
  - Integrated standards: CVE (244 products) CVSS (20 vendors) OVAL – Open Vulnerability and Assessment Language (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


National Vulnerability Database - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://nvd.nist.gov/
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 All
Search last 3 months
Search last 3 years
Add
Done
Internet

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.

About Us

NVD is a product of the

Search CVE Vulnerability Database (Perform Advanced Search)

Keyword search:

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

Show only vulnerabilities that have the following associated resources:

□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries

Recent CVE Vulnerabilities

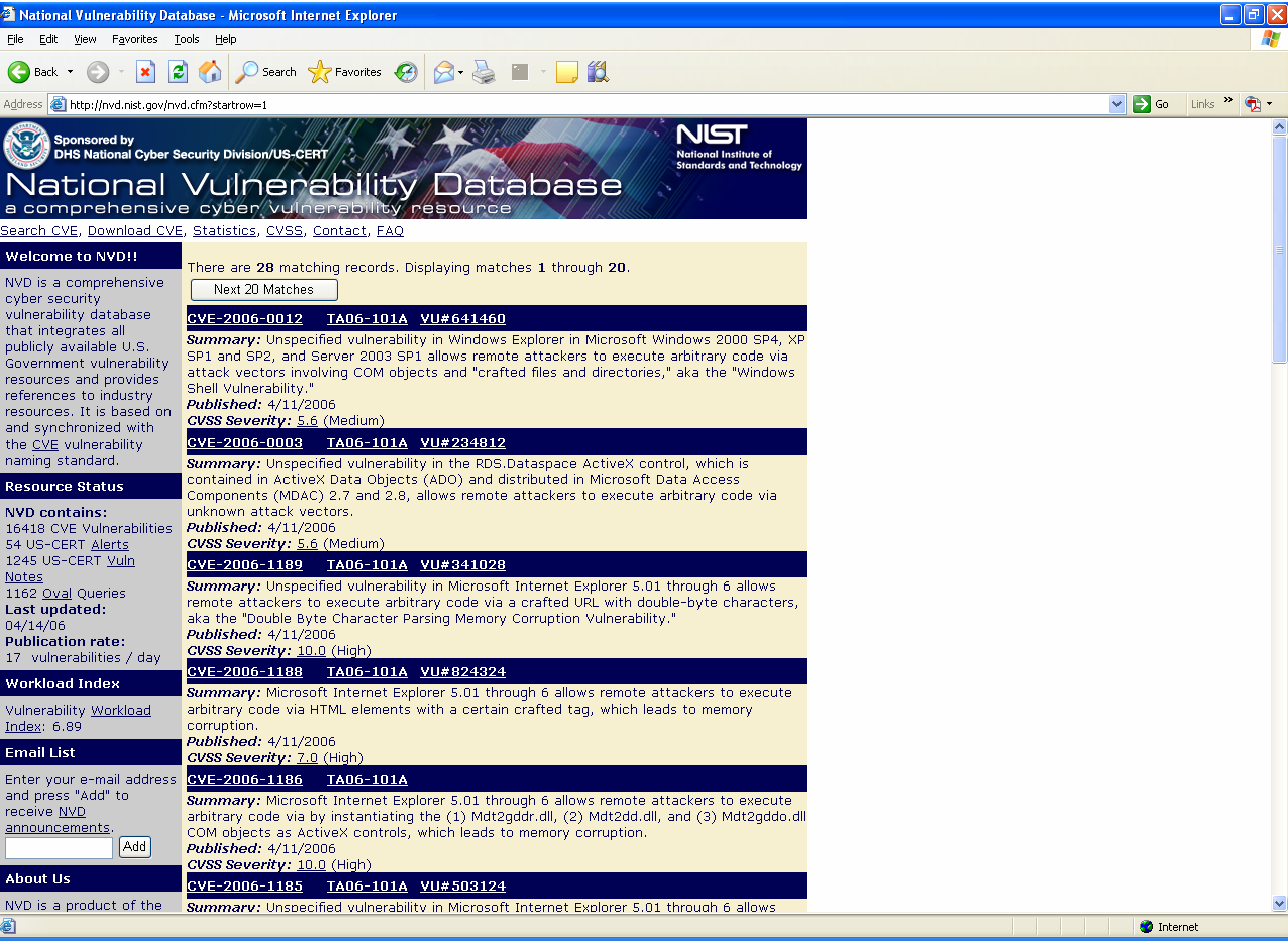
CVE-2006-1790 Publish Date: 4/14/2006
A regression fix in Mozilla Firefox 1.0.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the InstallTrigger.install method, which leads to memory corruption.

CVE-2006-1738 Publish Date: 4/14/2006
Unspecified vulnerability in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 allows remote attackers to cause a denial of service (crash) by changing the (1) -moz-grid and (2) -moz-grid-group display styles.

CVE-2006-1737 Publish Date: 4/14/2006
Integer overflow in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary bytecode via JavaScript with a large regular expression.

CVE-2006-1742 (Firefox, Thunderbird, Mozilla suite, SeaMonkey)
Publish Date: 4/14/2006 **CVSS Severity:** 2.3 (Low)
The JavaScript engine in Mozilla Firefox and Thunderbird 1.x before 1.5 and 1.0.x before 1.0.8, Mozilla Suite before 1.7.13, and SeaMonkey before 1.0 does not properly handle temporary variables that are not garbage collected, which might allow remote attackers to trigger operations on freed memory and cause memory corruption.

CVE-2006-1741 (Firefox, Thunderbird, Mozilla suite, SeaMonkey)
Publish Date: 4/14/2006 **CVSS Severity:** 2.3 (Low)


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
Internet

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

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

XCCDF
security
benchmark
automation

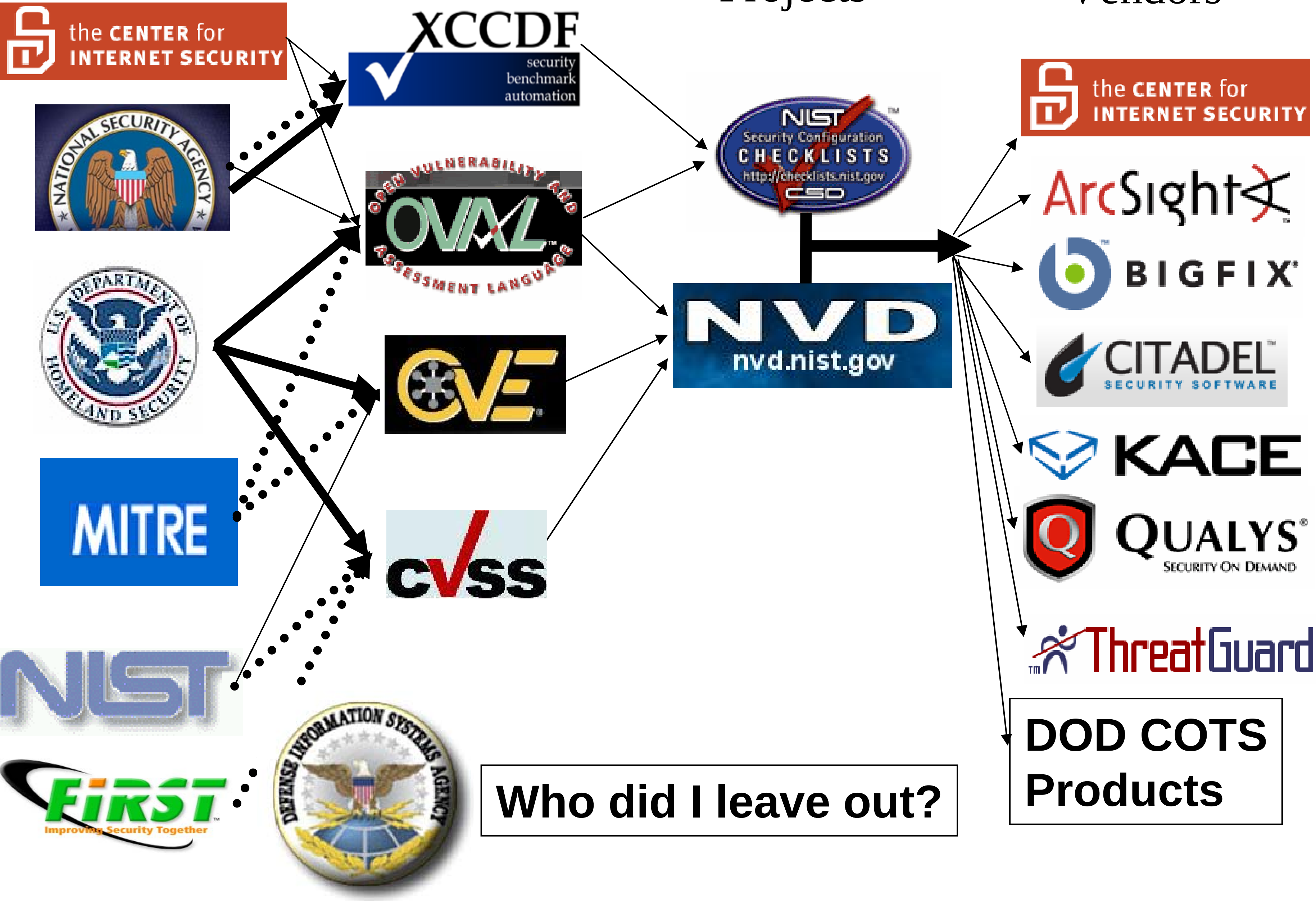
- Designed to support:
  - Information Interchange
  - Document Generation
  - Organizational and Situational Tailoring
  - Automated Compliance Testing
  - Compliance Scoring
- Published as NIST IR 7275
- Foster more widespread application of good security practices

Involved Organizations

Standards

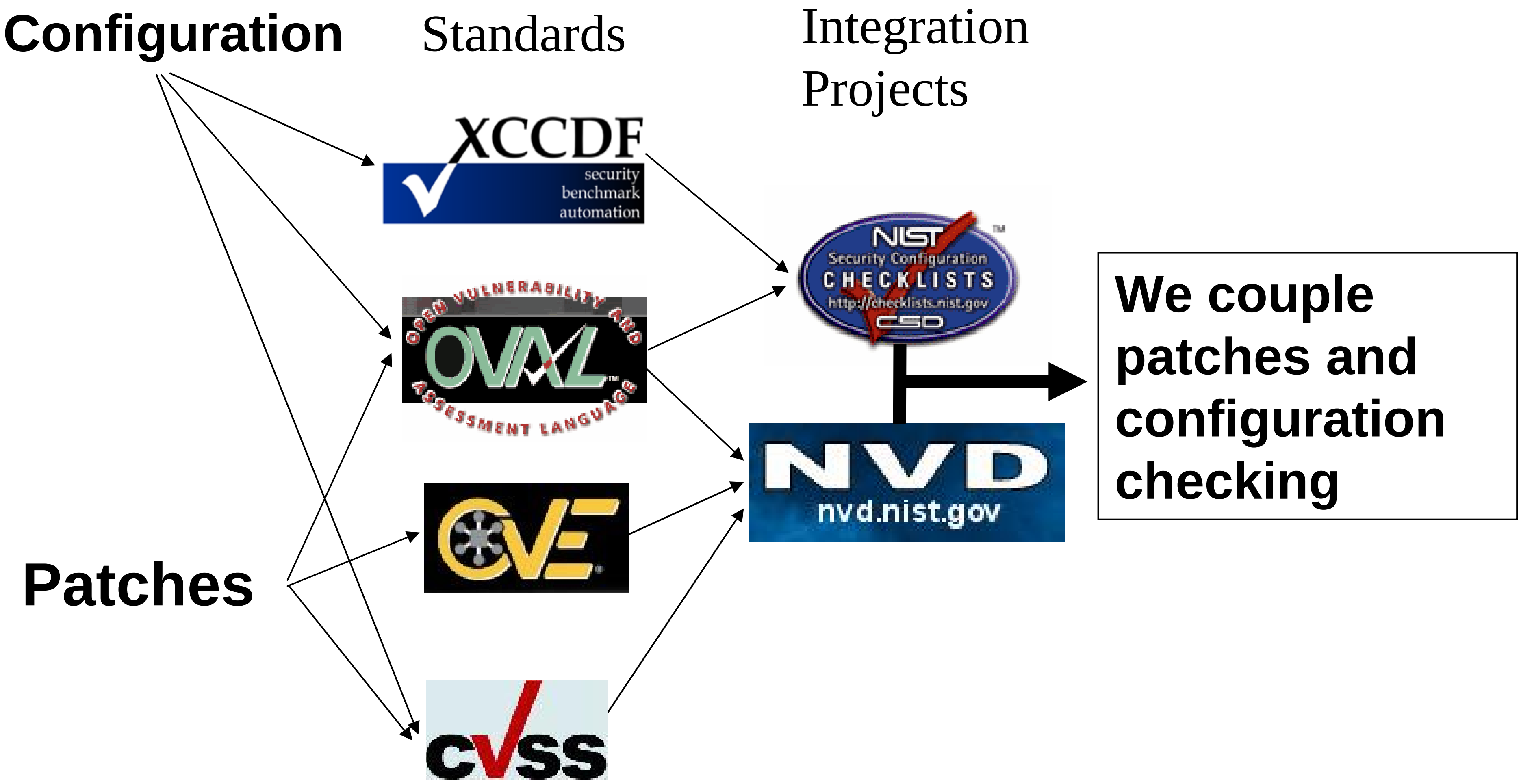
Integration Projects

IT Security Vendors


the CENTER for INTERNET SECURITY
NATIONAL SECURITY AGENCY
U.S. DEPARTMENT OF HOMELAND SECURITY
MITRE
NIST
FIRST
Improving Security Together
DEFENSE INFORMATION SYSTEMS AGENCY
XCCDF
security benchmark automation
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
OVAL
CVE
CVSS
NIST Security Configuration CHECKLISTS
http://checklists.nist.gov
CSD
NVD
nvd.nist.gov
the CENTER for INTERNET SECURITY
ArcSight
BIGFIX
CITADEL
SECURITY SOFTWARE
KACE
QUALYS
SECURITY ON DEMAND
ThreatGuard

DOD COTS Products

Who did I leave out?



Configuration

Standards

Integration Projects

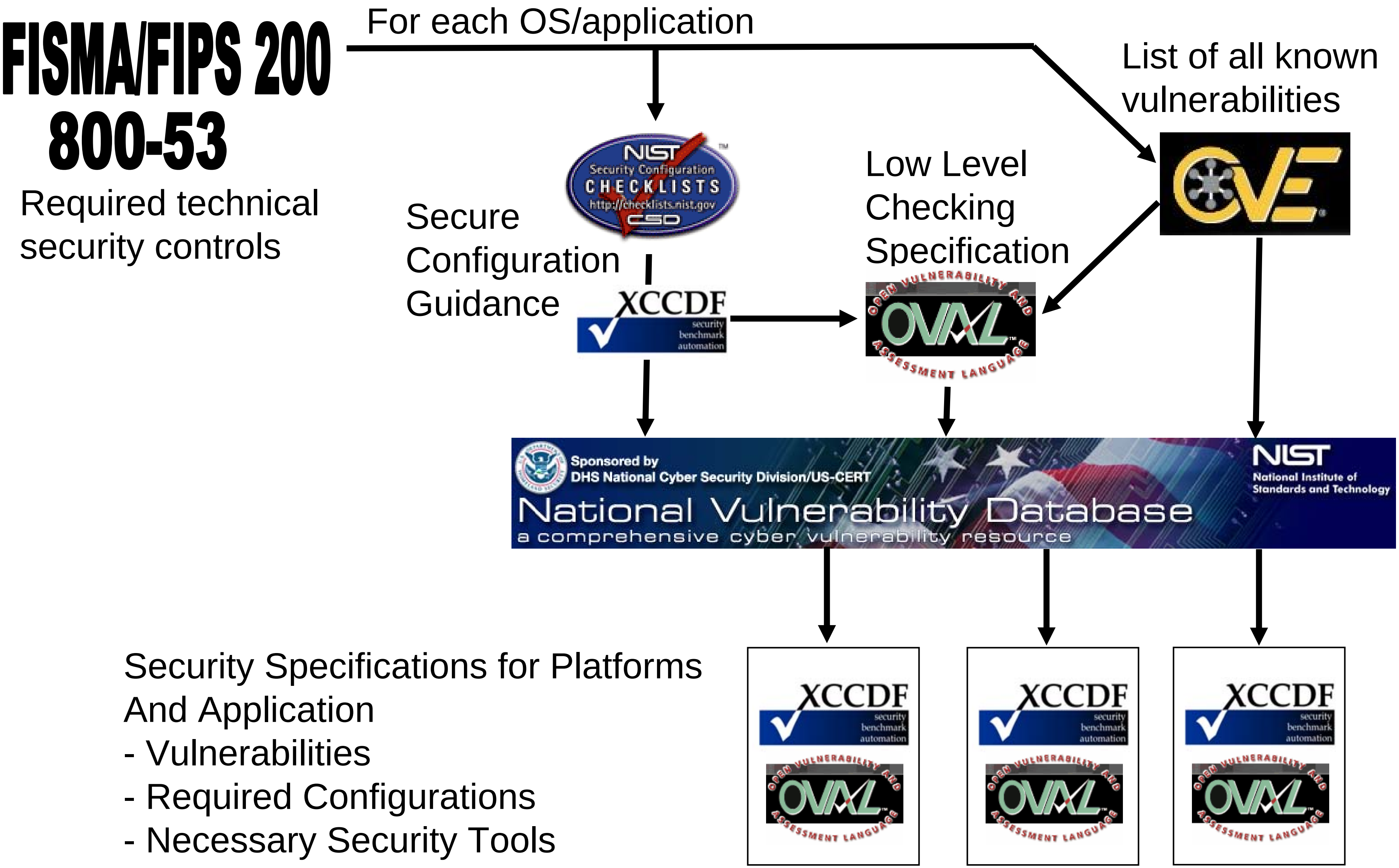
Patches

We couple patches and configuration checking

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

Secure Configuration Guidance

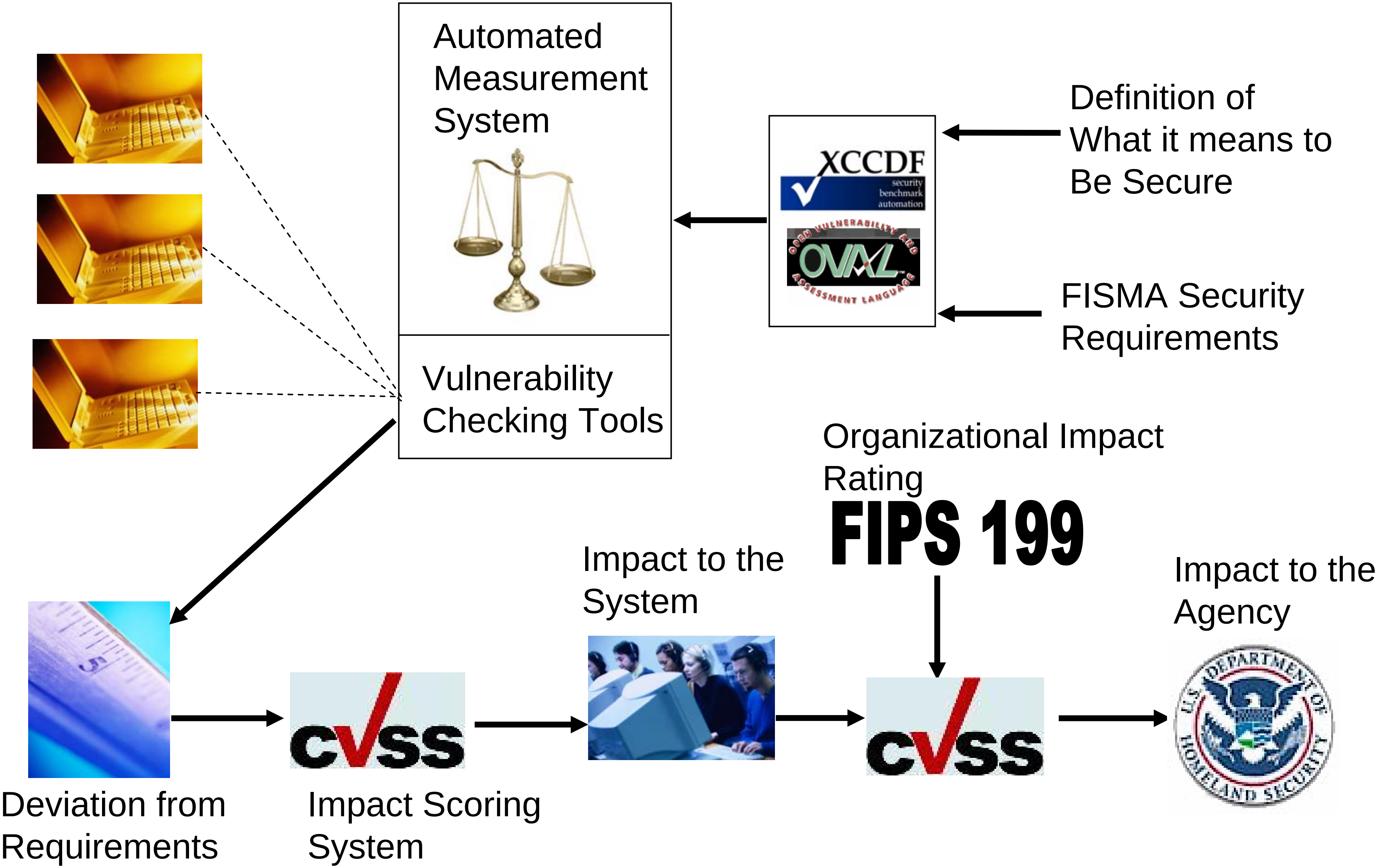
Low Level Checking Specification

List of all known vulnerabilities

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD
XCCDF security benchmark automation
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE OVAL
CVE
Sponsored by DHS National Cyber Security Division/US-CERT
National Vulnerability Database
a comprehensive cyber vulnerability resource
NIST National Institute of Standards and Technology
XCCDF security benchmark automation
OVAL
XCCDF security benchmark automation
OVAL
XCCDF security benchmark automation
OVAL

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

Automated Security Measurement System



Automated Measurement System

Vulnerability Checking Tools

Definition of What it means to Be Secure

FISMA Security Requirements

Organizational Impact Rating

FIPS 199

Impact to the System

Impact to the Agency

Deviation from Requirements

Impact Scoring System

XCCDF
security benchmark automation
OPEN VULNERABILITY AND ASSESSMENT LANGUAGE
OVAL
CVSS
CVSS
U.S. DEPARTMENT OF HOMELAND SECURITY

Today’s Status

- NIST Windows XP Configuration Guide (SP 800-68)
- http://csrc.nist.gov/itsec/download_WinXP.html
- Policy statements represented in XCCDF
- Configuration checks represented in OVAL
- Currently Beta-2 version
- Covers: registry settings, file permission checks, password policies, account lockout policies, audit policies
- Download at: http://checklists.nist.gov/NIST-800-68-WinXPPro-XML-Alpha-rev1.zip
- Content will be updated periodically; however, format will remain constant at least until the NIST Workshop in September 2006.

NIST 800-68 in Context of 800-53

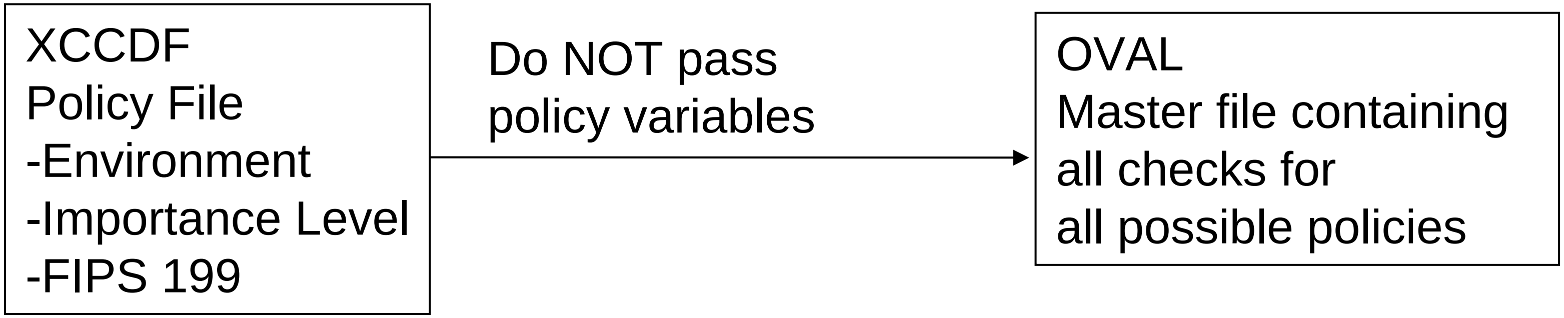
- 800-53, Appendix D specifies security control applicability according to High, Moderate, and Low impact rating of an IT System.
- 800-68 provides specific configuration information according to environment (Standalone, Enterprise, SSLF, and Legacy)
- The NIST XML specifies the applicable 800-68 security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

OVAL and XCCDF Implementation

Implementation with XCCDF (stand alone OVAL)

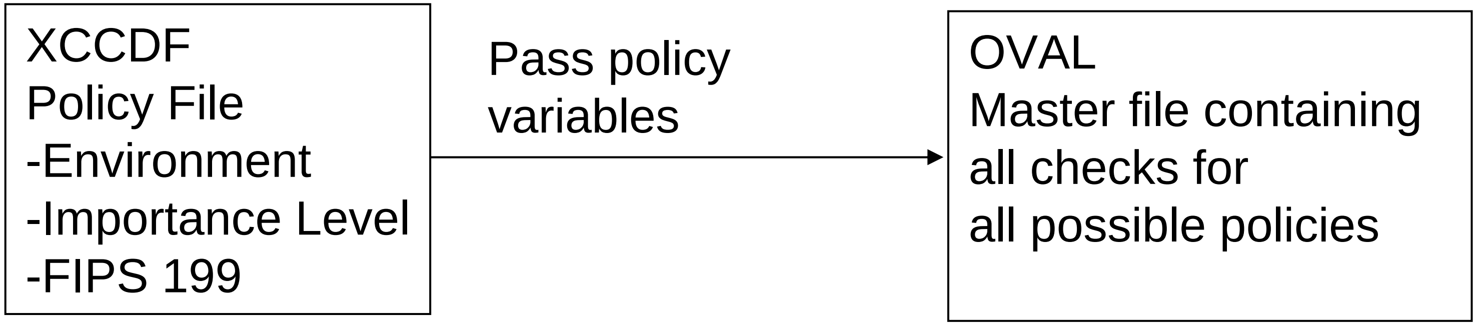


XCCDF
Policy File
-Environment
-Importance Level
-FIPS 199

Do NOT pass
policy variables

OVAL
Master file containing
all checks for
all possible policies

Implementation with XCCDF (dependant OVAL)



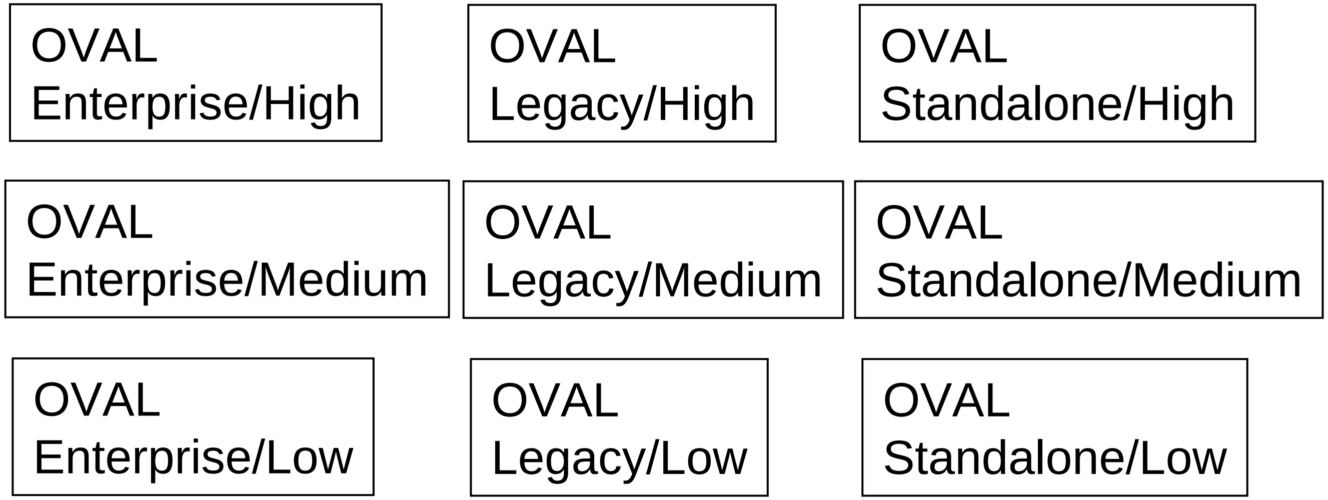
XCCDF
Policy File
-Environment
-Importance Level
-FIPS 199

Pass policy
variables

OVAL
Master file containing
all checks for
all possible policies

OVAL and XCCDF Implementation

Implementation without XCCDF



OVAL Enterprise/High

OVAL Legacy/High

OVAL Standalone/High

OVAL Enterprise/Medium

OVAL Legacy/Medium

OVAL Standalone/Medium

OVAL Enterprise/Low

OVAL Legacy/Low

OVAL Standalone/Low

OVAL files work by themselves

Each OVAL file checks with respect to a particular policy

Questions?

Stephen Quinn (NIST Checklist Program)
Peter Mell (National Vulnerability Database)
Computer Security Division
NIST, Information Technology Laboratory
stquinn@nist.gov, mell@nist.gov