



Creating Value from Vulnerability

**Vulnerability Analysis & Operations Group
Information Assurance Directorate
National Security Agency**

4 Sept 2007



NSA Information Assurance



Coming From...	Moving to...
Protect classified information...	and real-time defense of information & systems
Focus on GOTS crypto	Broad spectrum of COTS IA & IT
More products than services	More services than products, and more influence than “doing”
Avoid risk	Manage risk
Find & mitigate vulnerability	... and detect the threat



- **Improve the security of Commercial Technology**
- **Influence all stakeholders:**
 - **Practitioners, Buyers, Users, Suppliers, Authorities**
- **Increase partnership**
- **Build a Knowledge vs Product Business**
- **Bring a dynamic, operational focus**



VAO Vision



***The nation's most
capable, influential, and trusted
source of actionable information
on network vulnerabilities and intrusions.***



VAO in the News



washingtonpost.com

The Washington Post

Today's Paper | Subscribe | PostPoints

GOVEXEC.COM

FROM THE MAGAZINE



Government Computer News



InformationWeek

BUSINESS INNOVATION POWERED BY TECHNOLOGY

InformationWeek

FCW.COM





Stakeholders in Assurance



Authorities

Suppliers

Buyers

Users

Practitioners



Stakeholders in Assurance



Authorities

Suppliers

Buyers

Users

Practitioners

**NSA, DISA, NIST, Center
for Internet Security**



Stakeholders in Assurance



Authorities

Suppliers

Buyers

Users

DISA STIGs, NIST Checklists,
Corporate baselines

Practitioners



Stakeholders in Assurance



Authorities

Suppliers

Buyers

AF, DOD, Standard desktop load

Users

Practitioners



Stakeholders in Assurance



Authorities

**OS Vendors, Tool Vendors,
Compliance Checkers**

Suppliers

Buyers

Users

Practitioners



Stakeholders in Assurance



**DoD Policy, OMB, FISMA,
Security Content Automation
Program (SCAP)**

Authorities

Suppliers

Buyers

Users

Practitioners



Vulnerability "Plumbing"



"CONTENT"

New IT vulns

**Security
Guides &
benchmarks**

**Red and Blue
Team Reports**

Product tests

Incident reports

"PLUMBING"

CVE

OVAL

CCE, CPE

CVSS

XCCDF

"FIXTURES"

**Multiple tools to
measure, fix, report**

Integrated reports

Integrated tools

Policy compliance

**Rapid vulnerability
sharing,
assessment,
remediation**



Security Content Automation (SCAP)



- ... to automate compliance, manage vulnerabilities and perform security measurement

Security Content Automation Program Content - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links

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

[Overview](#), [Security Content](#), [Utilities](#), [Compatible Tools](#), [Information](#), [Contact](#) NVC

Welcome to SCAP!!

The Security Content Automation Program enables organizations to automate security compliance, manage vulnerabilities, and perform security measurement.

Email List

Enter your e-mail address and press "Add" to receive [Security Content Automation announcements](#).

Resource Status

The Security Content Automation Project contains:
Definitions and tests to

Security Content Automation Program Content

This page contains detailed checklists that specify NSA, DISA, and NIST recommended software configuration requirements. Each vulnerability check is mapped to high level compliance policies such that use of these checklists can automate an organization's technical control compliance activities. Organizations can also use the checklists, apart from compliance activities, to check for vulnerabilities (both misconfigurations and software flaws) and to measure their application security posture.

NIST recommends use of these files to produce security control testing evidence within Federal Information Security Management Act (FISMA) compliance efforts. More specifically, use of these files can automate production of NIST SP800-53a technical control testing evidence.

These checklists are written in a machine readable form and are intended to be used in conjunction with [compatible commercial tools](#).

Operating Systems, Databases, Servers

OS/Server	Available Content	Configuration Content By	Patch/Vulnerabilities Content By	Comments
Apache HTTP Server	Coming Soon			



Integrated Analysis & Reporting

Security “Sampling”

**Community events, tools, standards,
reporting, lessons,...**

**Red
Team**

**Blue
Team**

OPSEC

COMSEC

TechSec



To gain assurance, we must



- ***Organize...*** the data generators
- ***Standardize...*** the raw data
- ***Translate...*** into something useful upstream
- ***Link to...*** other business areas
 - e.g., network management, compliance



- **Bring content**
 - and good people to the conversation
- **Equip and organize the stakeholders**
 - esp. the Buyers
- **Abstract the interfaces**



To learn more...



- ***NSA Security Guidance***

- <http://www.nsa.gov/snac/>

- ***The Security Content Automation Program***

- <http://nvd.nist.gov/scap/scap.cfm>

- ***Common Vulnerability & Exposures***

- <http://cve.mitre.org>