Security Content Automation Protocol for Governance, Risk, Compliance, and Audit

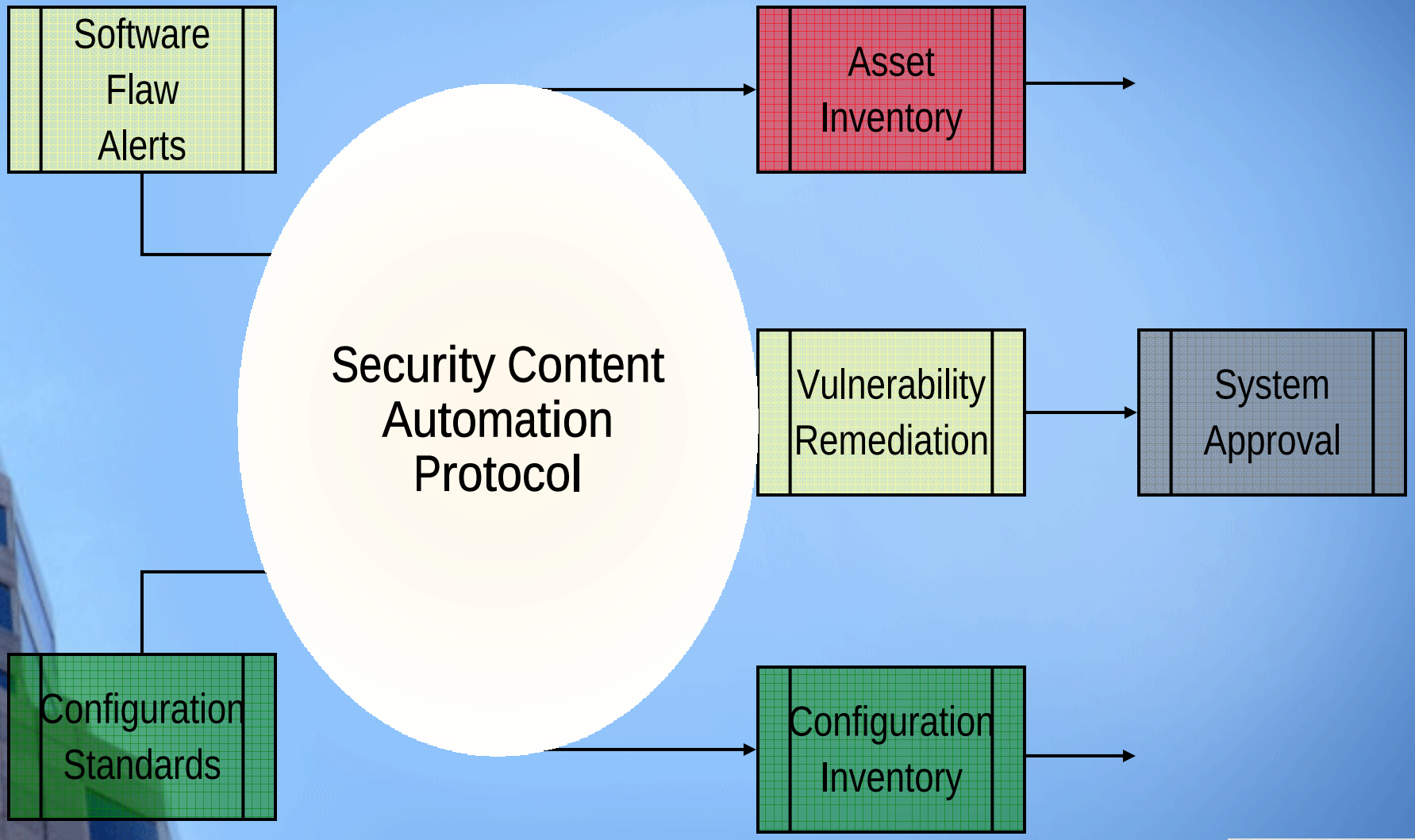
presented by:

Tim Grance
The National Institute of Standards and Technology

Agenda

- NIST's IT Security Automation Agenda
- Definitions of Security Content Automation Protocol (SCAP)
- How SCAP Works
- SCAP for Compliance
- Use Cases
- Emerging Use Cases
- SCAP Validation Program
- Relevant NIST Publications
- Recommendations

Enterprise Information Security Reporting Flow Diagram



Definitions of SCAP

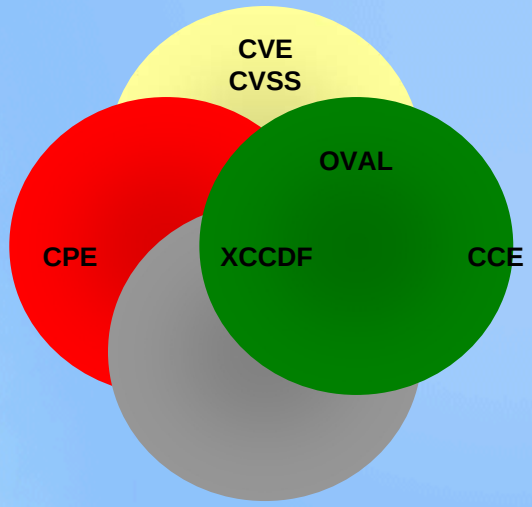
-A technology to bring interoperability to vulnerability management products of differing manufacture
-A standard input and output format for vulnerability management products
-Standardized and transparent expression of security configurations and software flaws
- A suite of vulnerability management specifications that together enable standardization and automation of vulnerability management, measurement, and technical policy compliance checking
-A vehicle for network hygiene
-The plumbing for delivering information security to the enterprise

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)

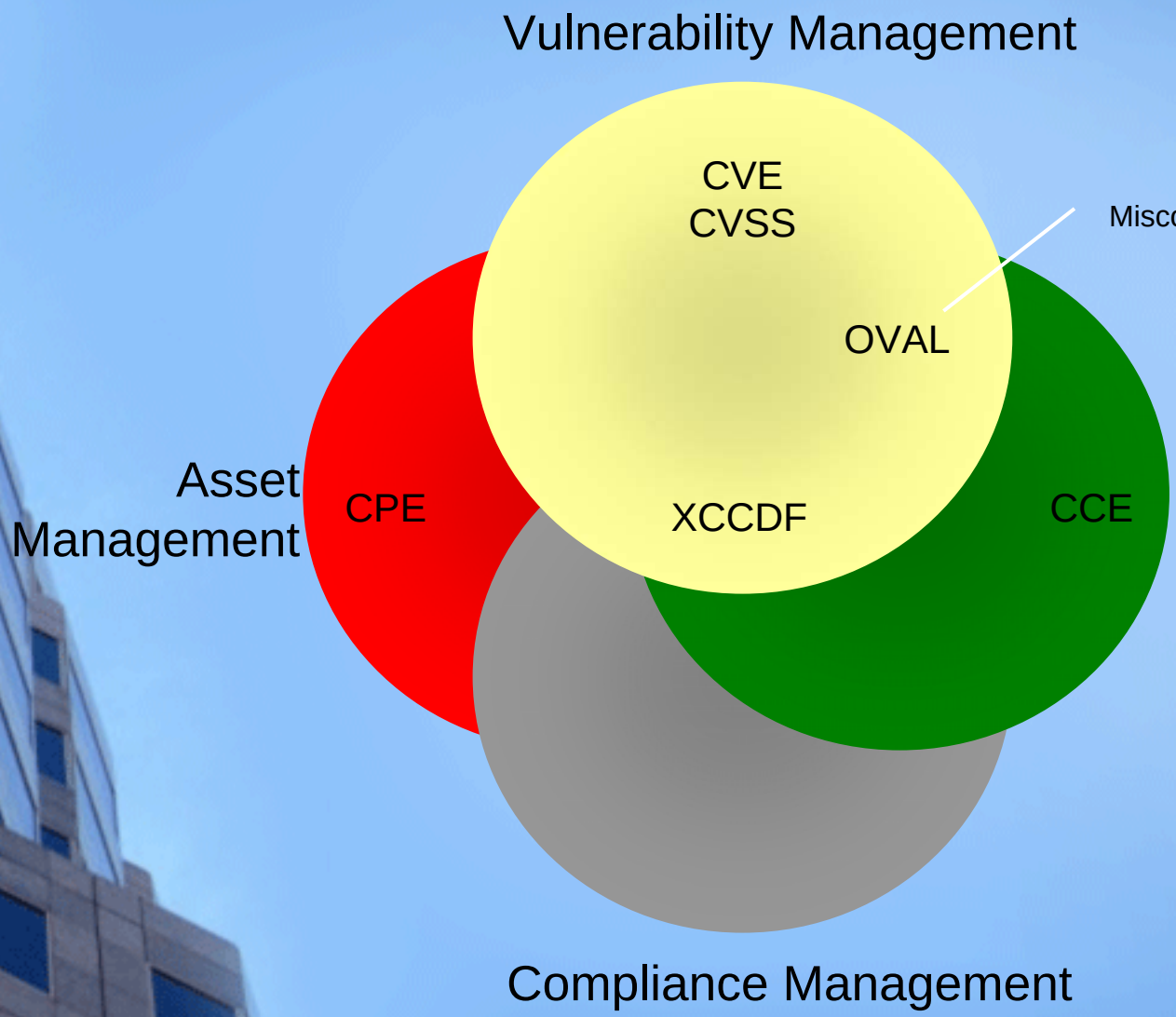
Standardizing How We Communicate

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 and 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

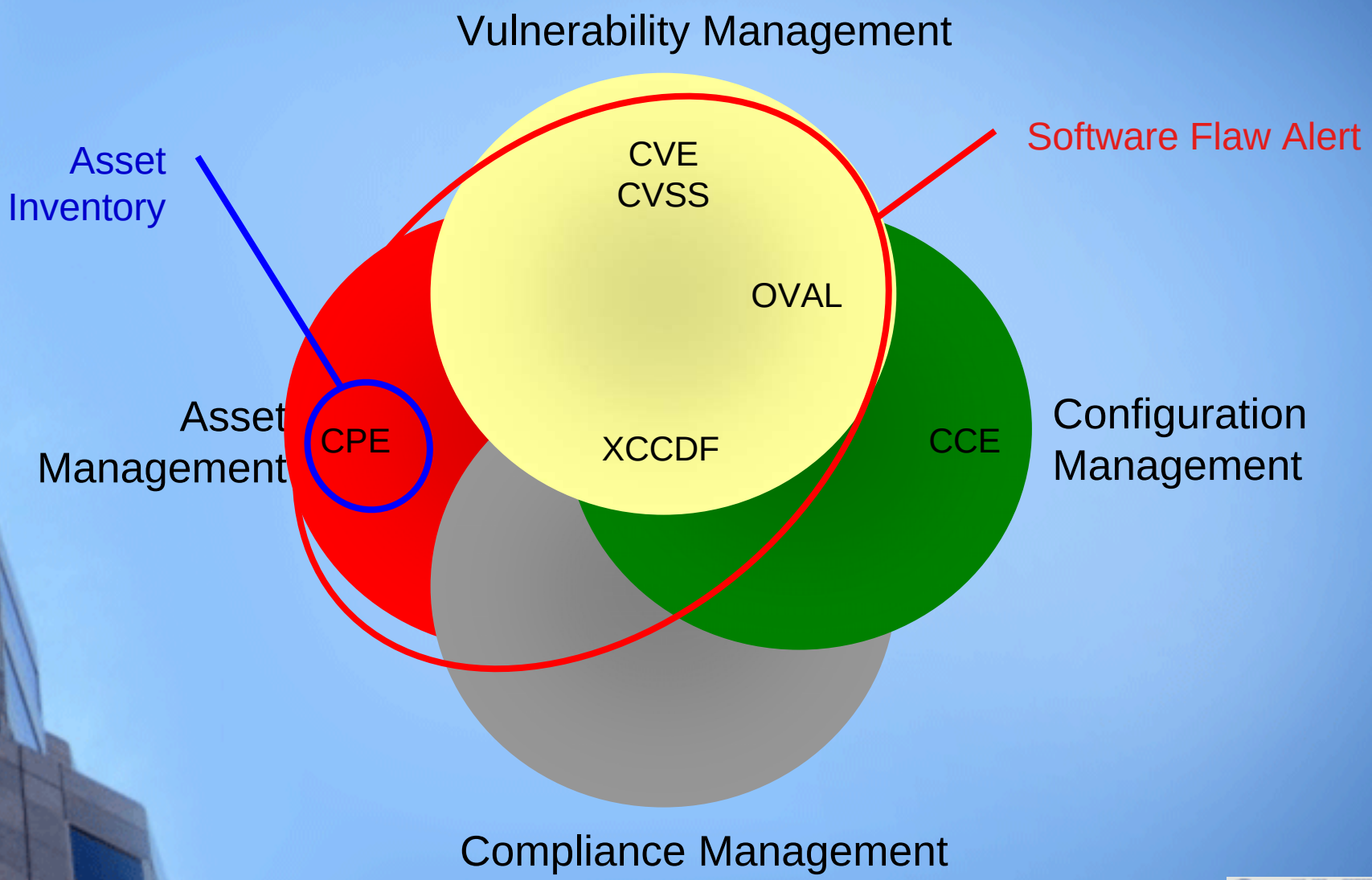
NIST

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

Understanding Software Flaw Exposure



Existing Federal Content

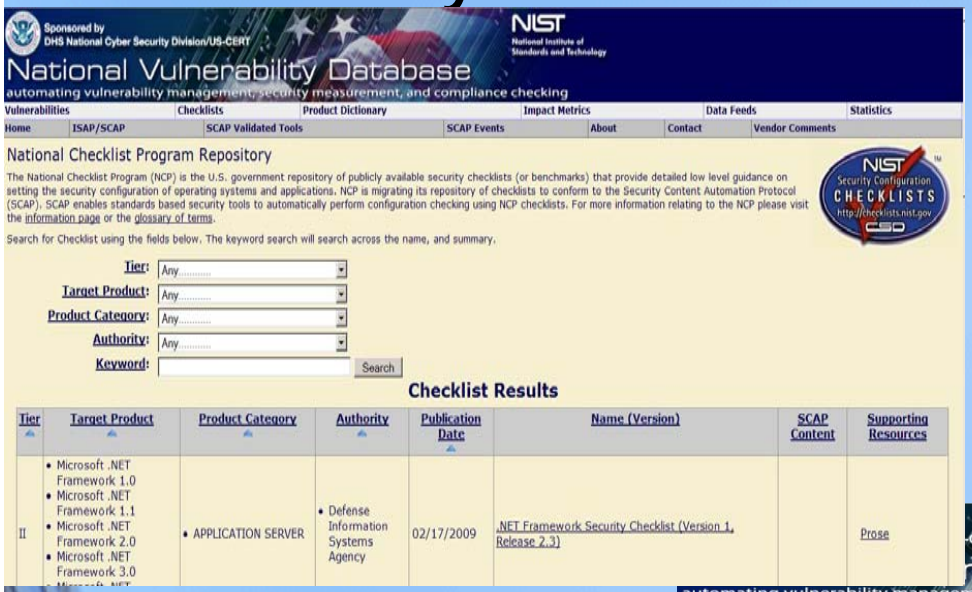
Standardizing What We Communicate

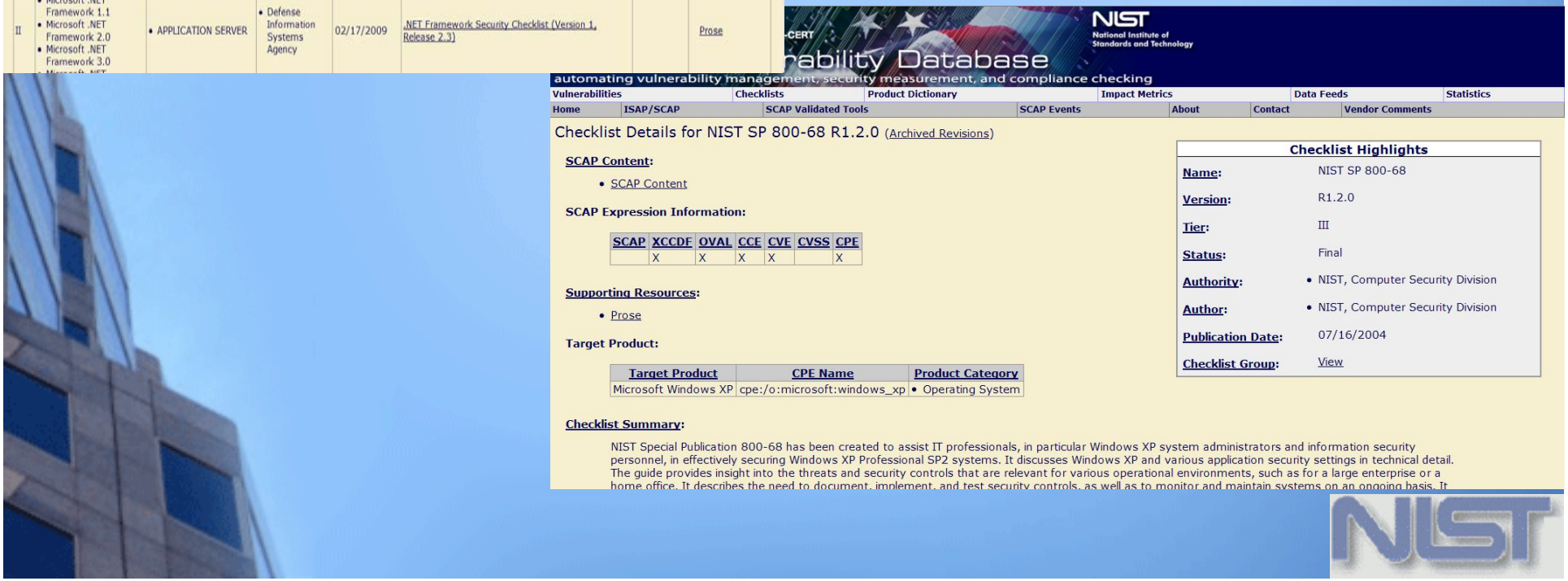
- In response to NIST being named in the Cyber Security R&D Act of 2002
- Encourages vendor development and maintenance of security guidance
- Currently hosts 135 separate guidance documents for over 165 IT products
- Translating this backlog of checklists into the Security Content Automating Protocol (SCAP)
- Participating organizations: DISA, NSA, NIST, Hewlett-Packard, CIS, ITAA, Oracle, Sun, Apple, Microsoft, Citadel, LJK, Secure Elements, ThreatGuard, MITRE Corporation, G2, Verisign, Verizon Federal, Kyocera, Hewlett-Packard, ConfigureSoft, McAfee, etc.

- Over 4 million hits per month
- About 20 new vulnerabilities per day
- Mis-configuration cross references to:
  - NIST SP 800-53 Security Controls (All 17 Families and 163 controls)
  - DoD IA Controls
  - DISA VMS Vulnerability IDs
  - Gold Disk VIDs
  - DISA VMS PDI IDs
  - NSA References
  - DCID
  - ISO 17799
- Reconciles software flaws from:
  - US CERT Technical Alerts
  - US CERT Vulnerability Alerts (CERTCC)
  - MITRE OVAL Software Flaw Checks
  - MITRE CVE Dictionary
- Produces XML feed for NVD content

NIST

National Checklist Program Hosted at National Vulnerability Database Website





How SCAP Works

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

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

Linking Configuration to Compliance

REFERENCES

IA-5 - Authenticator Management

NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10, 15.1.11, 15.1.12, 15.1.13, 16.1.3, 16.2.3
GAO FISCAM: AC-3.2
DOD 8500.2: IAKM-1, IATS-1
DCID 6/3: 4.B.2.a(7), 4.B.3.a(11)
CobIT DS5
ISO/IEC 17799: 11.5.2, 11.5.3
HIPAA SR 164.312(a)(1) Access Control
PCI Data Security Standard v1.1 8.5.10
800-68 Section 6.1 - Table A-1.4
DISA STIG Section 5.4.1.3
DISA Gold Disk ID 7082
PDI IAIA-12B
NSA Chapter 4 - Table 1 Row 4
CCE-100 - minimum-password-length

RULE

CCE-100 - minimum-password-length

test procedures…

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

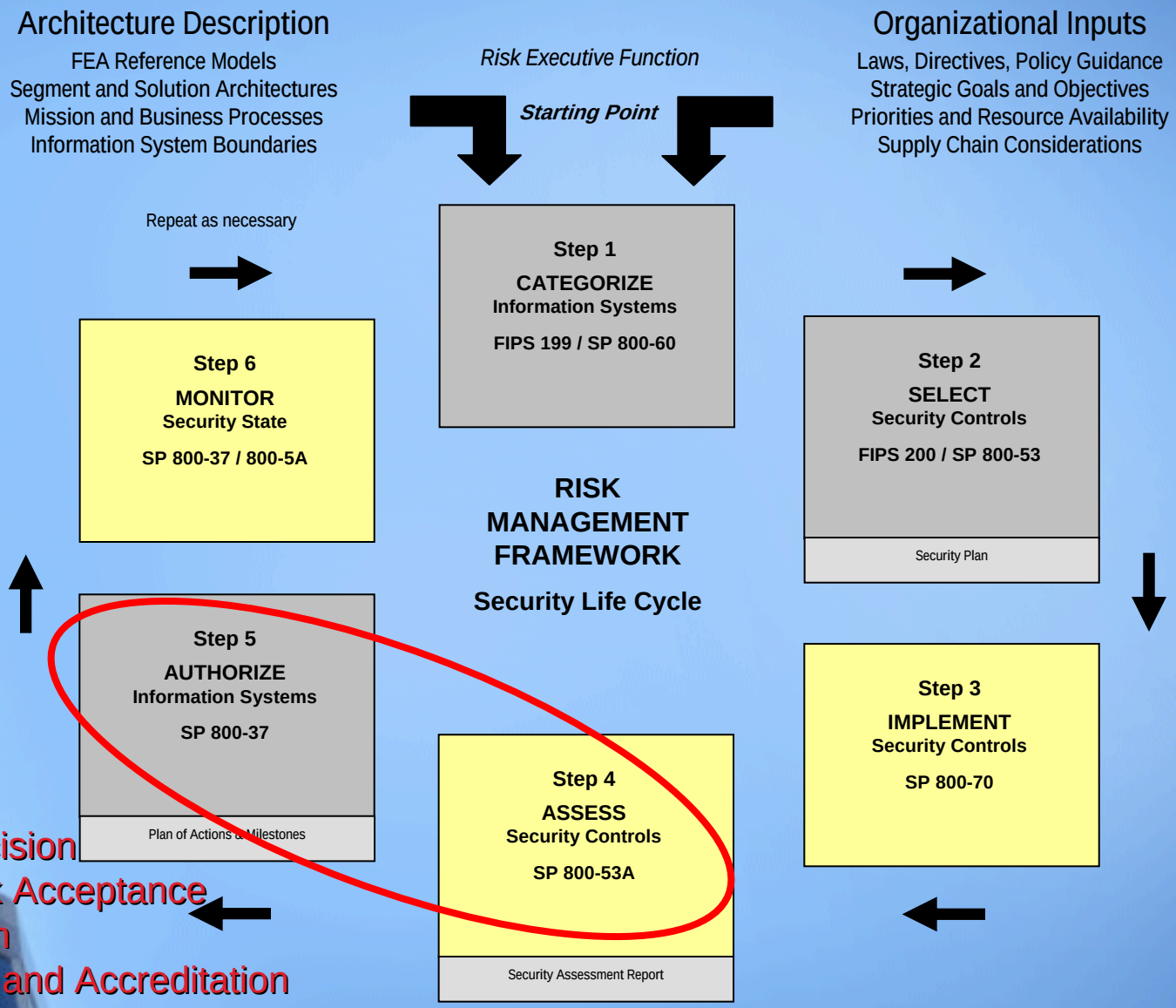
- A “Scan Once, Report Many” technology
- Make compliance a by-product of security

800-53 Controls with Automated Checking

Tool Set	Automation	Control Count	Control Percent	Control Example
Framework Tools	Full Automation	-	-	-
	Partial Automation	49	30%	PL-2 System Security Plan
Security Content Automation Protocol	Full Automation	31	19%	AC-11 Session Lock
	Partial Automation	39	24%	AC-8 System Use Notification
Future Automation Techniques or No Automation		44	27%	AC-1 Access Control Policy and Procedures
	Total Controls	163	100%	

Risk Management Framework

ORGANIZATIONAL VIEW



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

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.

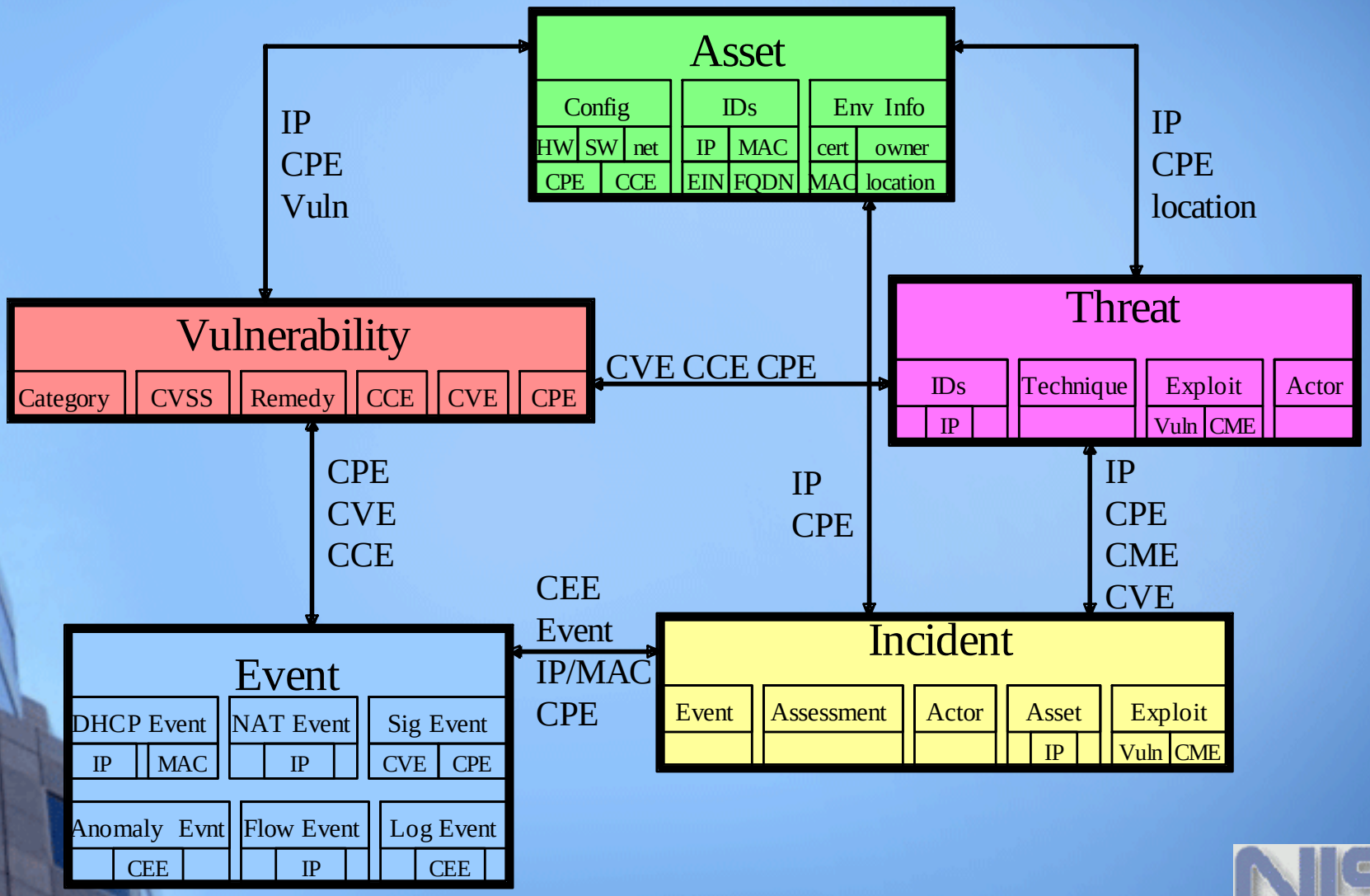
For additional information about this initiative, please call 1-800-FED-INFO. Additional information about the S-CAP can be found at: http://nvd.nist.gov/scap.cfm.

OFFICE OF MANAGEMENT AND BUDGET

"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."

NIST

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

PCI Security Standards Council

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

International Adoption

- Spanish Government
- Italian Government
- European Union/EC
- Japanese Government

Emerging Use Cases

- SCAP Checklists as software flaw alert format
- SCAP Reports as technical appendix to system risk acceptance documents
- SCAP Checklists as communication from central OCIO, IG, and audit bodies on implementation expectations
- SCAP Reports as evidence of implementation and adjustment of technical security controls (e.g., evidence for SAS-70 Type II audit)
- SCAP Reports to perform comparative analysis for infrastructure connections (e.g., long-term partnerships, merger, acquisition)

SCAP Validation Program Status

As of 6 January 2009,
11 months of operation…

- 10 Accredited labs

Validated Products

- 13 vendors
- 19 products
- 68 capabilities-based validations
- 13 standards-based validations

- All 13 vendors and 17/19 products are FDCC Scanner validated

…and more to come in 2009.

BIGFIX
Transforming IT Management
Gideon Technologies — Know your assets. Know your risk.
Lumension Security
McAfee
nCircle — Proactive Network Security
netIQ — An Attachmate Business
secure elements
Shavlik
symantec.
TENABLE Network Security
ThreatGuard
Triumfant

SCAP Documentation

- SP800-117: DRAFT Adopting and Using Security Content Automation Protocol
- *COMING SOON* SP800-126: Security Content Automation Protocol Specification
- SP800-70 Rev 1: DRAFT National Checklist Program for IT Products--Guidelines for Checklist Users and Developers
- IR-7511: DRAFT Security Content Automation Protocol (SCAP) Validation Program Test Requirements
- IR-7435: The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems
  IR-7275 Rev 3: Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4
- IR-7502: DRAFT The Common Configuration Scoring System (CCSS)

Recommendations

- Investigate use of SCAP for existing use cases – talk with stakeholders and NIST
- Consider emerging use cases – talk with NIST
- Determine if your current tool set has been SCAP Validated – visit http://nvd.nist.gov
- Read relevant NIST documents
- Join mailing lists to monitor community dialog
- Attend the Fifth Annual Security Automation Conference in Fall 2009

Questions?

Presenter:

Tim Grance

grance@nist.gov

SCAP Homepage: http://scap.nist.gov

SCAP Validation Tools: http://nvd.nist.gov/scapproducts.cfm

SCAP Validation Homepage: http://nvd.nist.gov/validation.cfm

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

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