



National Institute of Standards and Technology (NIST)

The Information Technology Lab Computer Security Division (893)

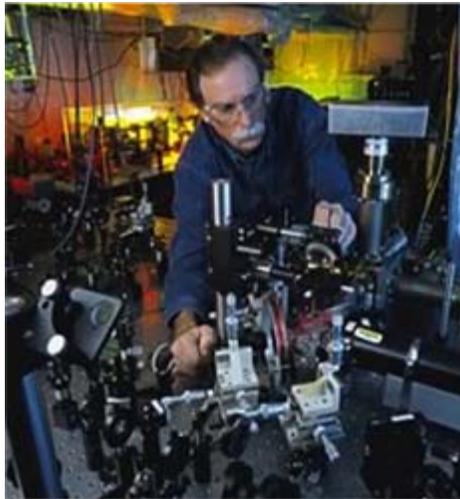


Now What?

What does NIST have for you to use and how do you get it?

How do you contact us and receive updates?

How else can you participate, influence, ask more questions?



© Geoffrey Wheeler



©Robert Rathe



©Robert Rathe



Agenda

- How do we align with other SDOs/Requirements?
- What are some of our products?
 - Special Publications
 - Federal Information Processing Standards
 - NIST Inter-Agency Reports
- How do you get these products?
- Do you have to use these products?
- Do you want to use these products?
- Other products available to you from CSD



NIST Participation and Alignment with SDOs

- Internet Engineering Task Force (IETF) Security Chair (IETF)
- Committee for National Security Systems (CNSS)
- International Organization for Standardization (Chair/Convener several Committees, Work Groups, and Task Forces) (ISO)
- American National Standards Institute (ANSI)
- InterNational Committee for Information Technology Standards (Biometrics Chair)
- Biometrics Consortium Co-Chair
- National Science & Technology Council Committee on Biometrics and Identity Management (Co-Chair)
- ISO 27002
- HIPAA



A Way NIST Helps

- The 800 Series Special Publications
 - A suite of guidelines to assist with the technological challenges in establishing and maintaining an information security program
 - Cover a WIDE range of program, process and technology. The RMF and then all the specifics that can “radiate” out from that wheel.
 - Written with deliberate flexibility to adapt to environments and support missions
 - Not mandatory for the Federal Civilian Agencies but can be required by other oversight bodies



How are SP 800 Docs Made?

- How we make these
 - Topics Selected
 - External Drivers e.g. Legislation, OMB Directives, HSPDs.
 - Technology Standards and Guidelines Needs/Gaps
 - Threat Activities
 - Vulnerability Areas
 - Requests from Constituents
 - Results of Research
 - Multiple Internal Drafts
 - Conducted in the Writing of the Guideline
 - Conducted Outside of the Authoring Team
 - Conducted Outside of the Division
 - Public Drafts
 - Posted on the Internet for Review and Comment
 - Multiple Public Drafts Used if Necessary
 - Phase in Period



Examples of Some SP 800 Docs.

NIST National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC: GO

ABOUT MISSION CONTACT STAFF SITE MAP

Computer Security Division Computer Security Resource Center

CSRC HOME GROUPS PUBLICATIONS DRIVERS NEWS & EVENTS ARCHIVE

CSRC HOME > PUBLICATIONS > BY SPECIAL PUBLICATIONS

CATEGORY TYPES

- by Draft Publications
- by FIPS Publications
- by Special Publications
- by NIST IRs
- by ITL Security Bulletins

NIST INFORMATION SECURITY DOCUMENT CATEGORIES

- by Topic Clusters
- by Family
- by Legal Requirement

Subscribe to the CSRC Publications Mailing List

Click Here to download the "Guide to NIST Information Security Documents."



Click Here to download the "Roadmap to NIST Information Security Documents."



*NOTE: Categories in the Families, Topic Clusters, and Legal Requirements listings are from the "Guide to NIST Information Security Documents."

PUBLICATIONS

Special Publications (800 Series)

Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

Special Publications

Number	Date	Title
SP 800-124	July 7, 2008	DRAFT Guidelines on Cell Phone and PDA Security Draft-SP800-124.pdf
SP 800-123	Jul 2008	Guide to General Server Security SP800-123.pdf
SP 800-121	Sept 2008	Guide to Bluetooth Security SP800-121.pdf SP800-121.pdf.zip
SP 800-116	September 10, 2008	DRAFT (second draft) A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) SP800-116-2nd-draft-v2.pdf Comments_SP800-116.xls
SP 800-115	Sept 2008	Technical Guide to Information Security Testing and Assessment SP800-115.pdf
SP 800-114	Nov 2007	User's Guide to Securing External Devices for Telework and Remote Access SP800-114.pdf
SP 800-113	Jul 2008	Guide to SSL VPNs SP800-113.pdf



SPs Published in FY08

- SP 800-114 User's Guide to Securing External Devices for Telework and Remote Access.
- SP 800-111 Guide to Storage Encryption Technologies for End User Devices.
- SP 800-38 Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
- SP 800-53 Rev. 2 Recommended Security Controls for Federal Information Systems.
- SP 800-28 Ver. 2 Guidelines on Active Content and Mobile Code.
- SP 800-61 Rev. 1 Computer Security Incident Handling Guide.
- SP 800-87 Rev. 1 Codes for the Identification of Federal and Federally-Assisted Organizations.
- SP 800-53 A Guide for Assessing the Security Controls in Federal Information Systems.
- SP 800-67 Rev. 1.1 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.
- SP 800-79-1 Guidelines for the Accreditation of Personal Identity Verification Card Issuers.
- SP 800-113 Guide to SSL VPNs.
- SP 800-55 Rev. 1 Performance Measurement Guide for Information Security.
- SP 800-48 Rev. 1 Guide to Securing Legacy IEEE 802.11 Wireless Networks.
- SP 800-123 Guide to General Server Security.
- SP 800-60, Rev. 1 Vol. 1 & 2 Guide for Mapping Types of Information and Information Systems to Security Categories and Appendices.
- SP 800-73-2 Interfaces for Personal Identity Verification.
- SP 800-121 Guide to Bluetooth Security.
- SP 800-115 Technical Guide to Information Security Testing and Assessment.



A Way NIST Helps

- Federal Information Processing Standards
 - Different than the Special Publications
 - Federal Standards Required for Use by All Civilian Federal Agencies
 - Waivers ONLY by the President
- How we make these
 - Only Done When Required or Great Compelling Need
 - Required by Legislation (FISMA)
 - Required for Encryption (Compelling Need)
 - Not Done Often
 - Announced Through Federal Register
 - All Comments Publically Posted
 - Must Be Approved by the Secretary of Commerce



Federal Information Processing Standards

Computer Security Division
Computer Security Resource Center

CSRC HOME GROUPS PUBLICATIONS DRIVERS NEWS & EVENTS ARCHIVE

- CATEGORY TYPES
- by Draft Publications
 - by FIPS Publications**
 - by Special Publications
 - by NIST IRs
 - by ITL Security Bulletins

- NIST INFORMATION SECURITY DOCUMENT CATEGORIES
- by Topic Clusters
 - by Family
 - by Legal Requirement

[Subscribe to the CSRC Publications Mailing List](#)



[Click Here](#) to download the "Guide to NIST Information Security Documents."



[Click Here](#) to download the "Roadmap to NIST Information Security Documents."

*NOTE: Categories in the Families, Topic Clusters, and Legal Requirements listings are from the "Guide to NIST Information Security Documents."

CSRC HOME > PUBLICATIONS > BY FIPS PUBLICATIONS

PUBLICATIONS

FIPS Publications

FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

FIPS

Number	Date	Title
FIPS 201-1	Mar 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors FIPS-201-1-chng1.pdf
FIPS 200	Mar 2006	Minimum Security Requirements for Federal Information and Information Systems FIPS-200-final-march.pdf
FIPS 199	Feb 2004	Standards for Security Categorization of Federal Information and Information Systems FIPS-PUB-199-final.pdf
FIPS 198-1	Jul 2008	The Keyed-Hash Message Authentication Code (HMAC) FIPS-198-1_final.pdf
FIPS 197	Nov 2001	Advanced Encryption Standard fips-197.pdf fips-197.ps
FIPS 196	Feb 1997	Entity Authentication Using Public Key Cryptography fips196.pdf fips196.ps
FIPS 191	Nov 1994	Guideline for The Analysis of Local Area Network Security fips191.pdf
FIPS 190	Dec 1994	Guideline for the Use of Advanced Authentication



FIPSs Published in FY08

- FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC)



A Way NIST Helps

- NIST Inter-Agency Reports (NISTIRs)
- How we make these
 - Results of Research
 - Results of a Workshop, Conference, Forum
 - Often very Technical in Nature and/or Complement Submissions to Other Professional Publications
- Non-Binding and Not Required for Implementation
 - Internal and External Draft Process Follows that of SP 800 Doc.



NISTIRs Published in FY08

- IR 7442 Computer Security Division - 2007 Annual Report
- IR 7516 Forensic Filtering of Cell Phone Protocols
- IR 7511 Ver. 1.1 Security Content Automation Protocol (SCAP) Validation Program Test Requirements
- IR 7502 The Common Configuration Scoring System (CCSS)



When Do These Apply To You?

- The Federal Information Security Management Act (FISMA) Says:
(<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>)

“§ 3544. Federal agency responsibilities

“(a) IN GENERAL.—The head of each agency shall—

“(1) be responsible for—

“(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

“(i) information collected or maintained by or on behalf of the agency; and

“(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;



When Do These Apply To You?

- OMB Says: (<http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf>)

Contractor Monitoring and Controls

35. Must Government contractors abide by FISMA requirements?

Yes, and each agency must ensure their contractors are doing so. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.” Section 3544(b) requires each agency to provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.” This includes services which are either fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) solutions.

Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local Governments, industry partners, providers of software subscription services, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing Government information and interconnecting systems.

Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems.



When Do These Apply To You?

- So, what does that mean?

Some Valid Questions to Ask:

Am I in some form of data interchange with a civilian agency of the federal government?

Do I have a contract with them and what does it say regarding information and information system security?

Am I acting on "behalf of that agency?" Is this work for, being represented as, being paid by that agency? What does the agency say and what does your CIO, CISO and GC say?

What is my security program and other security requirements? How does that map and/or satisfy the requirements of the civilian agency?



What Else Could You Use from NIST/CSD?

The National Vulnerability Database (NVD)

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

The Security Content Automation Protocol (S-CAP)

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

The Federal Desktop Core Configurations (FDCC)

<http://nvd.nist.gov/fdcc/index.cfm>

The NIST Checklist Program

<http://checklists.nist.gov/>

FIPS 140 and the Cryptographic Module Validation Program

<http://csrc.nist.gov/groups/STM/cmvp/index.html>



The National Vulnerability Database (NVD)

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

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | ISAP/SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 33411 [CVE Vulnerabilities](#)
- 143 [Checklists](#)
- 151 [US-CERT Alerts](#)
- 2275 [US-CERT Vuln Notes](#)
- 2097 [OVAL Queries](#)

Last updated: 10/28/08
CVE Publication rate: 18 vulnerabilities / day

Email List

NVD provides four mailing lists to the public. For information and

National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the [Security Content Automation Protocol](#) (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the [Information Security Automation Program](#) (ISAP).

Federal Desktop Core Configuration settings (FDCC)

NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the [FDCC](#) using the Security Content Automation Protocol ([SCAP](#)). [FDCC Checklists](#) are available here (to be used with SCAP FDCC capable tools). [SCAP FDCC Capable Tools](#) are available here.

NVD Primary Resources

- [Vulnerability Search Engine](#) (CVE software flaws and CCE misconfigurations)
- [National Checklist Program](#) (automatable security configuration guidance in XCCDF and OVAL)
- [ISAP/SCAP](#) (program and protocol that NVD supports)
- [SCAP Compatible Tools](#)
- [SCAP Data Feeds](#) (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- [Product Dictionary](#) (CPE)
- [Impact Metrics](#) (CVSS)
- [Common Weakness Enumeration](#) (CWE)



NVD

- RSS Feeds
- Common Vulnerability Scoring System

CVSS Version 2 Scoring Page (CVE-2008-1446)

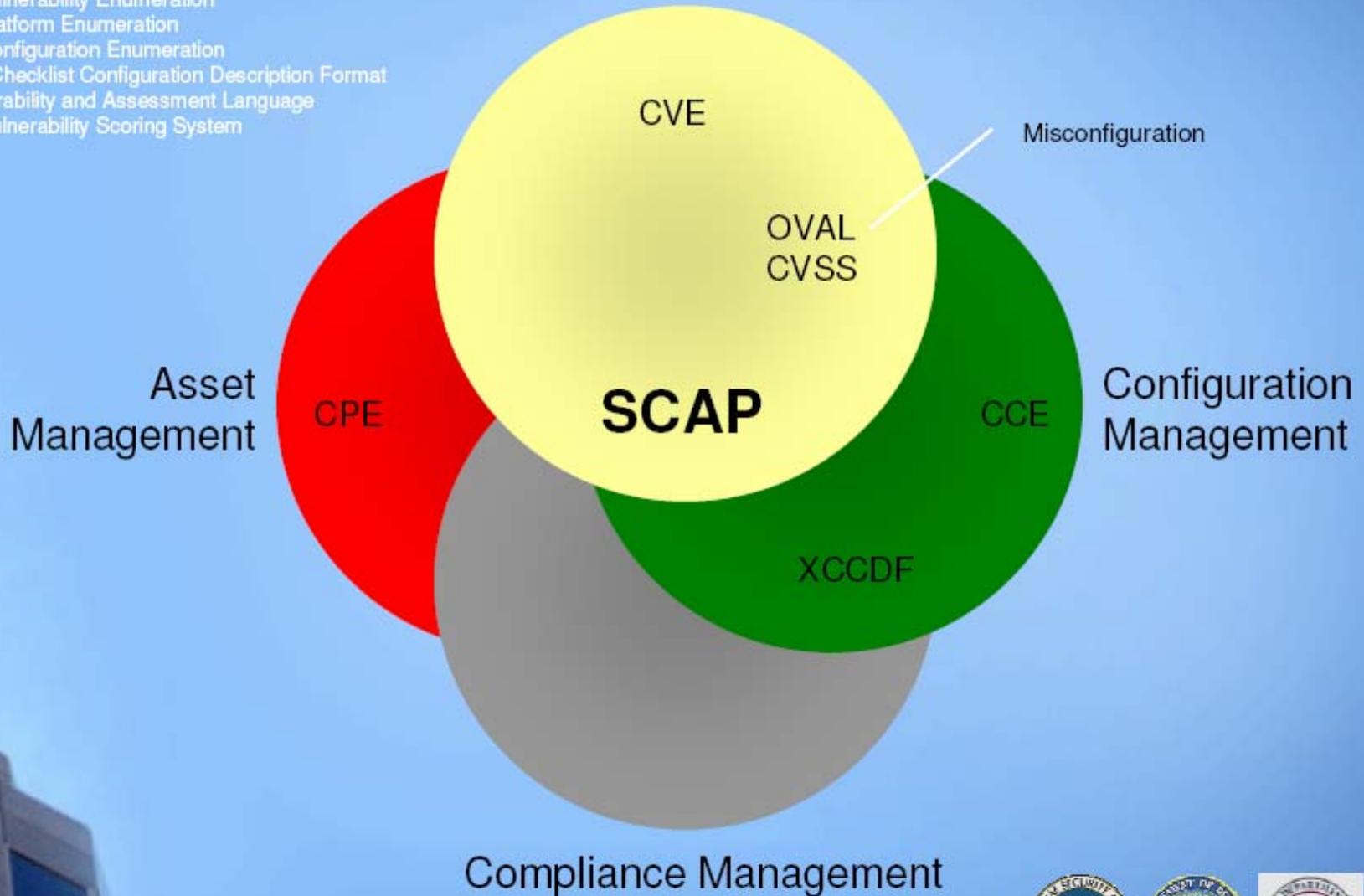
This page shows the components of the CVSS score for CVE-2008-1446 and allows you to refine the CVSS base score. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score. A [concise](#) form of this page is available to CVSS experts.

Update Scores	Reset Scores	View Equations	Environmental Score Metrics	
CVSS Base Score 9			This section addresses metrics that describe the effect of a vulnerability within an organization's environment. These metrics must be calculated separately for each organization.	
Impact Subscore 10				
Exploitability Subscore 8				
CVSS Temporal Score Undefined			General Modifiers	
CVSS Environmental Score Undefined			Organization specific potential for loss (CollateralDamagePotential) <input type="text" value="Not Defined"/>	
Overall CVSS Score 9			Percentage of vulnerable systems (TargetDistribution) <input type="text" value="Not Defined"/>	
<hr/>				
Base Score Metrics				
These metrics describe inherent characteristics of the vulnerability. These scores have already been calculated for this vulnerability.				
Exploitability Metrics				
Related exploit range (AccessVector)	<input type="text" value="Network"/>			
Attack complexity (AccessComplexity)	<input type="text" value="Low"/>			
Level of authentication needed (Authentication)	<input type="text" value="Single Instance"/>			
Impact Metrics				
Confidentiality impact (ConfImpact)	<input type="text" value="Complete"/>			
Integrity impact (IntegImpact)	<input type="text" value="Complete"/>			
Availability impact (AvailImpact)	<input type="text" value="Complete"/>			
Impact Subscore Modifiers				
System confidentiality requirement (draft proposal) (ConfidentialityRequirement)			<input type="text" value="Not Defined"/>	
System integrity requirement (draft proposal) (IntegrityRequirement)			<input type="text" value="Not Defined"/>	
System availability requirement (draft proposal) (AvailabilityRequirement)			<input type="text" value="Not Defined"/>	
<hr/>				
Temporal Score Metrics				
These metrics describe elements about the vulnerability that change over time. If all of these values are left as 'Undefined', the environmental score will be based on the base score.				
Availability of exploit (Exploitability)			<input type="text" value="Not Defined"/>	
Type of fix available (RemediationLevel)			<input type="text" value="Not Defined"/>	

Integrating IT and IT Security Through SCAP

Vulnerability Management

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System





SCAP Capability validations

- **FDCC Scanner:** a product with the ability to audit and assess a target system in order to determine its compliance with the Federal Desktop Core Configuration (FDCC) requirements. By default, any product validated as an FDCC Scanner is automatically awarded the Authenticated Configuration Scanner validation.
- **Authenticated Configuration Scanner:** a product with the ability to audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges. The FDCC Scanner capability is an expanded use case of this capability. Therefore, any product awarded the FDCC Scanner validation is automatically awarded the Authenticated Configuration Scanner validation.
- **Authenticated Vulnerability and Patch Scanner:** a product with the ability to scan a target system to locate and identify the presence of known software flaws and evaluate the software patch status to determine compliance with a defined patch policy using target system logon privileges.
- **Unauthenticated Vulnerability Scanner:** a product with the ability of determining the presence of known software flaws by evaluating the target system over the network.
- **Intrusion Detection and Prevention Systems (IDPS):** a product that monitors a system or network for unauthorized or malicious activities. An intrusion prevention system actively protects the target system or network against these activities.
- **Patch Remediation:** the ability to install patches on a target system in compliance with a defined patching policy.
- **Mis-configuration Remediation:** the ability to alter the configuration of a target system in order to bring it into compliance with a defined set of configuration recommendations.
- **Asset Management:** the ability to actively discover, audit, and assess asset characteristics including: installed and licensed products; location within the world, a network or enterprise; ownership; and other related information on IT assets such as workstations, servers, and routers.
- **Asset Database:** the ability to passively store and report on asset characteristics including: installed and licensed products; location within the world, a network or enterprise; ownership; and other related information on IT assets such as workstations, servers, and routers.
- **Vulnerability Database:** A SCAP vulnerability database is a product that contains a catalog of security related software flaw issues labeled with CVEs where applicable. This data is made accessible to users through a search capability or data feed and contains descriptions of software flaws, references to additional information (e.g., links to patches or vulnerability advisories), and impact scores. The user-to-database interaction is provided independent of any scans, intrusion detection, or reporting activities. Thus, a product that only scans to find vulnerabilities and then stores the results in a database does not meet the requirements for an SCAP vulnerability database (such a product would map to a different SCAP capability). A product that presents the user general knowledge about vulnerabilities, independent of a particular environment, would meet the definition of an SCAP vulnerability database.
- **Mis-configuration Database:** A SCAP mis-configuration database is a product that contains a catalog of security related configuration issues labeled with CCEs where applicable. This data is made accessible to users through a search capability or data feed and contains descriptions of configuration issues and references to additional information (e.g., configuration guidance, mandates, or other advisories). The user-to-database interaction is provided independent of any configuration scans or intrusion detection activities. Thus, a product that only scans to find mis-configurations and then stores the results in a database does not meet the requirements for an SCAP mis-configuration database (such a product would map to a different SCAP capability). A product that presents the user general knowledge about security related configuration issues, independent of a particular environment, would meet the definition of an SCAP vulnerability database.
- **Malware Tool:** the ability to identify and report on the presence of viruses, Trojan horses, spyware, or other malware on a target system

Sponsored by
DHS National Cyber Security Division/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checks

Vulnerabilities	Checklists	Product Dictionary	Impact Metrics	Data Feeds
Home	ISAP/SCAP	SCAP Validated Tools	SCAP Events	About
			Contact	Vendor C

FDCC

- [Home](#)
- [Disclaimer](#)
- [Contact](#)

NIST Resources

- [NIST Security Configuration Checklist for IT Products](#)
- [Security Content Automation Protocol](#)
- [Guidance for Securing Microsoft Windows Vista](#)
- [Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist](#)
- [Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist](#)
- [NIST Systems Administration Guidance for Windows 2000 Professional](#)
- [FISMA Implementation Project](#)
- [National Vulnerability Database](#)
- [Federal Agency Security Practices \(FASP\)](#)

Other Resources

- [OMB Memo M-07-11](#)
- [OMB Memo M-07-18](#)
- [OMB Memo 31 July](#)
- [OMB Memo 19 Dec](#)
- [OMB Memo M-08-22](#)

Federal Desktop Core Configuration FDCC

- [FDCC Major Version 1.0 Downloads - 2008-06-20](#)
- [FDCC Reporting Information](#)
- [In support of the OMB Memoranda](#)
- [Additional NIST Frequently Asked Questions - FAQs - 2008-01-28](#)
- [NIST Frequently Asked Questions - FAQs - 2007-07-31](#)
- [FDCC Implementers Workshop Workshop Presentations - 2008-02-03](#)
- [Workshop Agenda - 2008-02-03](#)
- [Third Annual Security Automation Conference Presentations - 2007-10-04](#)
- [Federal CIO Council 1 August 2007 FDCC Technical Exchange - 2007-10-30](#)
- [Please read the Download FAQs to resolve issues with downloading, logging on, and activating Windows Vista - 2007-08-20](#)

FDCC News

2008-06-20

[Major Version 1.0 of FDCC](#) released.

2008-05-01

[FDCC Proposed Updates Beta 2 Content and May Change List](#) posted.

2008-04-18

[FDCC 2008 Q2 XP and Vista VHDs](#) posted.

2008-03-21

[FDCC Proposed Updates Page](#) posted.

2008-03-21

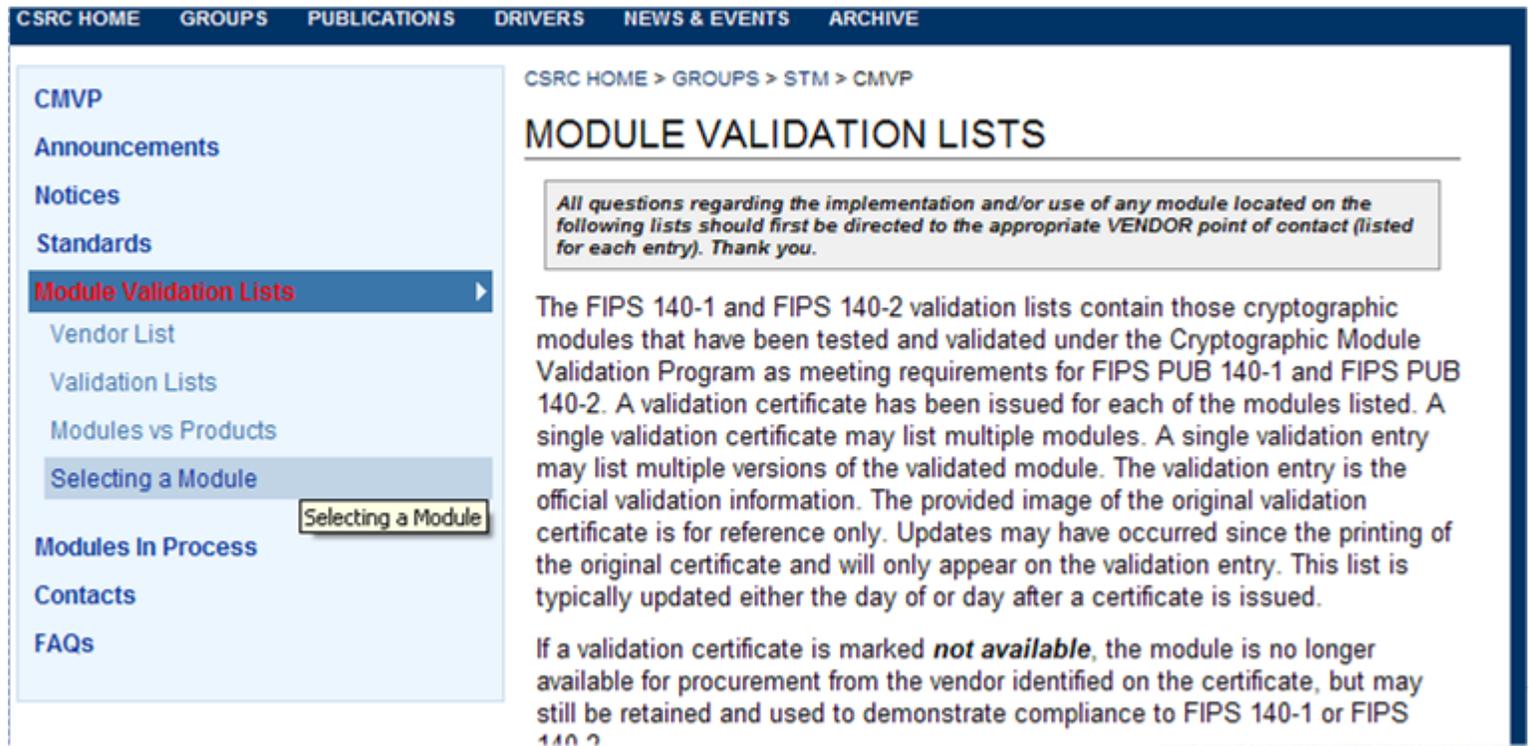
[FDCC Reporting Page](#) posted.

2008-02-26

Minor update made to [FDCC Reporting Format](#) - update pertains to the Schematron Stylesheet, please reference the changelog for details.

FIPS 140

- When selecting a module from a vendor, verify that the application or product that is being offered is either a validated cryptographic module itself (e.g. VPN, SmartCard, etc) or the application or product uses an embedded validated cryptographic module (toolkit, etc).
- Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module, the module provides all the cryptographic services in the solution, and reference the modules validation certificate number.
- The certificate number will provide reference to the CMVP lists of validated modules.



CSRC HOME GROUPS PUBLICATIONS DRIVERS NEWS & EVENTS ARCHIVE

CSRC HOME > GROUPS > STM > CMVP

MODULE VALIDATION LISTS

All questions regarding the implementation and/or use of any module located on the following lists should first be directed to the appropriate VENDOR point of contact (listed for each entry). Thank you.

The FIPS 140-1 and FIPS 140-2 validation lists contain those cryptographic modules that have been tested and validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 and FIPS PUB 140-2. A validation certificate has been issued for each of the modules listed. A single validation certificate may list multiple modules. A single validation entry may list multiple versions of the validated module. The validation entry is the official validation information. The provided image of the original validation certificate is for reference only. Updates may have occurred since the printing of the original certificate and will only appear on the validation entry. This list is typically updated either the day of or day after a certificate is issued.

If a validation certificate is marked **not available**, the module is no longer available for procurement from the vendor identified on the certificate, but may still be retained and used to demonstrate compliance to FIPS 140-1 or FIPS 140-2.



How to reach us

Look in the doc for the primary author:

CALL THEM

The screenshot shows the NIST Information Technology Laboratory website. The header includes the NIST logo and the text "National Institute of Standards and Technology Information Technology Laboratory". A search bar for CSRC is visible. The main navigation menu includes "ABOUT", "MISSION", "CONTACT", "STAFF", and "SITE MAP". The "STAFF" link is circled in black. Below the navigation, the page title is "Computer Security Division Computer Security Resource Center". A secondary navigation bar contains "CSRC HOME", "GROUPS", "PUBLICATIONS", "DRIVERS", "NEWS & EVENTS", and "ARCHIVE". On the left, a "Staff Information" dropdown menu is open, listing "Information Technology Laboratory (ITL) Division Information", "CSD Leadership", and "CSD Staff Directory". The main content area shows the breadcrumb "CSRC HOME > STAFF INFORMATION" and the heading "STAFF INFORMATION". Underneath, there is a section titled "ITL Division Information" with two bullet points: "National Institute of Standards and Technology (NIST)" and "Information Technology Laboratory (ITL) - Division 890".