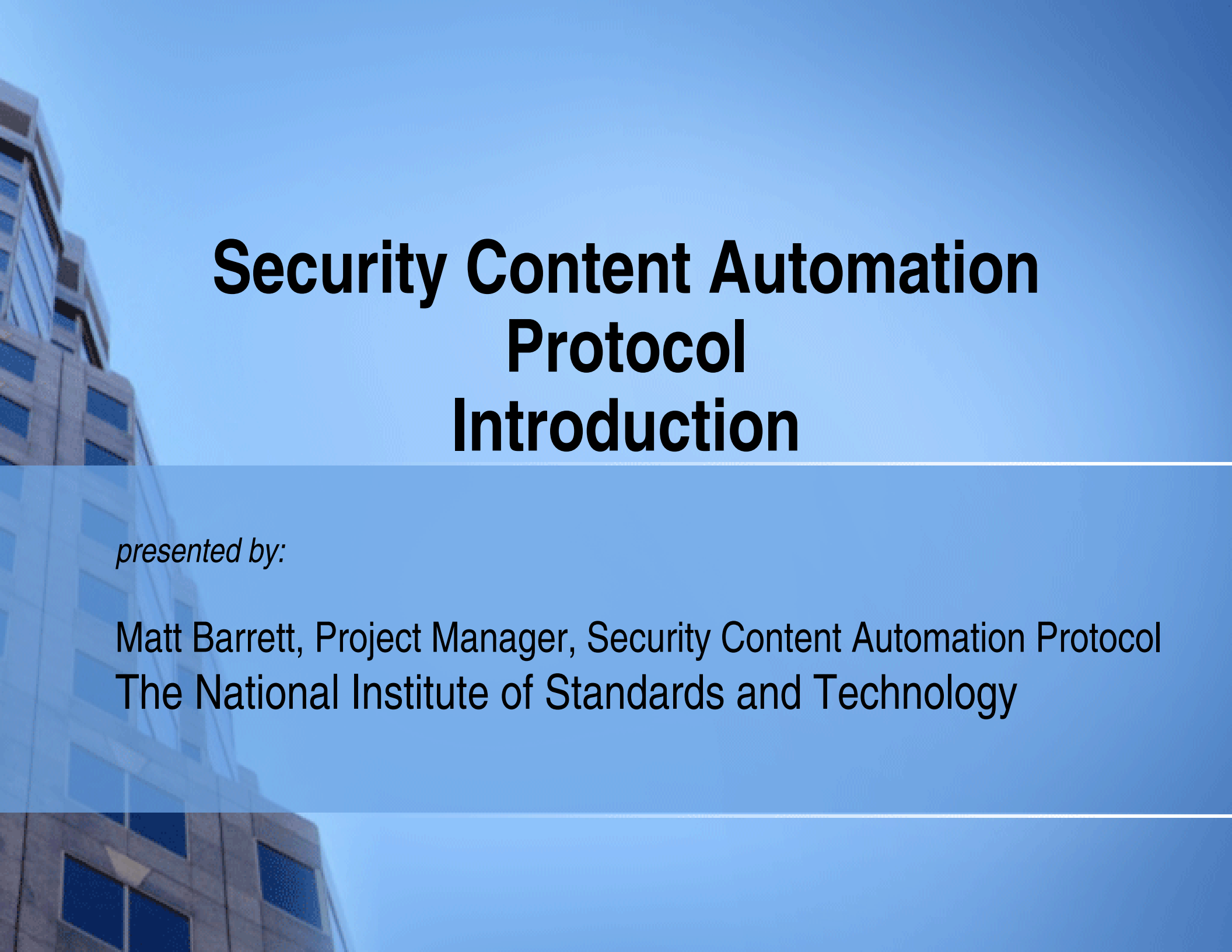


Security Content Automation Protocol Introduction

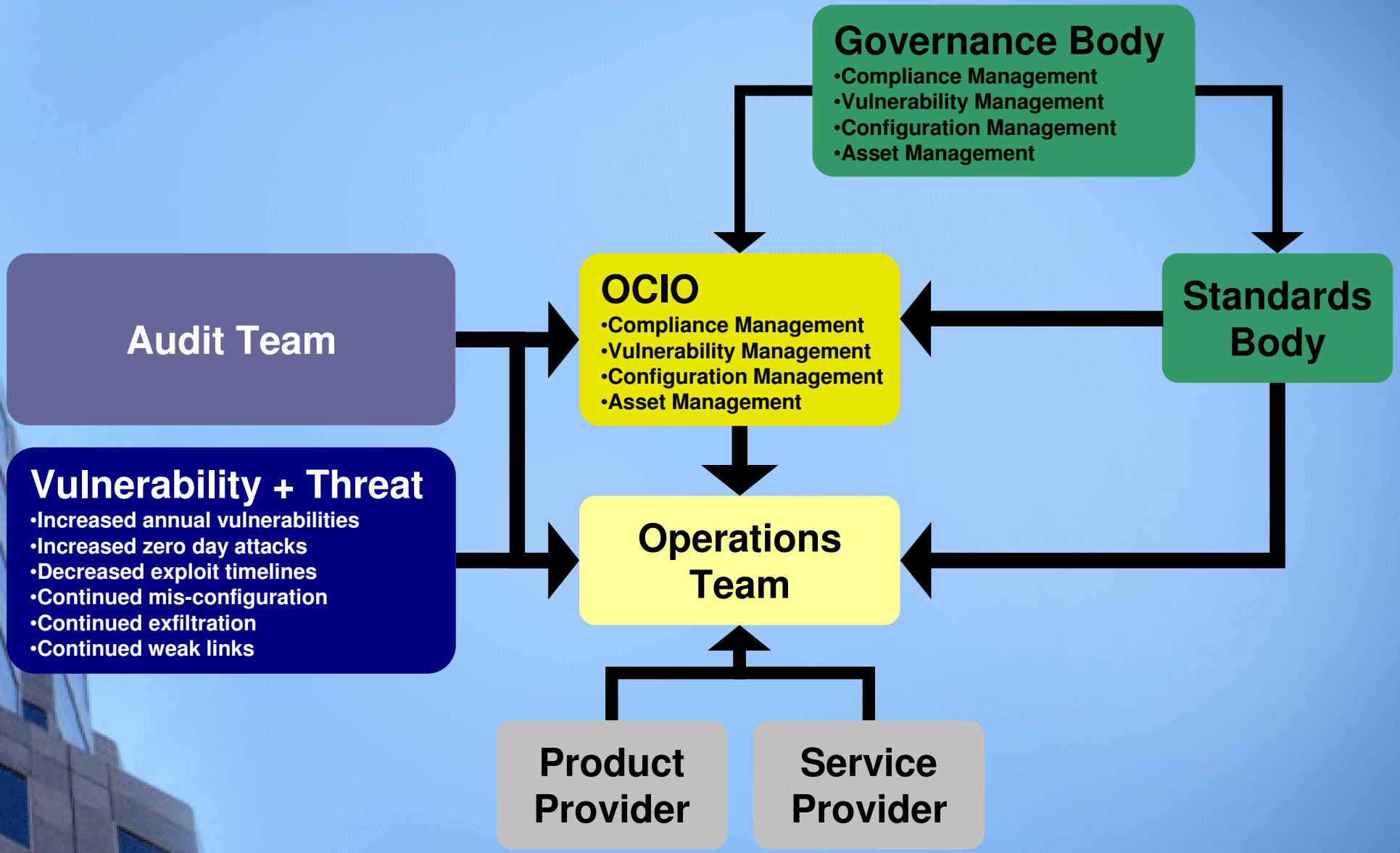
presented by:

Matt Barrett, Project Manager, Security Content Automation Protocol
The National Institute of Standards and Technology

Thoughts on Current State

- ***Automation and communication is normally limited to a single discipline*** - vulnerability, compliance, configuration, and asset management remain compartmentalized
- ***Automation and communication usually occurs through proprietary methods*** - therefore data sharing, analysis, aggregation, etc. is typically only possible within a product line
- ***Increasing number of mandates*** - means increasing number of frameworks, standards, regulations, guidelines, sometimes these documents conflict
- ***Slowly increasing number of security configurations*** - arguably the increase is not nearly as significant as increasing documents
- ***Increasing number and complexity of vulnerabilities and threats***

Current State Security Operations

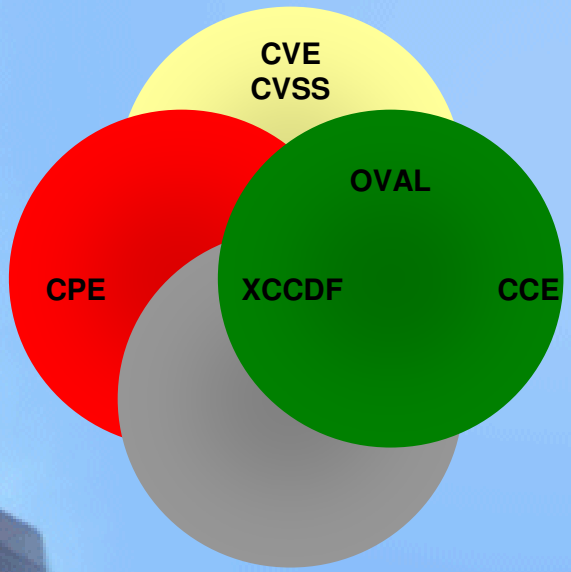


What is SCAP?

How

Standardizing the format by which we communicate

Protocol



What

Standardizing the information we communicate

Content

http://nvd.nist.gov

http://checklists.nist.gov

- 70 million hits per year
- 20 new vulnerabilities per day, over 6,000 per year
- Mis-configuration cross references
- Reconciles software flaws from US CERT and MITRE repositories
- Spanish translation
- 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

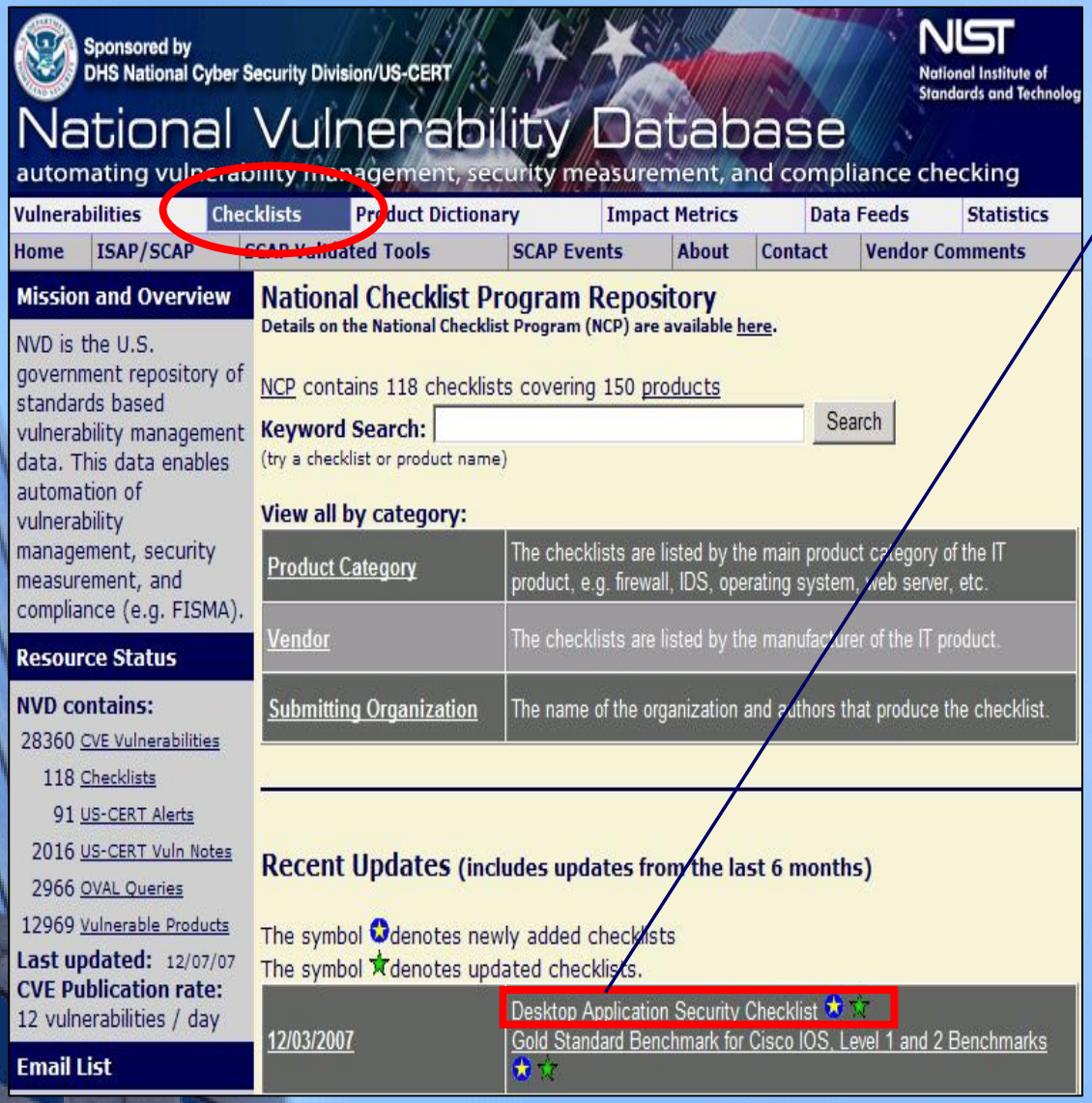
Standardizing What We Communicate

- 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 114 separate guidance documents for over 141 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 70 million hits per year
- 29,000 vulnerabilities
- 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

NIST

National Checklist Program Hosted at National Vulnerability Database Website



National Checklist Program

Checklist Summary #10: Desktop Application Security Checklist

Checklist Item Name	Desktop Application Security Checklist
Checklist Item Version Number	Version 2, Release 1.8
Status	Final
Creation Date	10/25/2007
Original Publication Date	2003-02-28
Revision Date	12/03/2007
Product Category	Web Browser
Vendor (s)	Microsoft Netscape
Product (s)	Microsoft ie Microsoft ie Netscape Communicator Netscape Communicator Netscape Communicator Netscape Netscape Netscape Communicator Netscape Communicator
Product Version (s)	Microsoft ie 5.5 Microsoft ie 6.0 Netscape Communicator 4.76 Netscape Communicator 4.77 Netscape Communicator 4.78 Netscape Netscape 6.2.3 Netscape Communicator 4.79 Netscape Communicator 4.8
CPE Name (s)	cpe:/a:Microsoft:ie:5.5 cpe:/a:Microsoft:ie:6.0

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 coming soon*
Software Flaw CVE
General Impact CVSS

Test Procedures **OVAL**

Patches **OVAL**

Commercial Government Tools

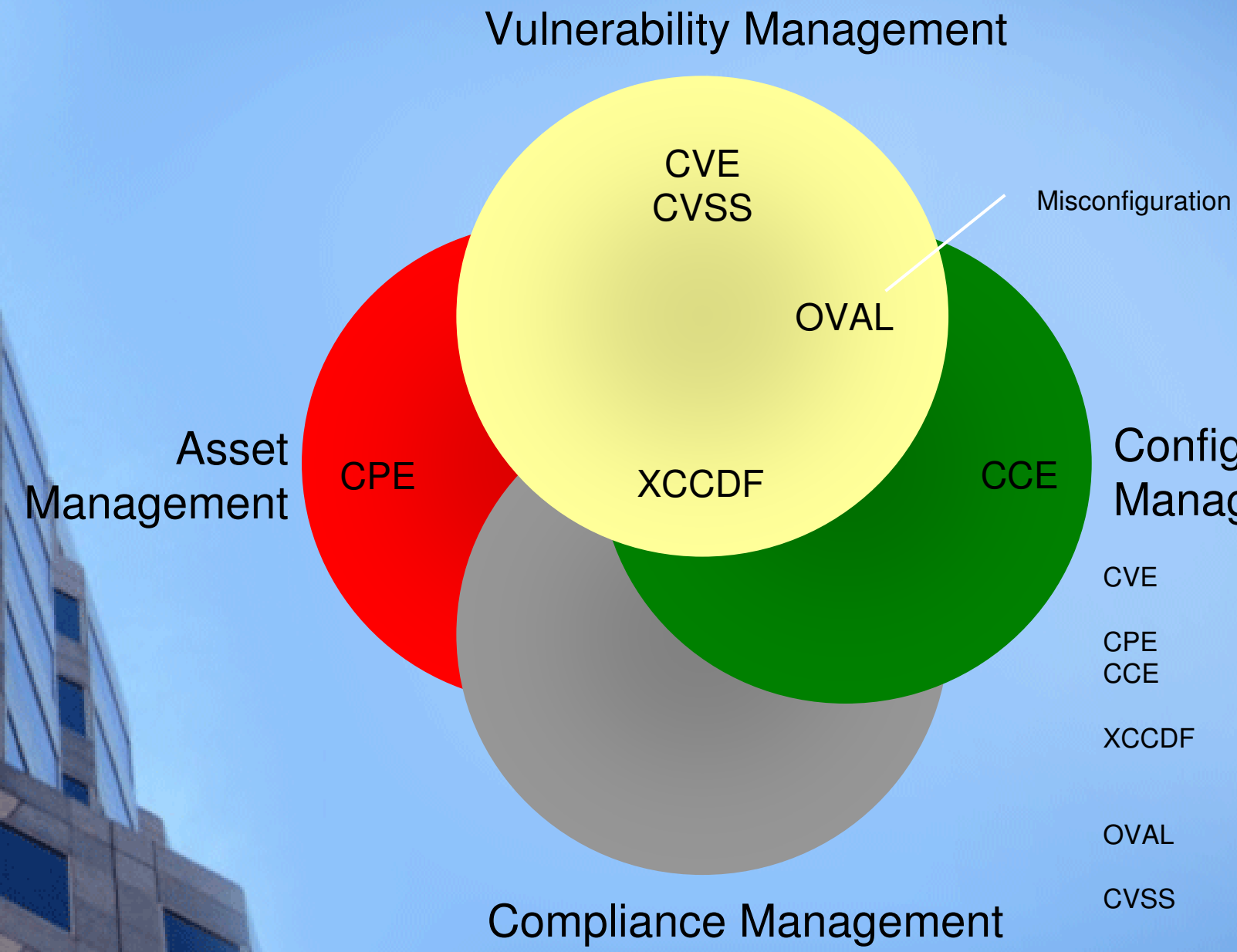
Specific Impact Results coming soon*

Specific Impact Results CVSS

**** NIST IR-7502: DRAFT The Common Configuration Scoring System (CCSS)***
http://csrc.nist.gov/publications/PubsDrafts.html

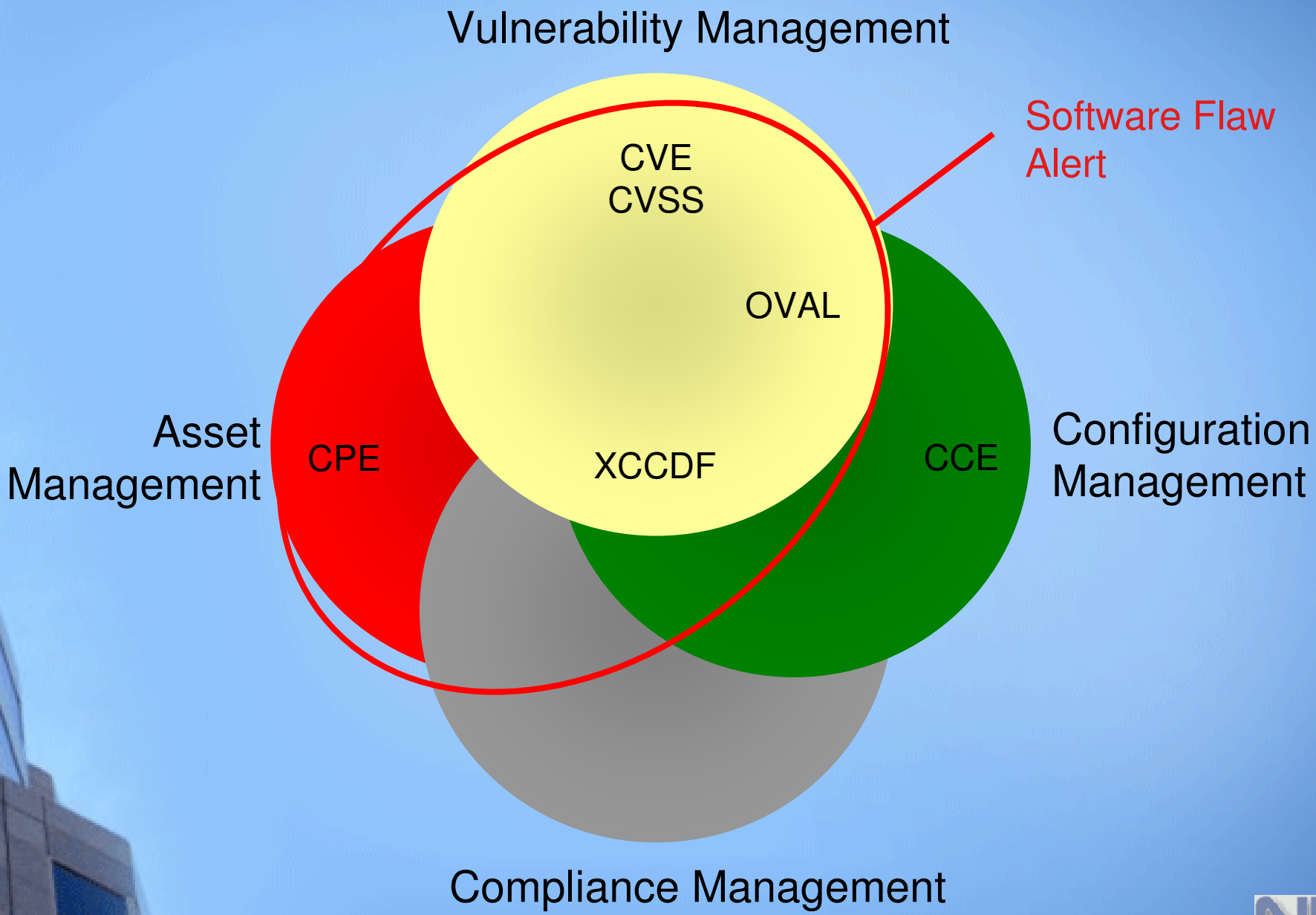
NIST

Integrating IT and IT Security Through SCAP



CVE	Common Vulnerability Enumeration
CPE	Common Platform Enumeration
CCE	Common Configuration Enumeration
XCCDF	eXtensible Checklist Configuration Description Format
OVAL	Open Vulnerability and Assessment Language
CVSS	Common Vulnerability Scoring System

Integrating IT and IT Security Through SCAP



Linking Configuration to Compliance

```
<Group id="IA-5" hidden="true">
 <title>Authenticator Management</title>
  <reference>ISO/IEC 17799: 11.5.2, 11.5.3</reference>
  <reference>PCI Data Security Standard v1.1 8.5.10</reference>
  <reference>European Data Protection Directive</reference>
  <reference> HIPAA SR 164.312(a)(1) Access Control </reference>
  <reference>CobIT DS5</reference>
  <reference>Bill 198 2002 (C-SOX)</reference>
 <reference>Financial Instruments and Exchange Law (J-
    SOX)</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>
```

Rationale for security configuration

Operational Efficiency

- Map it up-front
- Map it only once
- Map it with expertise - let technologists be technologists
- Support standardized builds
- Communicate clearly and definitively
- Communicate broadly

Slogans

- A “Scan Once, Report Many” technology
- Make compliance a by-product of security

Risk Management Framework

ORGANIZATIONAL VIEW

Architecture Description

FEA Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

Risk Executive Function

Starting Point

Organizational Inputs

Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53

Security Plan

Step 3
IMPLEMENT
Security Controls
SP 800-70

Step 4
ASSESS
Security Controls
SP 800-53A

Security Assessment Report

Step 5
AUTHORIZE
Information Systems
SP 800-37

Plan of Actions & Milestones

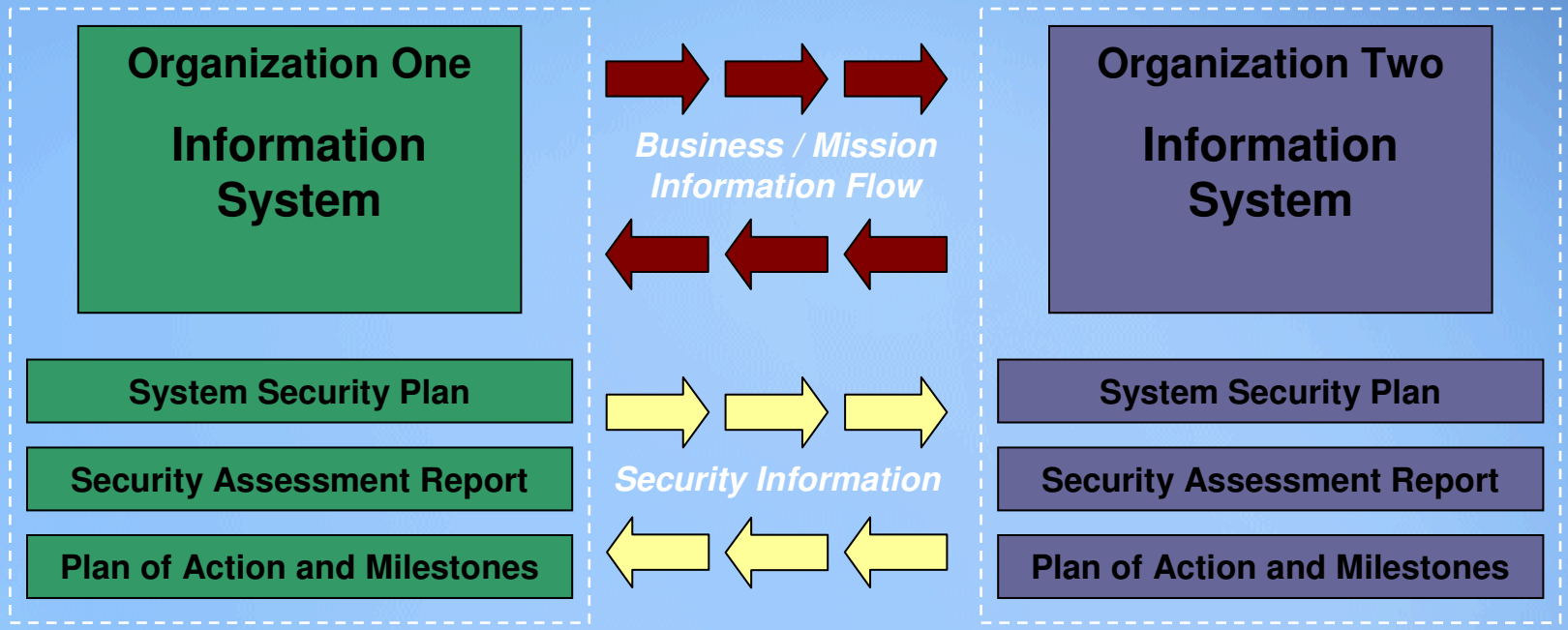
Step 6
MONITOR
Security State
SP 800-37 / 800-5A

RISK MANAGEMENT FRAMEWORK

Security Life Cycle

- Go Live
- System Risk Acceptance
- Accreditation
- Certification and Accreditation
- Similarly - SAS-70 Type II Audits

Agility in a Digital World



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

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

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

How do you make assessment/audit data:

- Uniform
- Sharable
- Consumable

How do you make an assessment/audit:

- Scalable
- Repeatable
- Low cost

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			

Use Case: The Office of Management and Budget Federal Desktop Core Configuration

Repeatable Assessments and Uniform Reporting

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.

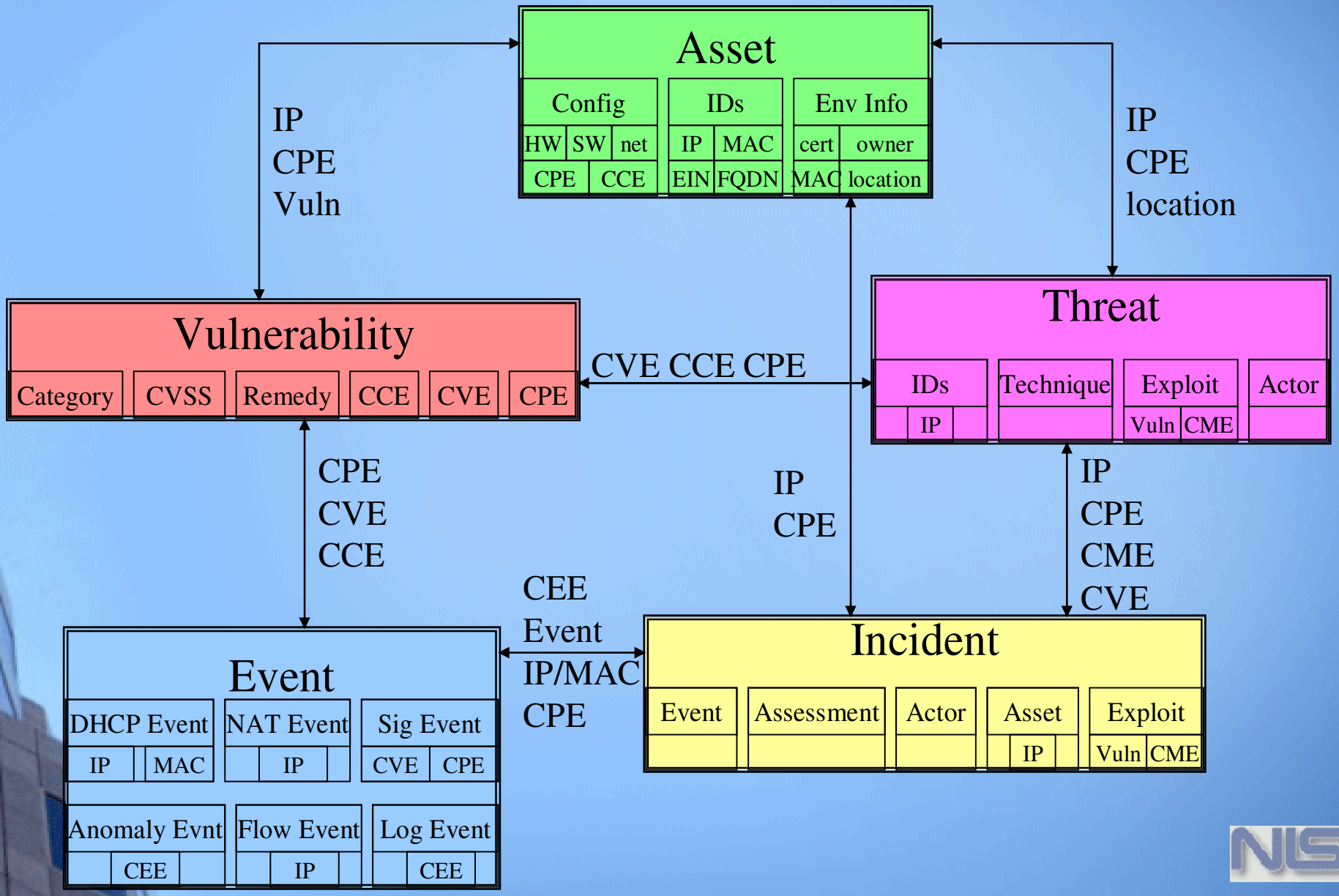
For additional information about this initiative, please call 1-800-FED-INFO. Additional information about the S-CAP can be found at: http://nvd.nist.gov/scap.cfm.

"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."**

Use Case: The Office of Secretary of Defense Computer Network Defense Data Pilot

Integrated and Timely Situational Awareness



Use Case: The Payment Card Industry Technical and Operational Reqs for ASVs

Standardized Software Flaw Content and Impact Scores

Version 1.1 of Technical and Operational Requirements for Approved Scanning Vendors (ASVs)

"The **detailed report** must be readable and accurate, and must include the following:

- …
- Detailed statement for each vulnerability found on the customer infrastructure, including:
  - …
  - Industry reference numbers such as CVE, CAN, or Bugtraq ID
  - Severity level - Common Vulnerability Scoring System (CVSS), http://www.first.org/cvss/, base score, as indicated in the National Vulnerability Database (NVD), http://nvd.nist.gov/cvss.cfm (where available)
  - …"

NIST

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

Contact Information

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

Steve Quinn
(301) 975-6967
stephen.quinn@nist.gov

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

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

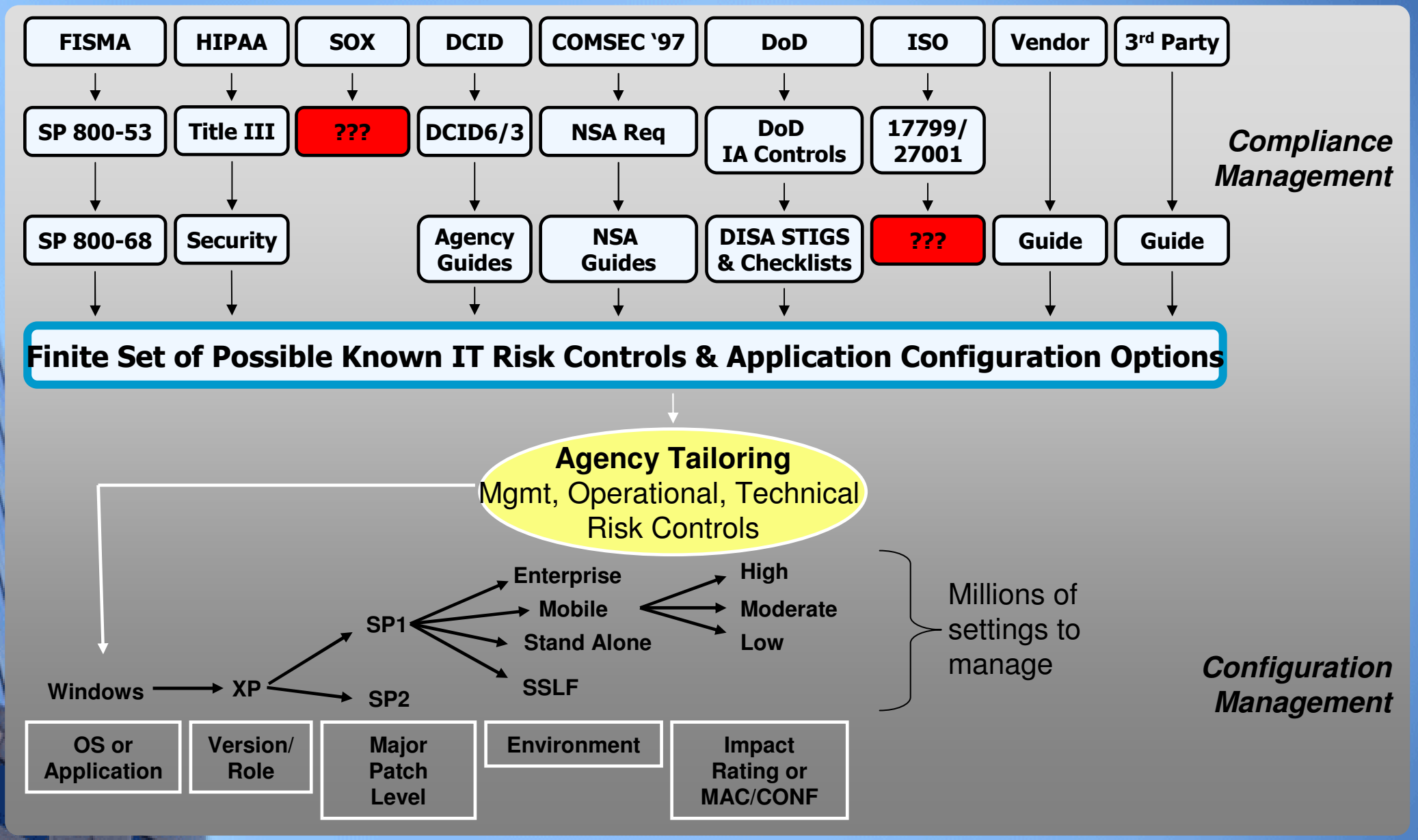
Murugiah Souppaya
(301) 975-4758
murugiah.souppaya@nist.gov

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

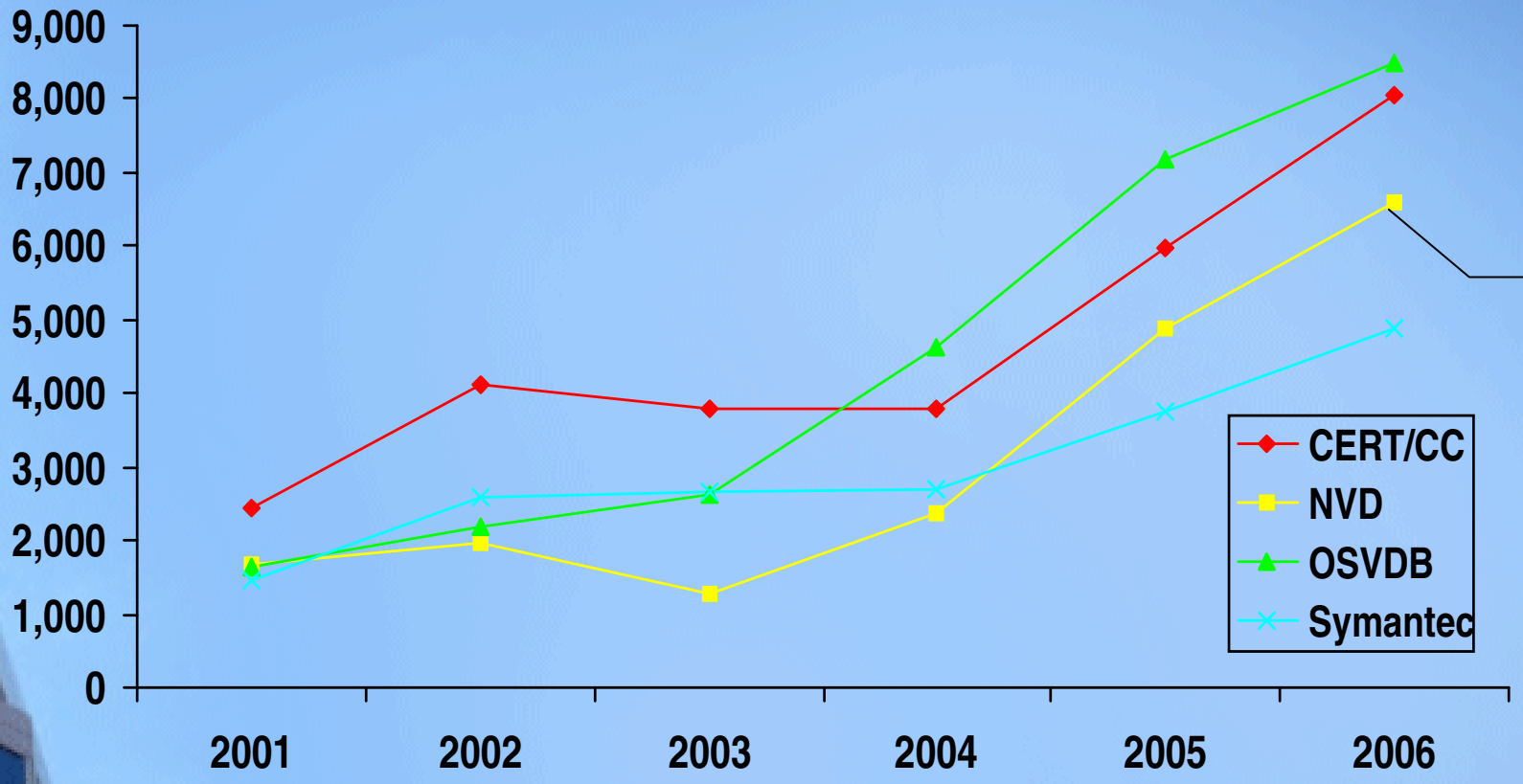
Information and Feedback
Web: http://scap.nist.gov
Comments: scap-update@nist.gov

Additional Information

Current State: Compliance and Configuration Management



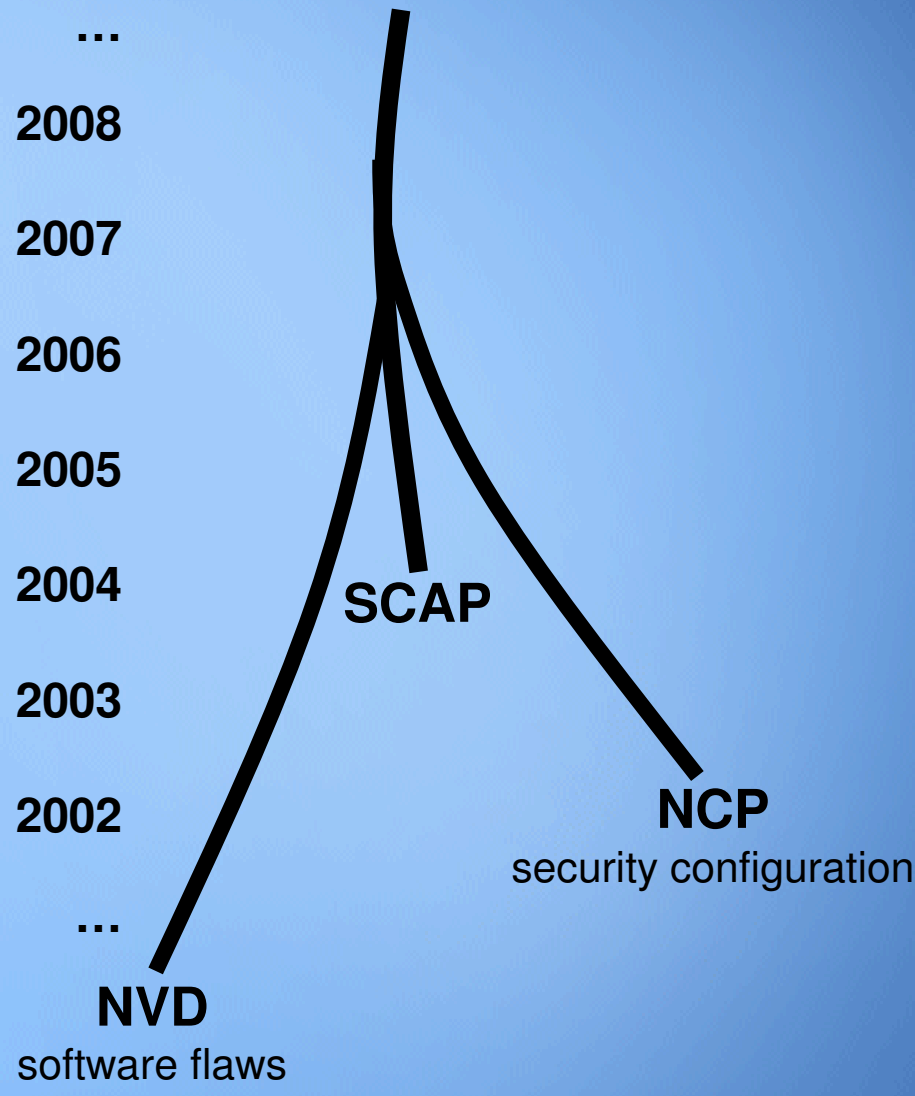
Current State: Vulnerability Trends



- Decreased timeline in exploit development
- 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.

Convergent Evolution of Post-Compilation Software Maintenance

- 2008-09: NVD will become production-ready for SCAP version 1.0
- 2007: OMB mandates use of SCAP validated tools for assessing Federal Desktop Core Configuration (FDCC)
- 2007: NCP legacy checklists become available through NVD Web site
- 2007: NCP promotes SCAP as the preferred format for all new checklists
- 2006-07: Announcements that the following guidelines will be available in SCAP format:
  - DISA Security Technical Implementation Guides (STIG)
  - JTF-GNO Information Assurance Vulnerability Management (IAVM) alerts
  - RedHat Security Guides
- 2006: NVD becomes reference data for SCAP
- 2006: SCAP reaches Beta formulation with publication of the NIST Draft Interagency Report (IR) 7343
- 2005: iCAT becomes NVD
- 2002: NCP established through Cyber Security R&D Act of 2002
- 1999: iCAT established



SCAP Value

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